Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 234029, 7 pages
doi:10.1155/2012/234029

Research Article

Traffic Rerouting Strategy against Jamming Attacks in WSNs for Microgrid

Yujin Lim,[1] Hak-Man Kim,[2] and Tetsuo Kinoshita[3]

[1] *Department of Information Media, University of Suwon, San 2-2 Wau-ri, Bongdam-eup, Hwaseong-si, Gyeonggi-do 445-743, Republic of Korea*
[2] *Department of Electrical Engineering, University of Incheon, 12-1, Songdo-dong, Yeonsu-gu, Incheon 406-840, Republic of Korea*
[3] *Department of Computer and Mathematical Sciences, Graduate School of Information Science, Tohoku University, Sendai 980-8577, Japan*

Correspondence should be addressed to Hak-Man Kim, hmkim@incheon.ac.kr

Received 4 November 2011; Accepted 25 February 2012

Academic Editor: Carlos Ramos

In a microgrid as an energy infrastructure, the vulnerability against jamming attacks is fatal. Thus, the ability to deal with jamming attacks and maintain an acceptable level of service degradation in presence of the attacks is needed. To solve the problem, we propose a traffic rerouting scheme in wireless communication infrastructure for islanded microgrid. We determine disjoint multiple paths as candidates of a detour path and then select the detour path among the candidates in order to reduce the effect of jamming attack and distribute traffic flows on different detour paths. Through performance comparison, we show that our scheme outperforms a conventional scheme in terms of packet delivery ratio and end-to-end delay.

1. Introduction

A microgrid is a localized grouping of electricity generation, energy storage, and loads, and it is normally connected to an upstream power grid [1–4]. However, by occurrence of fault occurrence in the power grid or by geographical isolation, a microgrid can be isolated from the power grid, and it is called an islanded microgrid [5]. Main goal of a microgrid operation is to balance the power between power supply and power demand. The severe power imbalance may happen due to power system faults and protection system malfunctions, and it may eventually lead to system collapse through a frequency instability process. Literatures [6–12] have employed a multiagent system to operate a microgrid economically and efficiently. A multiagent system is a system composed of multiple interacting intelligent agents to solve problems that are difficult or impossible for an individual agent or a monolithic system to solve [13]. It is a good solution for autonomous operation of a microgrid composed of distributed devices and systems. Figure 1 shows the islanded microgrid based on the multi-agent system. Each component has an agent, and the agent exchanges information among other agents. Especially, the agent in the microgrid operation & control center (MGOCC) gathers information about the supplied power and the load demands and operates the microgrid to balance the power.

In this paper, we consider a communication infrastructure based on the wireless sensor network (WSN) for geographically islanded microgrid operated and controlled by the multi-agent system. As an extension of the WSN, we employ a wireless mesh network (WMN) [14]. The WMN has been recently developed to provide high-quality services and applications over wireless personal area networks, wireless local area networks, and wireless metropolitan area networks [15]. The WMN has a hybrid network infrastructure with a backbone and an access network. It is operated in both ad hoc and infrastructure modes with self-configuration and self-organization capabilities. The WMN has been envisioned as the economically viable networking paradigm to build up broadband and large-scale wireless commodity networks. Installing a cabling infrastructure not only slows down implementation but also significantly increases installation cost. On the other hand, building a WMN enormously reduces the infrastructural cost because the mesh network

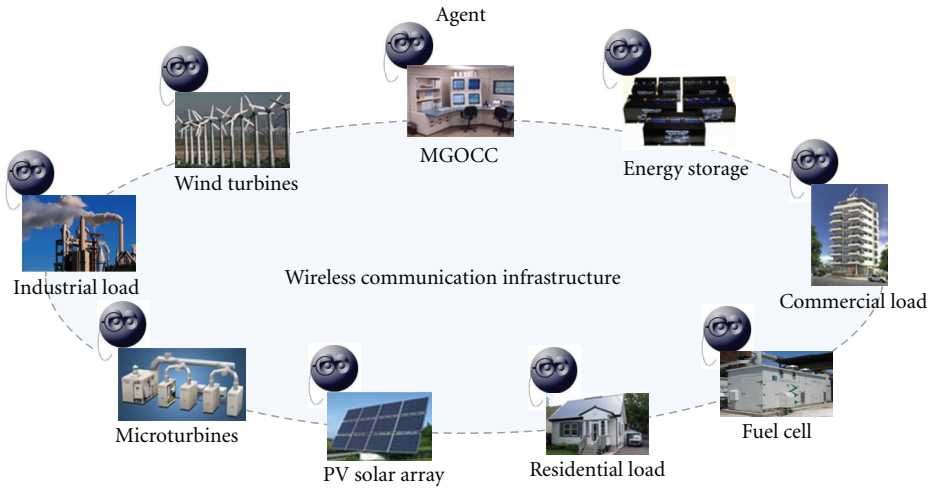

Figure 1: The islanded microgrid based on multiagent system.

needs only a few access points for connection. This reduction of network installation cost ensures rapid deployment of a metropolitan broadband network even in rural or scarcely populated urban areas. Thus, we employ the WMN to design a communication infrastructure for the islanded microgrid.

However, built upon open wireless medium, the WMN is particularly vulnerable to jamming attacks [16]. In the microgrid as an energy infrastructure, the vulnerability is a critical problem. Thus, the ability to deal with jamming attacks and to maintain an acceptable level of service degradation in presence of jamming attacks is a crucial issue in the design of the WMN. To solve the problem, traffic rerouting, channel reassignment, and scheduling schemes have been considered as jamming defense strategies. In this paper, we propose a traffic rerouting scheme in the WMN. To reduce the effect of jamming attacks, we determine multiple candidates of a detour path, and the multiple candidates are physically disjoint. Once the candidates are given, to distribute traffic flows on different detour paths, we stochastically select one candidate path as a detour path. We verify that our scheme improves the packet delivery ratio and end-to-end delay in comparison with a conventional scheme.

The remainder of this paper is structured as follows. Section 2 introduces a jamming attack and defines our WMN architecture. Section 3 explains our traffic rerouting scheme. Following this, we verify the proposed scheme by using NS-2 simulator in Section 4. Finally, Section 5 summarizes our study results.

2. System Model

2.1. Jamming Attack. Jamming represents the most serious security threat in the field of a wireless communication. Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission [17]. In the context of a wireless communication, jamming is the type of attack which interferes with the radio frequencies used by network nodes [18]. In the event that an attacker uses a rather powerful jamming source, disruptions of networks' proper function are likely to occur.

In jamming attacks, a jammer can simply disregard the medium access protocol (MAC) by continually transmitting signal on a wireless channel. By doing so, the jammer either prevents users from being able to commerce with legitimate MAC operations, or introduces packet collisions that force repeated backoffs [19]. The objective of the jammer is to interfere with legitimate wireless communications. The jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets. When the jamming occurs, the traffic going through the jammed area is disrupted, and the traffic needs to be rerouted around the jammed area.

We consider two rerouting strategies; global rerouting and local rerouting. They have tradeoffs between the rerouting latency and network performance after rerouting. In global rerouting, all traffic in the network will be rerouted. Local rerouting uses a set of detour paths to route around the jammed area locally. The local rerouting strategy can typically restore service much faster than the global rerouting because the restoration is locally activated. In this paper, we investigate the local rerouting strategies that can minimize the performance degradation in the event of jamming attacks.

Several approaches are proposed in recent works to address the jamming issue. Xu et al. [19] consider how to detect jamming where congested. They introduce the notion of consistency checking, where the packet delivery ratio is used to identify a radio link that has poor utility. Then signal strength consistency check is performed to classify whether the poor link quality is due to jamming. JAM (Jammed-Area Mapping) [20] focuses on the method to be used after jamming detection. It uses a priority message to inform neighbors of the attack detection, and it maps the jammed area as feedback for routing. However, it takes time for the routing protocol to update the information. During the time, normal traffic routed to the jamming area may become congested or dropped. Besides, a single detour path to a

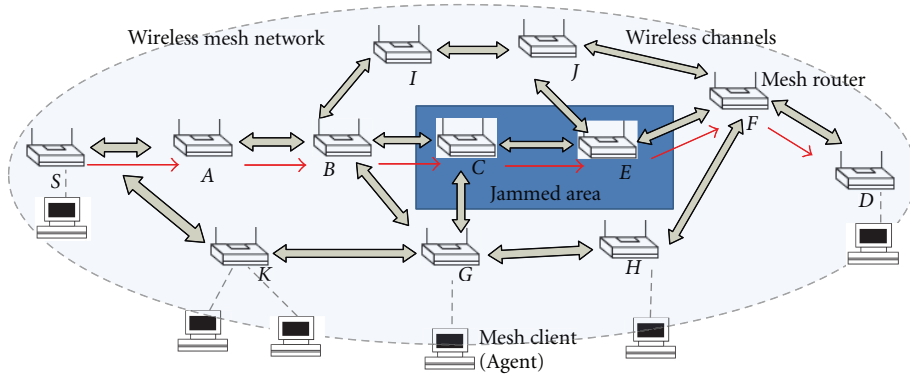

FIGURE 2: WMN system model.

destination generated by general routing protocols could easily become congested again. In this paper, we assume that the detection and mapping of jammed area are serviced by the conventional schemes [17, 20, 21]. In other words, the information of a jammed area, such as node ID in the area and locations of nodes, is fed back to nodes in the network by the service.

2.2. Architecture of WMN System. The WMN is a group of mesh clients and routers interconnected via wireless links. Mesh clients (MCs) can be various devices with wireless network interface cards such as PCs and laptops. In this paper, an agent takes a role of a MC, and hereafter we call an MC as an agent. Agents have limited communication resources and capability. Mesh routers (MRs) are usually powerful in terms of computation and communication capabilities. They normally stay static and act as access points to supply network connections for the agents. Due to limited radio coverage range and dynamic wireless channel capacity, message from an agent is usually transmitted through a multihop path to its destination. Ad hoc mode interconnections of the MRs construct the wireless mesh backbone network.

Our WMN structure is illustrated in Figure 2. On each MR, one wireless channel is assigned for communication with agents, while the other channel is assigned for communication with other MRs. When a source agent intends to send its data to a destination agent, the source agent sends the data to its neighboring MR, and the MR starts to construct a routing path towards the MR neighboring to the destination agent. Once the data arrives at the MR, neighboring to the destination and the MR forwards the data to the destination agent.

We model a multiradio multichannel WMN as a directed graph $G = (V, E, C)$, where $v \in V$ represents a WMN node (i.e., a MR) and $e \in E$ represents a wireless link between two nodes. We assume that our WMN uses a set of orthogonal wireless channels denoted by C. We consider the WMN under jamming attacks. The wireless communications of jammed nodes are interfered by RF signals or packets sent from jammers. A jammed node at channel $c \in C$ is denoted as $j_c \in J_c$, where J_c is a set of jammed nodes detected at channel c and J is the set of jammed nodes over all channels. An unjammed node is denoted as $u_c \in U_c$, where U_c is a set of unjammed nodes at channel c and U is a set of unjammed nodes over all channels where $U = V - J$. In Figure 2, nodes C and E are jammed nodes. When there is a traffic flow from source S to destination D, node B identifies that the next nodes C and E over its path are jammed by conventional jammed-area mapping services. Node B starts to discover local detour subpath to bypass the jammed area. For traffic flow f, $\text{pre}_f(J_c)$ represents a set of nodes sending data directly to one or more nodes in J_c. In Figure 2, node B is a member of $\text{pre}_f(J_c)$. The objective of our traffic rerouting scheme is to find detour path $b_f(v_{\text{pre}}, J_c)$ of flow f in the WMN, and $b_f(v_{\text{pre}}, J_c)$ is a detour path to solve the jamming problem caused by jammed nodes J_c with $v_{\text{pre}} \in \text{pre}_f(J_c)$.

3. The Proposed Traffic Rerouting Scheme

When a node $v_{\text{pre}} \in \text{pre}_f(J_c)$ detects jammed area, it constructs the detour subpath. However, if nodes to detect jamming attacks simultaneously switch to the new link, the amount of input traffic to the new link increases abruptly and congests the link. Packet loss is also increased. To solve the problem, we employ stochastic rerouting scheme to reduce the congestion and offer load balancing. In other words, a detour path is stochastically selected among multiple candidates of the detour path. To determine the candidates, we have considered multipath routing schemes in WSNs [22–28]. Our traffic rerouting scheme is composed of two steps; determining candidates of a detour subpath and selecting the detour subpath among the candidates. In this paper, we assume that all nodes in the WMN know their own location, a destination's location, and location information of the WMN system by using GPS or any localization schemes [29, 30]. In our proposed scheme, a packet sent from a source is forwarded to a destination using a conventional geographic routing scheme [31].

In the first step, we employ anchor points to construct the disjoint multiple candidates. An anchor point is a reference point to determine the next hop node over a candidate detour path. In other words, a node determines the closest node to the anchor node among its neighboring nodes as the next-hop node by using a conventional geographic routing scheme. Anchor points are divided into two groups; entry anchor points and exit anchor points. In this paper, we use k

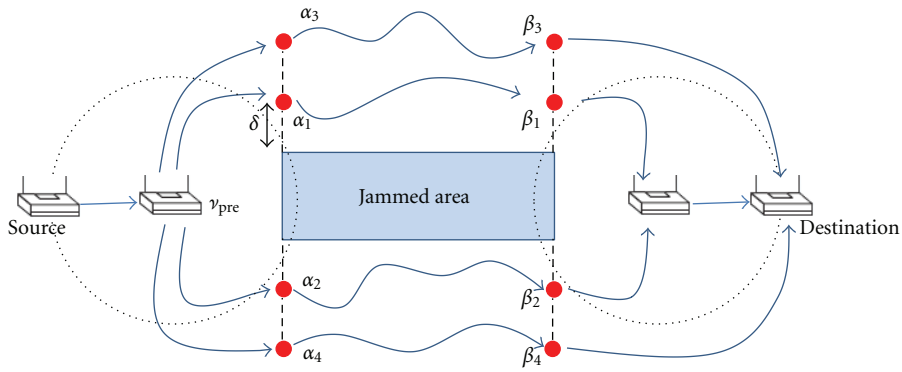

Figure 3: k multiple candidates of a detour subpath.

entry anchor points and k corresponding exit anchor points to construct k multiple candidates of the detour path. The number of candidates paths, k, is dependent on the degree of service desired by a microgrid. The separation distance between neighboring two entry points or neighboring two exit points is δ to make physically disjoint multiple candidates. As mentioned previously, jamming is the type of attack which interferes with the radio frequencies used by network nodes. Thus, in order to reduce the interference by the attack, we set δ to $R \leq \delta \leq 2R$, where R is a transmission range of a node. When v_{pre} identifies that the next node over its path is jammed, it determines entry anchor points and exit anchor points. It designates the first entry anchor point, α_1, with δ distance from the first jammed node in the jammed area. Then other entry anchor points, α_i $(1 < i \leq k)$, are designated with δ distance from the previous entry anchor point, α_{i-1}. Similarly, v_{pre} designates exit anchor points, β_1, with δ distance from the last jammed node in the jammed area. Other exit anchor points, β_i $(1 < i \leq k)$, are designated with δ distance from the previous exit anchor point, β_{i-1}. Once anchor points are determined, a 3-tuple $< v_{pre}, \alpha_i, \beta_i >$ is a candidate of the detour path. Figure 3 shows k disjoint multiple candidates.

Once k candidates of the detour subpath are determined, the second step of our traffic rerouting scheme is initiated to select the detour subpath among the candidates. When the candidates are determined, v_{pre} stochastically selects the detour path. The next nodes of v_{pre} over multiple candidates are ordered by link qualities of the next nodes, such as RSS (received signal strength), LQI (link quality indication), or SNR (signal-to-noise ratio). The link qualities of the next nodes are transformed into a value between 0 and 1 using the min-max normalization. Then, v_{pre} selects its next node with probability p, and the corresponding candidate is selected as the detour subpath.

When the detour path is selected, v_{pre} sends the data received from the source to the entry anchor point in the selected 3-tuple by using a conventional geographic routing scheme. When an intermediate node is in R range of the entry anchor point the node declares itself as an entry anchor node for the entry anchor point, and it sends the message to the corresponding exit anchor point. An exit anchor node is selected in similar way. In other words, when an intermediate node is in R range of the exit anchor point, the node declares itself as an exit anchor node for the exit anchor point, and it sends the data to the destination node. The traffic rerouting is completed.

4. Performance Evaluations and Discussions

To quantitatively evaluate the performance of the proposed scheme, we use NS-2 network simulator [32]. Our WMN delivers the microgrid-related data between agents. In a 1500 m by 1500 m grid, we deploy 30 MCs, that is, agents and 70 MRs. The MCs are randomly placed and MRs are equally spaced. MCs exchange 1024-byte CBR packets with other randomly selected MCs through MRs every second. As comparative routing mechanism, JAM [20] with a detour path is simulated. As performance metrics, PDR (Packet Delivery Ratio) and end-to-end delay of normal traffic are measured. PDR is the ratio of total number of packets received by the nodes to the total number of packets transmitted. End-to-end delay is the time taken for a packet to be transmitted across a network from source to destination. For the simulation parameters, we vary the number of normal flows and the number of nodes within the jammed area. The jammed area is located at the center of network; thus generated normal traffic would be destined for the jammed area in normal routing. In our experiments, the transmission range of a node is defined as 250 m, and two-ray ground propagation channel is assumed with a data rate of 54 Mbps. We used IEEE 802.11 g MAC, and the total simulation time is 3600 seconds. In figures, k indicates the number of candidates subpath in our scheme ("*PS*") and "*normal*" indicates that the network has no jamming traffic.

Figures 4 and 5 show PDR and end-to-end delay when the number of normal flows increases. The number of nodes in the jammed area is set to 4. JAM provides a high PDR until the number of normal flows is 5, but PDR decreases in the case with a lot of normal traffic, and this induces a high end-to-end delay. Since JAM selects the best single path to detour the jammed area, the selected path easily becomes congested when the number of normal flows increases. In comparison with JAM, our scheme increases PDR by about 10% and decreases the end-to-end delay by about 80% because of the stochastical traffic distribution among

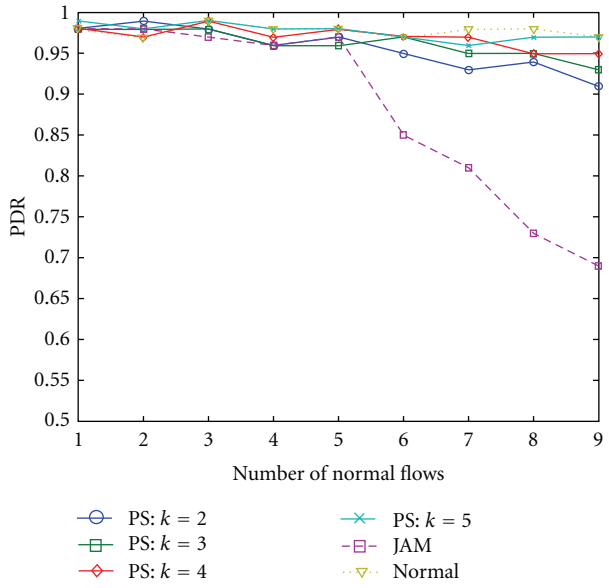

Figure 4: Performance comparison of PDR with varying the number of normal flows.

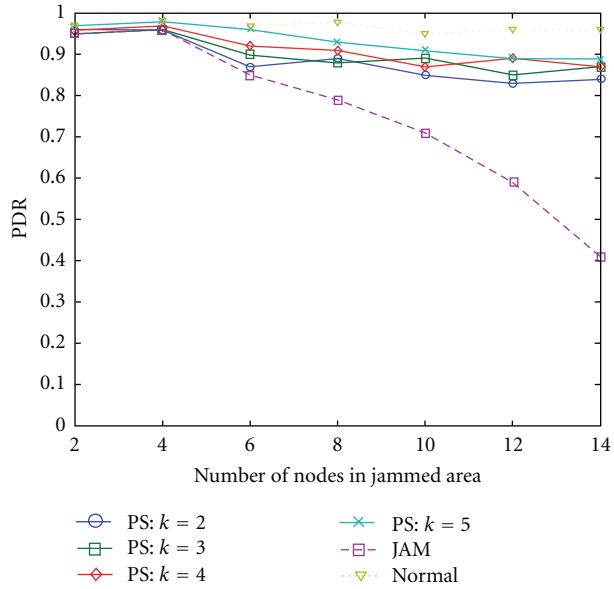

Figure 6: Performance comparison of PDR with varying the number of nodes in jammed area.

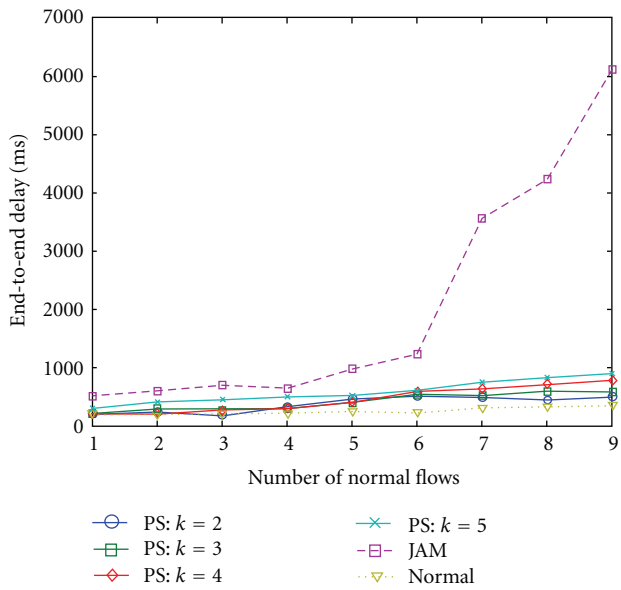

Figure 5: Performance comparison of the end-to-end delay with varying the number of normal flows.

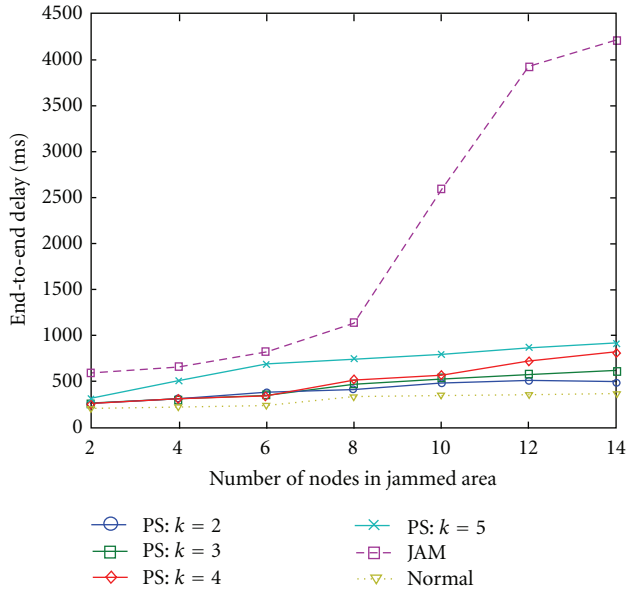

Figure 7: Performance comparison of the end-to-end delay with varying the number of nodes in jammed area.

multiple candidates. In our scheme, when k increases, the distance between the candidate path and the jammed area increases and the effect of the jamming attack decreases. Thus, PDR increases. However, when the distance increases, the length of the candidate subpath increases and the delay also increases.

Figures 6 and 7 show PDR and end-to-end delay when the number of nodes in the jammed area increases. The number of normal flows is set to 4. PDR and the end-to-end delay of JAM are worsened drastically in the big jammed area because of traffic concentration on a long detour path. However, our scheme stochastically distributes normal flows on disjoint multiple paths and efficiently balances the traffic load. Thus, we can see that our scheme achieves an improvement of about 20% and 75% in PDR and the end-to-end delay, respectively. For our scheme, we carried

out additional experiments to address a scalability problem. From the results, we can conclude that our scheme is scalable when the number of nodes increases from 2 to 50. For example, PDR and end-to-end delay are 78% and 1.42 sec, respectively, when the number of nodes is 50.

5. Conclusion

In this paper, we focused a traffic rerouting scheme under jamming attacks in wireless communication infrastructure for islanded microgrid. In conventional schemes, when nodes detect jamming attacks, they simultaneously switch to a new link, and the amount of input traffic to the new link increases abruptly and congests the link. To solve the problem, we employ a stochastic rerouting scheme to reduce the congestion and offer load balancing. First, we determine physically disjoint multiple paths as the candidates of a detour path to reduce the effect of jamming attack. Then, we stochastically select the detour path among the multiple candidates to offer load balancing. From the performance comparison, we show that the performance of our scheme is better than that of conventional scheme in terms of the packet delivery ratio and the end-to-end delay.

In our scheme, one of the factors affecting the performance is the distance δ. To optimize the performance, we need a dynamic decision scheme of δ in time-varying environments. We will consider developing the decision scheme as a future research direction.

Acknowledgment

This work was supported by the GRRC program of Gyeonggi province ((GRRC SUWON2011-B4), Research on Precision Location Tracking System for Real-Time Situation).

References

[1] B. Lasseter, "Role of distributed generation in reinforcing the critical electric power infrastructure," in *IEEE Power Engineering Society Winter Meeting*, pp. 146–149, February 2001.

[2] J. Y. Kim, S. K. Kim, and J. H. Park, "Contribution of an energy storage system for stabilizing a microgrid during islanded operation," *Journal of Electrical Engineering and Technology*, vol. 4, no. 2, pp. 194–200, 2009.

[3] J. Y. Kim, J. H. Jeon, S. K. Kim et al., "Cooperative control strategy of energy storage system and microsources for stabilizing the microgrid during islanded operation," *IEEE Transactions on Power Electronics*, vol. 25, no. 12, pp. 3037–3048, 2010.

[4] J. H. Jeon, J. Y. Kim, H. M. Kim et al., "Development of hardware in-the-loop simulation system for testing operation and control functions of microgrid," *IEEE Transactions on Power Electronics*, vol. 25, no. 12, pp. 2919–2929, 2010.

[5] H. M. Kim and T. Kinoshita, "A new challenge of microgrid operation," *Communications in Computer and Information Science*, vol. 78, pp. 250–260, 2010.

[6] A. L. Dimeas and N. D. Hatziargyriou, "Operation of a multiagent system for microgrid control," *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1447–1455, 2005.

[7] A. L. Dimeas and N. D. Hatziargyriou, "Agent based control for microgrids," in *IEEE Power Energy Society General Meeting*, June 2007.

[8] H. M. Kim, T. Kinoshita, Y. Lim, and T. H. Kim, "A bankruptcy problem approach to load-shedding in multiagent-based microgrid operation," *Sensors*, vol. 10, no. 10, pp. 8888–8898, 2010.

[9] H. M. Kimt and T. Kinoshita, "A multiagent system for microgrid operation in the grid-interconnected mode," *Journal of Electrical Engineering and Technology*, vol. 5, no. 2, pp. 246–254, 2010.

[10] H. M. Kim, T. Kinoshita, and M. C. Shin, "A multiagent system for autonomous operation of islanded microgrids based on a power market environment," *Energies*, vol. 3, no. 12, pp. 1972–1990, 2010.

[11] H. M. Kim, T. Kinoshita, and Y. Lim, "Talmudic approach to load shedding of islanded microgrid operation based on multiagent system," *Journal of Electrical Engineering and Technology*, vol. 6, no. 2, pp. 284–292, 2011.

[12] H.-M. Kim, W. Wei, and T. Kinoshita, "A new modified CNP for autonomous microgrid operation based on multiagent system," *KIEE Journal of Electrical Engineering & Technology*, vol. 6, pp. 139–146, 2011.

[13] M. Wooldridge, *An Introduction to Multiagent Systems*, John Wiley and Sons, New York, NY, USA, 2nd edition, 2009.

[14] OpenSG, "SG Network System Requirements Specification r3," May 2010.

[15] F. Huang, Y. Yang, and L. He, "A flow-based network monitoring framework for wireless mesh networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 48–55, 2007.

[16] S. Jiang and Y. Xue, "Providing survivability against jamming attack for multi-radio multi-channel wireless mesh networks," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 443–454, 2011.

[17] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.

[18] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 38–43, 2004.

[19] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '05)*, pp. 46–57, May 2005.

[20] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: a jammed-area mapping service for sensor networks," in *24th IEEE International Real-Time Systems Symposium (RTSS '03)*, pp. 286–297, December 2003.

[21] R. Muraleedharan and L. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using ant system," in *SPIE Symposium on Defense and Security*, Orlando, Fla, USA, April 2006.

[22] H. W. Oh, J. H. Jang, K. D. Moon, S. Park, E. Lee, and S. H. Kim, "An explicit disjoint multipath algorithm for cost efficiency in wireless sensor networks," in *21st International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC '10)*, pp. 1899–1904, September 2010.

[23] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," *ACM Mobile Computing and Communications Review*, vol. 1, pp. 10–24, 2002.

[24] E. P. C. Jones, M. Karsten, and P. A. S. Ward, "Multipath load balancing in multi-hop wireless networks," in *IEEE*

International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '05), pp. 158–166, August 2005.

[25] S. Waharte and R. Boutaba, "Totally disjoint multipath routing in multihop wireless networks," in *IEEE International Conference on Communications (ICC '06)*, pp. 5576–5581, July 2006.

[26] E. Gelenbe and E. C. H. Ngai, "Adaptive qos routing for significant events in wireless sensor networks," in *5th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS '08)*, pp. 410–415, October 2008.

[27] E. Gelenbe and E. C.-H. Ngai, "Adaptive random re-routing for differentiated QoS in sensor networks," in *Proceedings of the Visions of Computer Science Conference*, pp. 343–354, September 2008.

[28] E. Gelenbe and E. C.-H. Ngai, "Adaptive random re-routing in sensor networks," in *Annual Conference of ITA (ACITA '08)*, pp. 348–349, London, UK, September 2008.

[29] A. Islam, U. Iqbal, J. M. P. Langlois, and A. Noureldin, "Implementation methodology of embedded land vehicle positioning using an integrated gps and multi sensor system," *Integrated Computer-aided Engineering*, vol. 17, no. 1, pp. 69–83, 2010.

[30] F. G. Bravo, A. Vale, and M. I. Ribeiro, "Navigation strategies for cooperative localization based on a particle-filter approach," *Integrated Computer-aided Engineering*, vol. 14, no. 3, pp. 263–279, 2007.

[31] B. Karp and H. T. Kung, "Gpsr: greedy perimeter stateless routing for wireless networks," in *6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 243–254, August 2000.

[32] "The network Simulator ns-2," http://www.isi.edu/nsnam/ns/.