On the Self-Healing Mechanism in Smart Grid Networks

Keun-Woo Lim[1], Woo-Sung Jung[1], Young-Bae Ko[1] and YoungHyun Kim[2]

[1]Graduate School of Information and Communication, Ajou University, Korea
[2]Korea Electric Power Corporation, Research Institute, Korea
{kwlim27, woosung}@uns.ajou.ac.kr, youngko@ajou.ac.kr, yhkim@kepri.re.kr

Abstract

This paper proposes a self-healing wireless network mechanism to provide efficient servicing in Smart Grid network[1]. The nature of Smart Grid environment requires high level of wireless networking reliability and stability for providing accurate power related information to users. To provide these requirements in the wireless networking perspective, the proposed self-healing mechanism uses automated services to acquire various wireless environment parameters and use them to adapt and tune the network. Parameters such as MAC retransmission count, Bit Error Ratio (BER), and Received Signal Strength (RSS) are used and modified to detect various types of problems in the network. Then based on these detections, the network adaptively enforces its transmission policies to heal from these problems. Our self-healing mechanism eventually helps in increasing packet delivery and real-time properties of the wireless network, providing higher reliability for smart grid services. We evaluate the performance of our mechanism via NS-3 simulator and show that our mechanism can enhance the reliability of the smart grid network via efficient self-healing methods.

Keywords: *Self-Healing Networks, Smart Grid Networks, Transmission Reliability*

1. Introduction

The smart grid is a new paradigm of electrical infrastructure that is integrated with IT communication technologies to support various future electrical services. These properties make smart grid a vast area system, which is bound to connect most of the existing electrical infrastructure. The integrated networking technologies that support the smart grid system are required to guarantee high-performance, highly-reliable networking functions to accurately provide quality of service to users in the smart grid system [2, 3]. To support these requirements, wireless networking technologies such as ZigBee and WLAN mesh [4] have gained interest as methods for scalable and efficient management of the smart grid networks.

However, due to the dynamicity of its nature, wireless networking systems have some problems that may prevent them from meeting the requirements of the smart grid systems. Furthermore, various disturbances and interferences in the smart grid environment may affect the wireless conditions of the network, deteriorating its quality and causing faulty transmissions to occur. In order to guarantee high reliability and stability under smart grid environments, this phenomenon should be accounted for and the wireless network must be able to take appropriate actions by itself without human intervention to cope with these problems.

[1] A preliminary version of the paper has been presented at IST 2012 [1].

One method of alleviating these problems is utilizing the concept of Self-Organizing Networks (SON) [5]. Via self-organization, the network can automatically detect problems that occur in the network through various network parameters. When a problem is detected, the network can automatically make decisions to tune its parameters and adapt to the dynamic changes that are deteriorating the network conditions. Self-healing, a major part of self-organization that can provide these capabilities, is considered a vital requirement for efficient management of the wireless networks [6]. However, self-healing networks in smart grid can be very complex and difficult to achieve, as self-healing modules must compromise with various problems that may occur in wireless networks while also considering the unique properties of the smart grid systems.

For example, we focus on the Neighborhood Area Network (NAN) in the smart grid networking infrastructure. Nodes in the NAN can act as a data gathering backbone for Home Area Network (HAN) nodes generating Advanced Metering Infrastructure (AMI) data. At the same time, NAN must also handle its own data transmissions such as power quality monitoring and substation surveillance. Sudden increase in generation and burst of these data traffic may induce intra-network problems, such as transmission collision between packets. Also, situational interferences from exterior properties of network such as vehicles, buildings, and humans may interrupt with the signals and cause fading, inducing outer-network problems that also result in failure of packet transmissions. Considering these properties, efficient self-healing mechanisms for smart grid must provide countermeasures for these problems.

This paper proposes a self-healing network mechanism for supporting smart grid networks. To cope with the dynamicity of the smart grid network, a self-healing module is implemented to automatically enforce various data transmission policies according to the environments. Values such as MAC retransmission count [7], bit error ratio (BER), and received signal strength (RSS) are extracted from the transmission layers and utilized to sense the current conditions of various applications and service in the smart grid network. By using these methods, the self-healing mechanism aims to maintain the reliability of the network. We observe using NS-3 simulator that our self-healing module can enhance the network to be more resistant to network changes and provide more stable services to smart grid users.

2. Background and Related Works

2.1. Need of Self-Healing in Smart Grid Networks

Self-healing is a vital feature in smart grid that aims to automate the healing process of the entire power system. For the smart grid systems to maintain high standards of reliability, the wireless networking and communication protocols used in the smart grid system must also provide means of efficient self-healing procedures. This can be a very challenging task to achieve, as these self-healing modules must compromise with various problems that may occur in these wireless networks while also considering the unique properties of the smart grid systems.

For example, we focus on the Neighborhood Area Network (NAN) in the smart grid networking infrastructure. Nodes in the NAN can act as a data gathering backbone for Home Area Network (HAN) nodes generating Advanced Metering Infrastructure (AMI) data. At the same time, NAN must also handle its own data transmissions such as power quality monitoring and substation surveillance. Sudden increase in generation and burst of these data traffic may induce intra-network problems, such as transmission collision between packets. Also, situational interferences from exterior properties of network such as vehicles, buildings, and humans may interrupt with the signals and cause these signals to fade, inducing outer-network problems that also result in failure of packet transmissions.

Considering these properties, efficient self-healing mechanisms for smart grid must provide countermeasures for these problems. To do this, an accurate detection method is required to pinpoint the occurrence of these interferences in the communication layers. Also, specific policies must be given to the network protocols to adapt to these deteriorated environments and maintain the reliability of the network.

2.2. Related Works

Currently, much research has been made on self-healing network systems, but only a few of them have their focus on Smart Grid networks. For example, Wang [5] emphasizes on the requirement of self-healing in AMI based Smart Grid architecture, and surveys two methods by using C12.22 and SIP standards. However, these schemes are restricted on the specific protocols and cannot be adoptable for lower-layer protocol problems.

While not exactly proposed for self-healing in smart grid, automatic route repairing methods such as AODV local route repair [8] can be utilized in the smart grid networks. However, these works do not provide enough functions to accurately detect and adapt to the status of the network. Various works for self-management and automated problem detection in sensor networks have been presented [9, 10]. Ramanathan [9] utilizes various intra-network metrics to detect faulty operations and reports them to the sink node in a centralized manner. On the other hand, Bourdenas [10] provides a more scalable local self-healing architecture to adaptively treat faulty sensor nodes in the network. These works in sensor networks may be of interest, but they cannot ultimately be the ideal case in Smart Grid environments because whereas sensor networks consider energy efficiency as the utmost importance, Smart grid environments must also consider reliability as another critical factor.

3. The Proposed Self-healing Mechanism

The overall mechanism of our self-healing module follows the basic policy-based self-managing module defined by Agrawal [11]. As seen in Figure 1, the proposed mechanism is implemented independent to other layers of the network. Each node is just locally required to maintain the self-healing module to adapt to various problems in the network. For our network architecture, we assume the area of NAN, where nodes inside the network form a multi-hop architecture. These NAN nodes are managed by multiple gateway nodes, which act as a portal to exterior networking backbones. NAN nodes have a property that most of their transmitted data are directed towards the gateway nodes. Note that many of the smart grid applications, such as Advanced Metering Infrastructure (AMI) and periodical monitoring from HAN, power monitoring data, and substation monitoring have such a client-to-server transmission property.

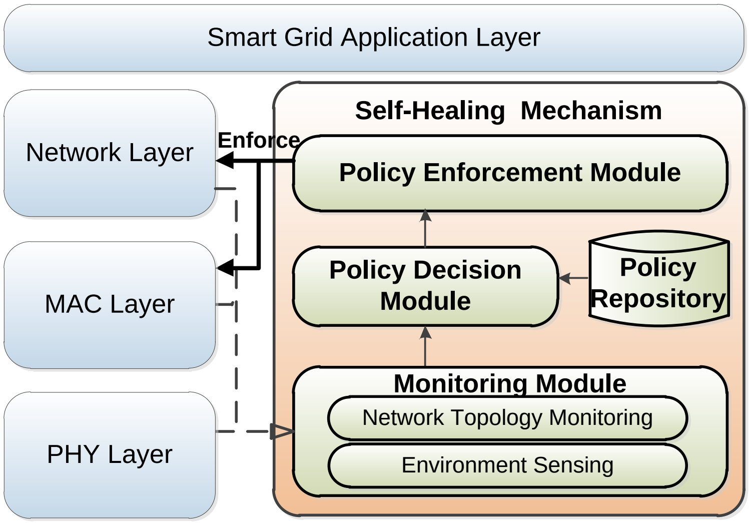


Figure 1. Proposed Self-Healing Mechanism

3.1. Monitoring Module

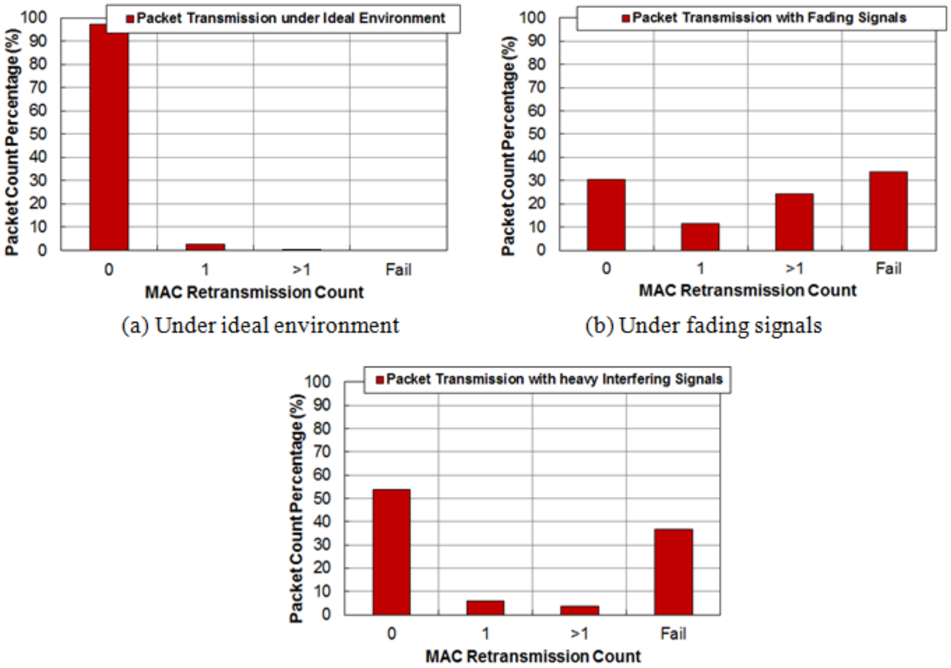
The monitoring module is in charge of recognizing the current formation of the network and periodically sensing the status of the wireless environment. In a multi-hop network with multiple gateways installed to support backbone connections, the monitoring module of each node must recognize the number, ID, and hop count of all the gateways in the network. This information is stored by each node and maintained for use in other modules. To acquire this information, the gateway nodes will periodically broadcast advertisement messages to all the nodes in the network. Any node receiving this advertisement message will update their gateway information and rebroadcast the packet to other nodes. Since only the existence of each gateway needs to be known to each node, the periodic rate of this advertisement should be long enough to reduce the effect it may induce on other important data transmissions.

The environment sensing module retrieves the current channel information of the network, such as the MAC retransmission count, BER, and the RSS. These values will be periodically transmitted to the policy decision module, which will utilize and modify these values to provide more suitable monitoring decisions in the smart grid environment.

3.2. Policy Repository

The policy repository defines and manages the types of policies that we will enforce in the network. Based on the information from the monitoring module, network related policies such as redundancy control and back-off timer control are defined in the repository. Types of policies that we desire can also be added, triggered on/off, or removed by configuring the repository. The information in the repository is used by the policy decision module to decide and enforce the appropriate policies.

3.3. Policy Decision Module



(a) Under ideal environment

(b) Under fading signals

(c) Under heavy interference

Figure 2. Observation of the Network Effects on MAC Retransmissions

Problem Detection: The MAC retransmission count can be utilized to decide that a certain problem is deteriorating the network. We have made a simple experiment via NS-3 simulation to justify this statement. 36 nodes were placed in a grid with 4 gateways at each corner of the grid. The 802.11s4 was used with the 54Mbps 802.11a as the PHY/MAC standard. The initial distance between each node is 100m. MAC level retransmission limit is set to 5, where any packet exceeding that amount is dropped. Figure 2(a) shows that the under an ideal environment, most of the transmitted MAC frames do not attempt any retransmissions. For Figure 2(b), we increased the distance between each node to 200m and produced more fading in the signals. As a result, nearly 70% of the frames that have been transmitted attempted at least one MAC level retransmission. For Figure 2(c), we generate more data to create more interference for the nodes. As a result, the retransmission values increased and MAC frames were either successfully transmitted without a retransmission or completely dropped. From these results, we can observe that multiple MAC level retransmissions can be a good indicator for detecting that some problem is affecting the reliability of the network. Using these observations, we will define a new indicator, named as smart grid problem indicator sg_{pi}:

$$sg_{pi} = \sum_{i=low\_category}^{high\_category} (N_r(i)\times\omega_i)/(N_s+N_f) \qquad (1)$$

where i = the category of the smart grid application, Nr(i) = retransmission count of packet with category i, and ω_i = the weight of the category depending on its priority and importance. The Ns and Nf values will respectively represent the successful and failed delivery of the packets. Therefore, (1) will average the total amount of MAC retransmissions that has been attempted per every transmitted packet, with more penalties on the retransmission of more important smart grid data, such as on-demand AMI and power quality data requests and management data.

The indicator sg_{pi} will notify the policy enforcement module that a problem has occurred in the network if sg_{pi} is larger than threshold value N. The value of N can be changed to control the sensitivity of the self-healing mechanism, with smaller N values increasing the chance of problem being triggered. However, it should not be too short to prevent excessive sampling. If the problem is triggered, further policies are decided by measuring the modified RSS and BER values in step 2.

Problem Confirmation: As seen in Fig. 2, the sg_{pi} value based on retransmission values cannot exactly pinpoint whether the problem is a fading signal problem or a heavy interference problem. Instead, this is confirmed by observing the changes that occur in the RSS and BER values. Under reliable circumstances, the values of RSS and BER in each received packet are utilized by each node using the moving average of each value. The moving average, $fade_{ci}$, is calculated as shown below,

$$fade_{ci} = \sum_{i=1}^{n} (RSS_j \times \omega_i) \big/ n \tag{2}$$

j = 1 is the most recent RSS information that is acquired from the most recently received frame, and n = number of RSS information that will be considered in the moving average. This moving average will also consider the weight of each data category to react more sensitively to important smart grid data.

The $intf_{ci}$ value is also calculated similarly to (2), but instead calculates the BER value. We must consider that this moving average will only calculate the $fade_{ci}$ and $intf_{ci}$ values when the network is considered stable, and when there are no problem triggers from step 1. If the received RSS values are lower than the $fade_{ci}$ by more than the *trigger_threshold_value*, it is confirmed that the network is suffering from signal fading. The interference trigger is turned on instead when the BER values are higher than the $intf_{ci}$. The value of the *trigger_threshold_value* may vary according to the aggressiveness of the self-healing module that the user desires. Once it is confirmed that there is a problem, the policy decision module passes this information to the policy enforcement module.

3.4. Policy Enforcement Module

The policy enforcement module receives information from the policy decision module and enforces different policies:

Redundancy Enforcement: Upon confirmation of fading problem, the module will enforce the redundancy policy to increase the data delivery ratio. By using the monitoring module, the enforcement module can realize the number of gateways in the network as well as the hop-count and link cost to each gateway. The module will process the data packet transmitted from the application layer, create multiple copies of it, and then apply different destination gateways to each copy of the data. The forwarded packets generated by other nodes are not increased to prevent transmission looping problems or excessive redundancy. Even though increasing the redundancy may increase the chance of traffic collision and congestion, it can be a suitable method for increasing reliability in smart grid environments. This is because the nodes in the smart grid environment do not constantly generate heavy real-time traffic such as streaming multimedia data.

Back-off Timer Enforcement: Upon confirmation of interference, the module is required to transmit on-going data traffic in a safer manner. The back-off timer enforcement component controls this by enforcing new back-off timers to the MAC layer. Increasing the back-off timer will deter the transmission of each packet between the nodes in that region, allowing less transmission collisions and interference at cost of slightly higher delay. To control the level of enforcement, formula (3) is used,

$$CW_{MAX\_adj} = CW_{MAX} \times \left(1 + \frac{N_f}{N_s + N_f}\right) \tag{3}$$

where CWMAX = the default maximum setting of the contention window. The enforced back-off timer policy will last until the calculation of the MAC level retransmission in (1) reports that the condition of the network is stable again.

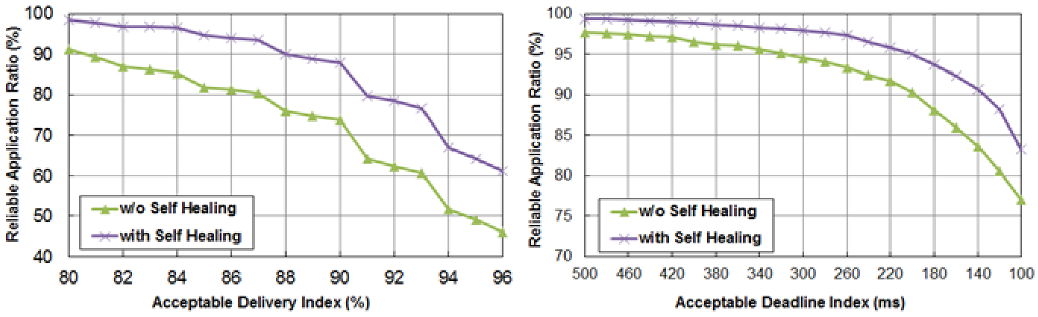
4. Performance Evaluation

The performance of our proposed self-healing mechanism is evaluated using the NS-3 simulator. 34 general NAN nodes are placed randomly in a 400 * 400 network with 2 gateways placed on opposite corners of the network. Each node is equipped with two 5 GHz 802.11a radios which can utilize one of 7 orthogonal channels per radio. Data transmission rate for each radio can support up to 54Mbps. Each node will transmit each of the 7 applications listed in the smart grid application service set defined by KEPRI which is shown in Table 1. AMI are the metering data generated at the HAN layer and transmitted through the NAN nodes. Power quality monitoring data and video surveillance data are NAN applications. The Requested on-demand data has the highest category (ω_1), while the other AMI and power quality data belongs in the second category (ω_2). The video surveillance data will be in the lowest category (ω_3). The values of each weight are differed to provide differentiation between smart grid data.

Table 1. Smart Grid Application Set

Type of Service	Weight depending on category	Transmission Interval (Second)	Application Size (Bytes)
Requested AMI Data	ω_1	On-demand	123
Requested Power Quality Data	ω_1	On-demand	1000K (per second)
Periodic AMI Data	ω_2	15	1024
Periodic Power Quality Data	ω_2	4	4096
AMI Management Data	ω_2	15	1024
Power Management Data	ω_2	15	1024
Video Surveillance	ω_3	0.16	1024

In a simulation time of 500 seconds, each periodic application is initiated at 10 seconds and continued until the end of simulation. The on-demand data are randomly pulled by the server from each node, at a rate of one generation per node. The value of *n* in equation (2) is configured to 5, while the sampling period of equation (1) is set to 1 second. These values are carefully chosen for the smart grid environment to prevent over-passiveness or over-activeness of our mechanism. For the NAN nodes, we utilize the IEEE 802.11s based multi-hop mesh network, while the 802.11 is used to form the structure for MAC and PHY layers and provide the MAC retransmission count, BER, and RSS values. In this paper, we have mainly focused our simulation environment on the smart grid NAN.



(a) Application-level Delivery Ratio (b) Application-level Deadline Meet Ratio

Figure 3. Performance Evaluation of Transmission Reliability

Figure 3(a) shows the packet delivery ratio of all the applications generated by each node. For comparison in Figure 3, the weight values for the self-healing mechanism are all configured to 1. Packet delivery ratio represents the total amount of successfully transmitted data packets divided by the total transmissions that have occurred in the network. The acceptable delivery index is the threshold for deciding whether a certain application of a node was considered to be transmitted reliably. The reliable application ratio on the y-axis will represent the percentage of the applications that had a packet delivery ratio over the index. With the self-healing module installed and the acceptable reliability threshold configured as 90%, more than 88 percent of the applications have managed to be reliably transmitted. Even when the reliability threshold is high as 96%, more than 60% of the applications managed to exceed the threshold. On the other hand, without our self-healing mechanism, the reliability of each application degrades more than 15% in the worst case.

Figure 3(b) shows the reliability of the proposed mechanism when transmission deadline requirements are configured. Reliable application ratio is determined by whether the average transmission latency of a certain application is lower than the acceptable deadline index. Even though the back-off policy is expected to increase the latency of the self-healing mechanism, the proposed mechanism actually meets higher deadline requirements because the back-off policy can reduce the contention and retransmissions that are occurring in the network. This in turn provides better transmission opportunities for each node.

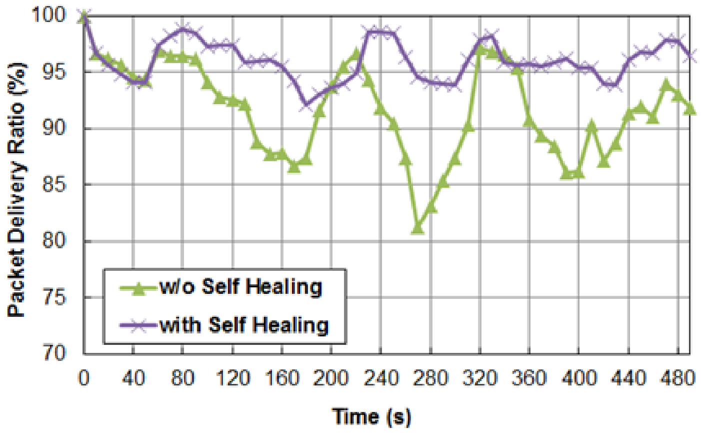
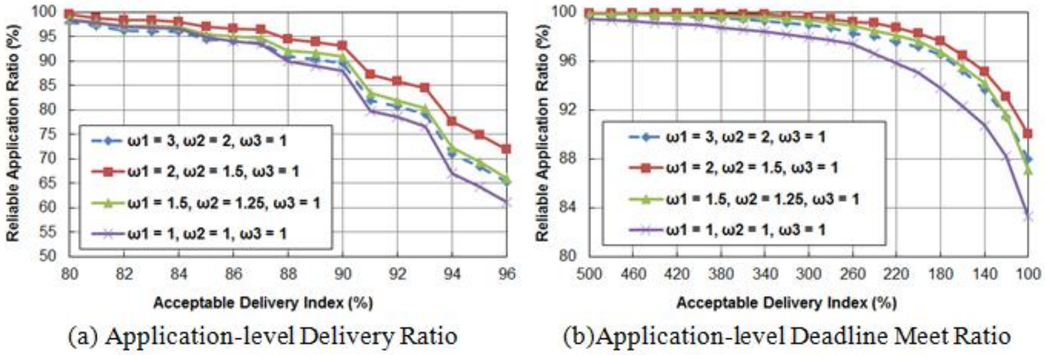


Figure 4. Delivery Ratio in Relation to Time

Figure 4 shows a scenario of the packet delivery ratio in relation to time. The packet delivery tends to fluctuate highly when the proposed self-healing mechanism is not used. This is because when bursts of on-demand data are made, the network cannot easily adapt to these problems in the network. On the other hand, the network with the proposed mechanism can effectively sense these variations in the network and make appropriate changes to it. As a result, the delivery ratio is maintained above 95%, never going under 90%.



(a) Application-level Delivery Ratio (b)Application-level Deadline Meet Ratio

Figure 5. Performance of the Self-Healing Scheme with Weight Variations

Figure 5 shows the effect of weights for different applications in the network according to their importance when the proposed self-healing scheme is applied. The value of ω_1, ω_2, and ω_3 are modified to alter the sensitivity of our proposed self-healing mechanism. Figure 5(a) and (b) shows that efficient control of the weights for different smart grid applications can increase the performance of our mechanism as much as 10%. In fact, compared to the scheme without self-healing in Figure 3, finest tuning of our self-healing scheme (ω_1=2, ω_2=1.5, ω_3=1) can guarantee more than 25% performance increase. We can also see from the scenario (ω_1=2 outperforms ω_1=3) that if the weight is too high, the network becomes degraded from the self-healing mechanism being too sensitive. Therefore, it is important to designate accurate weights for different smart grid data categories, and more research will be conducted in the future for optimization of these values.

5. Conclusion

The self-managing, self-healing issues in the smart grid systems are a vital problem that needs to be solved to provide high-reliability service. Accordingly, smart grid networking systems must also provide these high-reliability functions to support realization of smart grid. We propose a self-healing network mechanism for smart grid networking systems that can adaptively adjust to the current status of the network and enforce appropriate policies. Via simulation, we have shown that our self-healing mechanism can provide higher guarantee to the overall networking system. For our future work, we will consider implementing our work on actual testbeds to evaluate the performance in more realistic scenarios.

Acknowledgements

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (2012-003573)

References

[1] K. Lim, W. Jung, Y. Ko and Y. Kim, “On the Self-Healing Smart Grid Networks for Enhancing Transmission Reliability”, Proceedings of the 2012 International Conference on Information Science and Technology, Edited by A. Stoica and J. Kang, **(2012)** April 28-30; Shanghai, China.

[2] K. Moslehi and R. Kumar, “Smart Grid - a reliability perspective”, IEEE Transactions on Smart Grid, vol. 1, Issue 1, **(2010)**, pp. 57-64.

[3] M. Kang, D. Lee and J. Koo, J. IWIT, vol. 10, **(2010)**, pp. 225.

[4] M. Lee, J Zheng, Y. Ko and D. Shrestha, “Emerging Global Standards for Wireless Mesh Technology”, IEEE Wireless Communications, vol. 13, **(2006)**, pp. 56.

[5] K. Mills, Wiley Wireless Communications and Mobile Computing, vol. 7, **(2007)**, pp. 1.

[6] J. Wang and V. Leung, Proceedings of the 3rd International Conference on Information Networking, Edited by Y. Jang, C. Toh, N. Ohta and Z. Niu, **(2011)** January 26-28; Kuala Lumpur, Malaysia.

[7] S. Choi, Y. Choi and I. Lee, IEEE Transactions on Wireless Communications. 5, 203 **(2006)**.

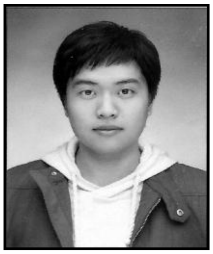
[8] C. Perkins, E. Royer, S. Das and I. Chakeres, IETF RFC 3561, **(2003)**.

[9] N. Ramanathan, K. Chang, R. Kapur, L. Girod, E. Kohler and D. Estrin, Proceedings of the 3rd ACM Conference on Embedded Networked Sensor Systems, Edited by J. Redi, **(2005)** November 2-4; San Diego, CA.

[10] T. Bourdenas and M. Sloman, Proceedings of the 8th International Conference on Pervasive Computing, Edited by A. Kruger and M. Spasojevic, Lecture Notes in Computer Science, Springer, **(2010)** May 17-20; Helsinki, Finland.

[11] D. Agrawal, S. Calo, K. Lee, J. Lobo and D. Verma, Editor IBM Press, “Policy Technologies for Self-Managing Systems”, Pearson plc, Upper Saddle River, New Jersey **(2009)**.

Authors



Keun-Woo Lim

Keun-Woo Lim received his B.A in English Literature, B.S and M.S in the School of Information and Computer Engineering at Ajou University, Korea, in 2007 and 2009 respectively. He is currently studying for his Ph. D. degree of Computer Engineering in Ajou University. His research interests are in area of Wireless mesh networks. Refer to http://uns.ajou.ac.kr/~kwlim27.

Woo-Sung Jung

Woo-Sung Jung received B.S. in electrical and computer engineering, information and computer engineering and M.S. degree from Ajou University, Korea in 2007 and 2009 respectively. He is currently studying for his Ph. D. degree of Computer Engineering in Ajou University. His research interests are in wireless networking and embedded systems.

Young-Bae Ko

Young-Bae Ko is currently a Professor in the School of Information and Computer Engineering at Ajou University, Korea, leading the Ubiquitous Networked Systems Lab. Prior to joining Ajou University in 2002, he was with the IBM T. J. Watson Research Center, New York, as a research staff member in the Department of Ubiquitous Networking and Security. He received his Ph.D. degree in computer science from Texas A&M University. His current research interests are in ad hoc/mesh networks and content centric networks. He was the recipient of a Best Paper award from ACM Mobicom 1998. He has served in various activities, most notably as general chair in IEEE SECON 2012 and as editorial board of ACM Mobile Computing and Communications Review. See http://uns.ajou.ac.kr for further details.

YoungHyun Kim

Younghyun Kim is a senior researcher at Korea Electric Power Company (KEPCO). He received the BS degree in information and telecommunication engineering from Korea Aerospace University in 2002, and the MS degree in engineering of information and communication from Gwangju Institute of Science and Technology (GIST) in 2004. His research interests include communication system design, analysis and implementation both at the physical layer and at the resource management layer for power systems.