Region-based group and hierarchical key management for secure smart grid communications

V. Madhu Viswanatham*

School of Computing Science and Engineering,
VIT University,
Vellore, Tamil Nadu, India
Email: vmadhuviswanatham@vit.ac.in
*Corresponding author

A.A. Chari

Department of OR &SQC,
Rayalaseema University,
Kurnool, Andhra Pradesh, India
Email: chari_anand@yahoo.com

V. Saritha

School of Computing Science and Engineering,
VIT University,
Vellore,Tamil Nadu, India
Email: vsaritha@vit.ac.in

Abstract: Considering the security requirements of smart grid in modern environment where they are used in cities, states and countries it has become imperative to develop a region-based security protocol for them. To provide security to group-based applications, the group members need to have a secret key which is common to all. The task of providing security to the group applications is a very critical task in smart grid. Considering this challenge for secure group applications, we propose a region-based group and hierarchical key management protocol. The protocol becomes scalable and reconfigurable dynamically by grouping the smart meters which behave as nodes in the smart grid based on the range of distribution substation (DSS). These TUs are hierarchically divided into different DSSs. The number of times the packet is encrypted is based on the number of levels in the hierarchy. As the levels in the hierarchy increases, the security is increased but the complexity also increases. The proposed protocol proves to be good, typically adapted to mobility of nodes and the performance of the protocol shows significant results.

Keywords: smart grid; secure communications; hierarchical key management.

Reference to this paper should be made as follows: Viswanatham, V.M., Chari, A.A. and Saritha, V. (2016) 'Region-based group and hierarchical key management for secure smart grid communications', *Int. J. Smart Grid and Green Communications*, Vol. 1, No. 1, pp.50–61.

Biographical notes: V. Madhu Viswanatham is an Associate Professor in the School of Computing Science and Engineering, VIT University, Vellore, India. He received his PhD in Computer Science and Technology from SK University, Anatapur, India. His research interests are in the areas of information security, wireless networks, grid computing and cloud computing. He has several years of experience working in academia, teaching and research.

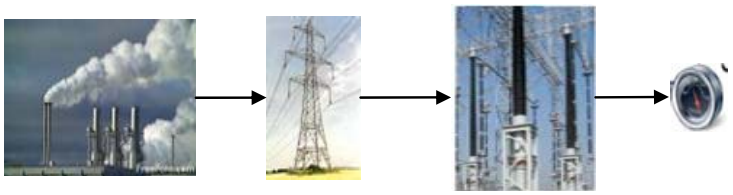
A.A. Chari is a Professor in the Rayalaseema University, Kurnool, India. His research interests include operational research, computer networks and web services. He has several years of experience working in academia, teaching and research.

V. Saritha is with the School of Computing Science and Engineering, VIT University, Vellore, India. She received her BTech in Electronics and Communication Engineering from Andhra University, Visakhapatnam, India and MTech in Computer Science and Engineering from VIT University, India. She has several years of experience working in academia, teaching and research. Her research interests include mobile and wireless systems and databases.

1 Introduction

The grid of electricity meters or the network of smart meters (SM) is referred as smart grid. It can also be referred as modern electricity grid. The thousands of consumers are being evolved over many years that need to be served by the electricity grids. As the population is being increased and the utilisation of power is increasing by them for various purposes, the challenge of the electricity distribution system is increased in generating the required power. Recently, the consumers are increasing their power consumption more and more. There are many factors like high price of electricity, reduced power generation, increasing debt of power which is related to electricity distribution system. Smart grids are very helpful to overcome all these constraints. The smart grid is used to control the power consumption by making the consumers to be aware of their power consumption and their respective prices. It is assumed that the overall power consumption can be controlled by making the end users aware of their power consumption as the end users will try to manage the power consumption based on the tariffs of the electricity, which will in turn help in power saving. Hence, the end users can be served in a cost effectively and scantiness of power can be lowered by power producers and power distributors by deploying SM (Misra et al., 2013). So, as in the other networks, the efficiency, reliability, control system and safety are required parameters in the smart grid system (Yan et al., 2013). The smart grid communication system is used to optimise the power consumption, proper utilisation of the power generated, increase the customer satisfaction (Misra et al., 2013). A smart grid is a hierarchical structure as shown in Figure 1. The highest level in the hierarchical structure is the main power station (MPS), and then comes transmission units, distribution substations, and finally SM as leaves.

Figure 1 Hierarchical structure of the smart grid (see online version for colours)



Due to considerable research and development in the field of smart grid communication, their security in real time systems has become a major consideration. Smart grid communication systems have some special properties due to which they are highly vulnerable to security attacks by adversary. The presence of wireless medium is the major weakness utilising which any adversary can attack the network. Also, lack of infrastructure providing secure communication is a big challenge in this unique network environment.

The hybrid technologies which are a combination of wired and wireless technologies are used in the existing electrical utility. The wired technology that can be used in the electrical system is copper-wire line, fibre optics, etc. The wireless technology that can be used in the electrical system is similar to the technology that can be used in cellular networks (Fan and Gong, 2013). The applications like supervisory control and data acquisition (SCADA)/energy management systems (EMS), distribution management systems (DMS), enterprise resource planning (ERP) systems are monitored/controlled by these smart systems.

As the network of electricity system is increasing day by day, the smart grid systems should be scalable such that it can support the network of any size and future set of functions. It must also be persistent in order to maintain the communication between the MPS and the SM in the hierarchical structure of the smart grid communication (Madani et al., 2007). The smart grid is not just making the electric grid more economical, greener, eco-friendly, but also insists security into the grid. The initiative source of security threats can be inside or outside of the electric security system. The threats from the industrial surveillance, radicals and black hat hackers can be treated as the outside threats. The security provision to electrical utilities is a very big challenge as the radicals and the intruders try to obtain the access of the details related to the system. The power production, generation and supply may be heavily interrupted by these revolutionary forces. Some of the internal threats could be from the employees of the same system who are discontent or it could result from the mistakes of the employees whose main intension might not be causing damage to the system. The systems security is affected weather the damage is caused intentionally or unintentionally which affects the generation or transmission of power.

There are four levels in the hierarchy of the smart grid communication system. The security threat can be at any level of the hierarchy. It can be considered that the substation is the significant level where the threat might be high as its communication involves with the control centre, other substations, remote monitoring systems and external data networks. So, highest priority is given to this location while providing the

security to the smart grid system. The security concern in the substation arises when the network interacts with the public network (Weerathunga, 2012).

The main objective of this paper is to develop a key management (KM) scheme for smart grid communication system by organising the network in a region-based fashion so that the scheme could be uniformly implemented over the entire network. This KM scheme is self-enforceable, i.e., it derives itself from each hierarchical level in a regular fashion. The scheme is successful in defending the network from security attacks and also maintains confidentiality of data transmitted between the nodes. The security model describes in detail the secure communication and the keys which are used at each hierarchical level.

The rest of the paper is organised as follows: Section 2 discusses the related work carried out in this area; the proposed protocol is discussed in Section 3. Performance analysis is given in Section 4 and finally Section 5 concludes the paper.

2 Related work

The survey of the smart grid communication infrastructures is presented in Misra et al. (2013). The authors presented the background, motivation and also the basic needs of the smart grid communication infrastructures. The authors also specified that the security is one of the major challenges in the smart grid communications as day by day there is an increase in vulnerabilities. The risk is increasing as the system is becoming more automated.

Naruchitparames et al. (2011) presented a model for secure communications in smart grid. In this model, the gateway between the intra and inter network communications is considered to be a smart meter. The appliances in the house are arbitrated using the smart meter by making it to function as firewall and supervise the incoming and outgoing traffic. Service providers are introduced as third parties in order to manage the contracted customers.

In Bou-Harb et al. (2013), the authors focused on the aspect of the communication security. The authors also presented about the network security related to all the possible communications. The authors claim that the proposed solution will reduce the vulnerabilities, risks and improve the cyber security of the smart grid.

In Metke and Ekl (2010), the security technologies like public key infrastructures and reliable computing for different smart grid communication networks are discussed by Metke and Ekl. The authors also discussed about basic necessities of the security system to make the future smart grid to operate successfully without any security threats. The elementary challenges in the smart grid communication system are acknowledged and the enduring consistency attempt in the industry are introduced in Yu et al. (2011), the communication infrastructures like home area networks, neighbourhood area networks, etc., are illustrated and also discussed the process of attaining the architectures of the communication infrastructures. The home area network is discussed more in detail by Naruchitparames et al. (2011). The application manager interface (AMI) infrastructure, security issues and the needs of the home area network are presented in Metke and Ekl (2010). The secure communication mechanism is modelled on home area network which is considered to be a subpart of the smart grid.

In Fan and Gong (2013), the authors used cryptographic techniques to provide the security in the communications of the smart grid and its control system. The authors also provided the comprehensive analysis of the vulnerability and cyber security of the smart grid.

Certification, reliability verification, admission control and discretion are the basic security mechanisms. The data belonging to one group should not be able to read by another group members or non-group members in group communication to make the session to be secure. A common key among the group members need to be found and preserve for the safe message service in the group. This common key is used to encrypt or decrypt the message switching within the group and is called as group key or traffic encryption key (TEK). The properties that must be met by the group key according to the model of Younis et al. (2006) are: the group key must be strong enough such that no inactive opponent can determine any group key and it must be impossible to estimate the group key by the unreceptive challenger; the autonomy of the group key must assure that the inactive opponent cannot discern any other group key using any proper subset of group keys; fragile forward concealment assures that the ex-group members must stay out in accomplishment of the new keys; fragile backward concealment assures that latest group members should not be able to determine the earlier used group keys.

After each join or leave node operation, i.e., when the members in the group changes, the two properties: fragile forward concealment and fragile backward concealment indicate that a rekeying process restores the group key. So, if there are numerous changes in the group members, then rekeying process may provoke overhead in the communication process. 1-affects-n scalability (Dondeti et al., 1999) is used to measure the performance of the rekeying process in terms of its pleased property – how well it scales to large and dynamic groups. If the consistent topologies like tree or a cluster-based structure are used to manage the secure group in the group KM may boost 1-affects-n scalability. To diminish the force of the key updating process (1-affects-n), dissimilar neighbouring TEKs can be generated for different clusters. The computation and communication overhead might become extreme to manage their virtual topology using these schemes. And also these schemes might not be always suitable for secure group communications or KM. Guaranteeing the admittance to an applicable group key at any time by only the legitimate members is the responsibility of the KM. So, in the case of multicast communications, subsistence of protected, strong KM scheme is very much crucial. In Chang and Chung (2003), Jablon (1996), and Rafaeli and Hutchison (2003), KM schemes are proposed to improve the protection and reduce the space required to store the keys. Clustering (Tseng et al., 2007) and hierarchical trees (Amir et al., 2004; Chiang and Huang, 2003; Liu and Zhou, 2002; Steiner et al., 1996; Yang and Zheng, 2001) are the two mainly familiar schemes for group organisations. Rekeying can be done very faster in clustering. The cost of the rekeying increases significantly during the change in the group members (group members join or leave the group), when the group size is large. Hierarchical tree structure is implemented by the majority group organisations. The reduction in the rekeying cost and the trouble-free KM during the modifications in the members of the group is the most important objective of a hierarchical tree. Increase in group size increases maintenance cost is one of the drawback in hierarchical tree structure.

3 Region-based group and hierarchical KM protocol

In this protocol we consider the network to be designed in a hierarchical fashion where smart grid communication system comprises of four hierarchical levels: MPS, transmission unit (TU), distribution substation (DSS) and SM. Here, SM are considered to be the nodes of the network. Sometimes, TUs, DSS or SM need to be introduced. Rarely, SM need to be changed from one position to another. If it is considered that SM are installed at the appliances of the consumers, then the SM change their location occasionally. When the smart meter crosses the DSS range but not the TU boundary, then the DSS membership is changed and the membership of TU is preserved. Both the TU membership and the DSS membership are changed when the smart meter crosses the boundary of the TU. A secret group key KG is shared among all the members under the MPS and secret key, K_{RLi} is shared among all the members of the TU in one level of the hierarchy in secure group communications.

The range of the DSS plays a very important role in the computation of the cost for group KM. The optimal DSS size is discovered and is operated using this value for our proposed region-based group and hierarchical KM scheme (HKMS) in order to reduce the KM rate in terms of network traffic. Each smart meter in the smart grid has a unique ID. The key distribution server generates a very large size of key pool S and assigns t number of secret keys from S to each smart meter in the grid. So in a range of DSS, each smart meter computes its DSS key.

$$K_{RK} = F\left(K_S, ID\right) \tag{1}$$

where F is a predefined random function pre-equipped in each node.

Once the DSS key generation process is completed, secret DSS-leader key K_{RL} is generated which is shared by all the leaders.

$$K_{RL} = H\left(K_{RK} \| T\right) \tag{2}$$

where T is the current timestamp of the leader.

Finally, TU-leader key K_{GLi} is derived by means of

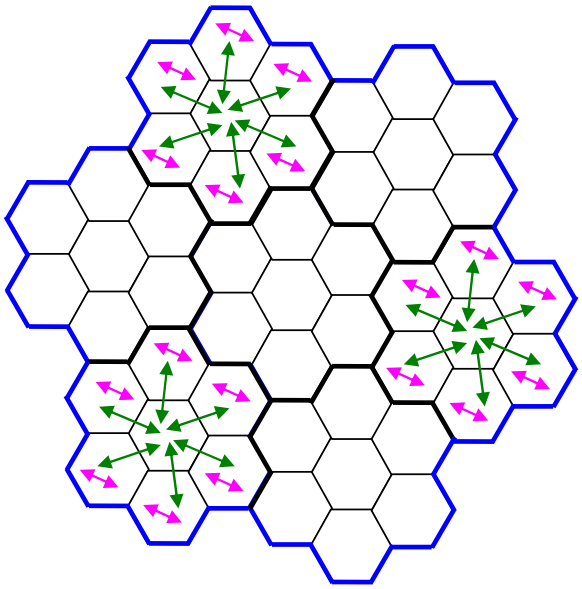
$$K_{GLi} = H\left(K_{RL} \| c\right) \tag{3}$$

where H is a cryptographically secure hash function which is computationally infeasible to revert, K_{RL} is the region-leader key, c is a fresh counter which will be incremented whenever a TU membership event occurs. The super-leader is elected among the TU-leader, which generates the MPS-leader key.

$$K_{SGLi} = H\left(K_{GLi} \| c\right) \tag{4}$$

As the level increases, the number of secret keys increases. The process of generating the keys is in hierarchical order from DSS to TU, TU to MPS, etc. The process of rekeying takes place whenever there is a change in the system. The change might be the smart meter leaving/entering a DSS/TU/MPS. When a smart meter is leaving one DSS and entering another DSS, rekeying needs to be done in both the DSSs. The membership view can be maintained at different levels of the system like DSS view, leader view, TU view, MPS view.

Figure 2 Region-based group and hierarchical KM (see online version for colours)



The structure of the protocol can be well explained using Figure 2. In Figure 2, each cell is treated as a range of DSS. Seven cells together are referred as a TU. So, a DSS-leader is selected from each cell. TU-leader is selected from each group of seven cells. Seven groups together are referred as next level of groups, TU. So, one leader is selected in this level. As the number of DSS increase, the number of levels increases, so as the number of secret keys are increased. As the complexity of the system increases with area to be covered, the outsider attacks.

3.1 Security model

Some of the requirements for secure group communications like confidentiality, reliability and certification need be satisfied by the proposed protocol, region-based and hierarchical group KM. This protocol deals with both outsider and insider attacks.

As the MPS key is generated by all TU-leader by applying a cryptographically secure hash function using the TU-leader key as a hash key, MPS key secrecy is assured since it is impossible to estimate for an opponent to determine the MPS key without knowing the secret key to hash function, which in our scheme is the TU-leader key. The subsequent keys are also dependent on its lower level keys, so it is not possible to hack the system from outside. Fragile forward and backward concealment (Naruchitparames et al., 2011) properties are preserved by means of immediate rekeying, i.e., a rekeying operation is performed whenever there is a change in the membership. Fragile forward concealment is guaranteed since an inactive opponent who knows a contiguous subset of old group keys cannot determine any subsequent group key. Fragile backward concealment is guaranteed since an inactive opponent who knows a contiguous subset of group keys cannot determine previous group key.

As is used hash with two dissimilar values which are the leader key and fresh counters to produce a TU key, key independence is assured. Certification is provided for

each member through the private and public keys. The challenge/response mechanism is used to certify the identity of the member which is newly joining a group based on its public/private key pair. The generation of the DSS, TU, MPS keys guarantees the certification of the source. The encrypted message is exchanged among the members of the group. This encrypted message is decrypted using the secret key which guarantees the secrecy. As there are DSS, TU and leaders, different keys are determined at DSS level, leader level and at TU level. So, the members in the range of DSS use DSS key to encrypt/decrypt their messages, leaders use leaders key to encrypt/decrypt their messages and respectively with the members in the range of TU using TU key to encrypt/ decrypt their messages in the communication process. TU key is determined based on the leader key using MAC. But the leader key depends on the DSS key, so, the member of the DSS who has and can only use the regional key, can decrypt the group key.

The intra-DSS communication is carried out among the members of the DSS using their shared secret DSS key. The inter-DSS/intra-TU communication is carried out among the leader using their shared secret leader key. Finally, the inter-TU communication is carried out by the shared secret TU key. Similarly, MPS communications are carried out by the shared secret MPS key. The different number of levels in the hierarchy of keys, the integrity is preserved.

It is mostly impossible for the outsider attacks as the keys are dependent on it sub-level keys. So, in our protocol, we are completely avoiding outsider attacks. To talk about the insider attack, each level is having different keys, so level wise attacks are controlled. Also we deal with fragile forward and backward concealments. To control the attacks which may occur at the same level could be managed by having the private key and by encrypting the packet twice.

3.2 Rekeying protocol

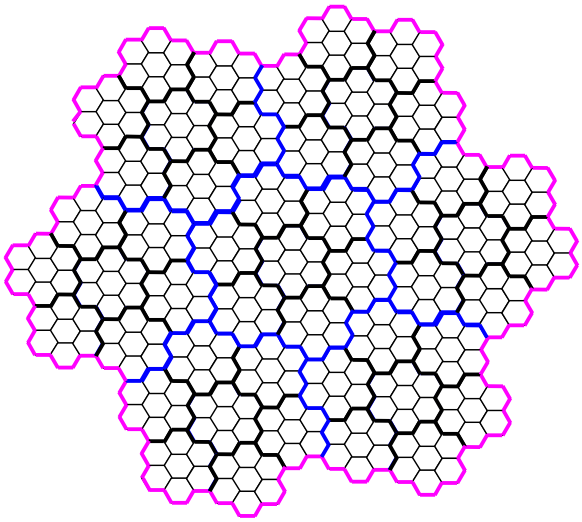
The rekeying protocol is executed only when any smart meter leaves from any level of the grid. This need not be done when any smart meter is being installed a particular location in the network because there is no problem with the security requirements. It must be observed that any smart meter belongs to a particular DSS also belongs to a particular TU, similarly a particular MPS. So, when any smart meter leaves from any DSS, the DSS level secret key is to be rekeyed. As the DSS level is the lowest level in the network, the upper level secret keys are to be rekeyed. When the TU secret key is rekeyed, as MPS key is dependent on the group level secret key, the MPS key is also need to be rekeyed. When a smart meter leaves a DSS and enters another DSS, then rekeying is to be done only in the DSS from which the smart meter leaves. As we are not doing rekeying when a new smart meter enters the grid, the cost of rekeying process is reduced to more extent.

3.3 Illustrative example

In Figure 3, we showed how the grid is divided into DSS, which are shown in black coloured border, TU which are with blue coloured border, and MPS with pink coloured border. For each DSS, DSS key is generated. Let us represent the DSS key as K_{RKi}, for each DSS, leader is elected, and leader key is generated. This is represented as K_{RLi}, for each TU, TU key is generated and is represented as K_{GLi}, then TU-leader is elected and TU-leader key is generated and is represented as K_{SGLi}. The key are dependent on its

descendents key. So, it is very difficult or highly impossible for the intrusion. When the communication is taking place from the higher level of the hierarchy to the lower level, then the MPS leader is sending the decrypted message using K_{SGLi} to the next level of the hierarchy, and then the each TU leader decrypts the message using K_{GLi} and sends to the DSS level leaders. DSS level leaders decrypt the message using K_{RLi}, and sends to the members of the DSS, i.e., SM which is finally decrypted by the destination member using K_{RKi}. Similarly, the reverse way of communication is also carried out. When the member of the DSS is moving from one DSS to another, then there is a need to change the DSS key. As DSS leader key is dependent on the DSS key, it also needs to be modified. Similarly, the TU leader key and MPS leader key also need to be changed. When ever, there is a change in the SM movement, the keys need to be altered based on the movement. The complexity of the system is slightly increased to improve the confidentiality. The advantage of the proposed protocol is that the cost is reduced as the cost is calculated when the member enters the DSS/TU as it not required because the keys are not modified when a member joins the DSS.

Figure 3 Network with DSS, TU, MPS (see online version for colours)



4 Performance analysis

We develop a performance model to evaluate the grid traffic cost generated for region-based group and hierarchical KM protocol for smart grid. The total communication Cost is the cost of the smart meter leaving the grid. The computation of the cost includes different cases:

$$\text{Cost} = \text{cost}_{\text{DSS member}}$$

$$C_{\text{DSS member}} = \left(N - N_{\text{DSS-leader}} - N_{\text{TU-leader}} - N_{\text{MPS-leader}} - \ldots\right) * C_{\text{MPS}} / N$$

$$P_{\text{DSS-leader}} = N_{\text{DSS}} / \left(N_{\text{DSS}} + N_{\text{DSS member}} + N_{\text{TU member}} + N_{\text{MPS member}}\right)$$

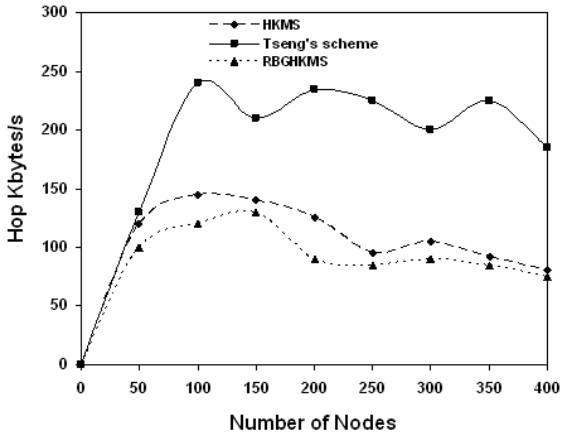
Similarly, $P_{TU\text{-}leader}$ and $P_{MPS\text{-}leader}$ are calculated.

where $C_{MPS} = C_{MPS\ update} + C_{MPS\ rekey}$.

Table 1 Basic model parameters

Notation	*Description*
Cost	Total communication cost
$Cost_{DSS\ member}$	Cost when DSS member leaves
N	Total number of nodes
$N_{DSS\text{-}leader}$	Number of DSS leaders
$N_{TU\text{-}leader}$	Number of TU leaders
$C_{MPS\ update}$	Cost of updating the MPS information
$C_{MPS\ rekey}$	Cost of rekeying the MPS key
$P_{DSS\text{-}leader}$	Probability of the DSS member to be a DSS-leader
$P_{TU\text{-}leader}$	Probability of the TU member to become a TU-leader
$P_{MPS\text{-}leader}$	Probability of the MPS member to become a MPS-leader

Figure 4 Overall cost vs. number of nodes



The simulation is carried out 30 runs. The average of all the runs is considered in plotting the graphs. The simulation time for each run is 40 s. The area of the grid is considered to be 1,500 sqm. The number of SM is considered to be 300. Three levels of hierarchy are taken. So, the complete grid is partitioned into DSS, TU and MPS. The number of bits times the number of hops these information travels is calculated as cost. The cost is calculated in terms of hop Kbytes/s. We compare the proposed protocol with the HKMS because both the protocols use hierarchical structure for the network. The disadvantage of the HKMS scheme is that it has the overhead of the communication node separately besides head node. This overhead increases the hop count also which in turn increases the cost. In Tseng's scheme, the network is partitioned into clusters but the hierarchy is not followed, which increases the integrity of the system. The cost of the proposed protocol is reduced when compared to the Tseng's scheme because of the fragile forward and backward concealment. The graph in Figure 4 shows that the performance of the

proposed protocol is better when compared to HKMS and Tseng's scheme. Actually, the HKMS and Tseng's scheme are proposed for MANET. We considered these schemes as they closely related to the concept, implemented for the smart grid and then compared with the proposed protocol. The performance is improved because the proposed protocol does not consider the communication node and leader node separately. So, the complexity of the protocol is reduced.

5 Conclusions

In this paper, we have proposed a protocol which organises the grid in a hierarchical fashion and then implements a KM scheme for each level. The different secret keys are generated at different levels which increases the security of the data. The cost of the system is calculated by considering different cases like when the smart meter leaves from DSS level, TU level or MPS level, DSS leader, TU leader or MPS leader. It is also shown that the cost of rekeying is less when compared to the legacy systems. At each level private keys are also generated during communication.

References

Amir, Y., Kim, Y., Nita-Rotaru, C., Schultz, J.L., Stanton, J. and Tsudik, G. (2004) 'Secure group communication using robust contributory key agreement', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 15, No. 5, pp.468–480.

Bou-Harb, E., Fachkha, C., Pourzandi, M., Debbabi, M. and Assi, C. (2013) 'Communication security for smart grid distribution networks', *Communications Magazine*, Vol. 51, No. 1, pp.42–49, IEEE.

Chang, C-C. and Chung, C-Y. (2003) 'An efficient session key generation protocol', *Proceedings of the 2003 IEEE International Conference on Communication Technology*, pp.203–207.

Chiang, T-C. and Huang, Y-M. (2003) 'Group keys and the multicast security in ad hoc networks', *Proceedings of the 2003 IEEE International Conference on Parallel Processing Workshops*, Kaohsiung, Taiwan, pp.385–290.

Dondeti, L., Mukherjee, S. and Samal, A. (1999) *A Distributed Group Key Management Scheme for Security Many-To-Many Communication*, Technical Report.

Fan, X. and Gong, G. (2013) 'Security challenges in smart-grid metering and control systems', *Technology Innovation Management Review*, pp.42–49.

Jablon, P.D. (1996) 'Strong password-only authenticated key exchange', *Proceedings of the 1996 Computer Communication*, pp.5–26.

Liu, J. and Zhou, M. (2002) 'Key management and access control for large dynamic multicast group', *Proceedings of the 4th IEEE Conference on International Workshop*, pp.121–128.

Madani, V., Vaccaro, A., Villacci, D. and King, R.L. (2007) 'Satellite based communication network for large scale power system', *iREP Symposium – Bulk Power System Dynamics and Control – VII*, Revitalizing Operational Reliability.

Metke, A.R. and Ekl, R.L. (2010) 'Security technology for smart grid networks', *Smart Grid, IEEE Transactions on*, Vol. 1, No. 1, pp.99–107.

Misra, S., Krishna, P.V., Saritha, V. and Obaidat, M.S. (2013) 'Learning automata as a utility for power management in smart grids', *Communications Magazine*, Vol. 51, No. 1, pp.98–104, IEEE.

Naruchitparames, J., Giine, M.H. and Evrenosoglu, C.Y. (2011) 'Secure communications in the smart grid', *Consumer Communications and Networking Conference (CCNC)*, pp.1171–1175, IEEE.

Rafaeli, S. and Hutchison, D. (2003) 'A survey of key management for secure group communication', *ACM Computing Surveys (CSUR)*, Vol. 35, No. 3, pp.309–329.

Steiner, M., Tsudik, G. and Waidner, M. (1996) 'Diffie-Hellman key distribution extended to group communication', *Proceedings of the Third ACM Conference on Computer and Communications Security*, pp.31–37.

Tseng, Y-M., Yang, C-C. and Liao, D-R. (2007) 'A secure group communication protocol for ad hoc wireless networks', *Advances in Wireless Ad Hoc and Sensor Networks and Mobile Computing*, Book Series Signal and Communication Technology.

Weerathunga, P.E. (2012) *Security Aspects of Smart Grid Communication*, University of Western Ontario-Electronic thesis and dissertation Repository, p.843.

Yan, Y., Qian, Y., Sharif, H. and Tipper, D. (2013) 'A survey on smart grid communication infrastructures: motivations', requirements and challenges', *Communications Surveys & Tutorials*, Vol. 15, No. 1, pp.5–20, IEEE.

Yang, P. and Zheng, S. (2001) 'Security management in hierarchical ad hoc network', *Proceedings of the 2001 International Conferences on Info-Tech and Info-Net (ICII)*, pp.642–649.

Younis, M., Ghumman, K. and Eltoweissy, M. (2006) 'Location-aware combinatorial key management scheme for clustered sensor networks', *Parallel and Distributed Systems, IEEE Transactions on*, Vol. 17, No. 8, pp.865–882.

Yu, R., Zhang, Y., Gjessing, S., Yuen, C., Xie, S. and Guizani, M. (2011) 'Cognitive radio based hierarchical communications infrastructure for smart grid', *Network*, Vol. 25, No. 5, pp.6–14, IEEE.