A Secure Spectrum-Aware Routing Scheme by Detecting Black Hole Attacks for Smart Grid Applications

Azadeh Jafarinezhad and Mohsen Dorsetan
Electrical Engineering Department, Imam Reza International University, Mashhad, Iran
Email: {azd.jfrn, mohsen.dorsetan}@gmail.com

Sayyed Majid Mazinani
Iranian Construction Engineering Organization Province of Khorasan Razavi, Mashhad, Iran
Email: smajid.mazinani@gmail.com

Masoud Shirkhani
Electrical Engineering Department, Ilam Science and research Islamic Azad University, Ilam, Iran
Email: masoud.shirkhani@gmail.com

***Abstract*—Recently, cognitive sensor network (CSN) emerges as a key technology to enhance spectrum efficiency of wireless sensor network (WSN) and thus creates opportunistic transmissions over links. Dynamic and opportunistic spectrum access capabilities of CSN can be benefited to address many of the unique requirements and challenges of smart grid for WSN. The migration of power grids from an isolated network to a public communication network has created many challenging issues in the security of smart grids and one of the major challenges of CSN face today is security. This paper proposes a secure spectrum-aware routing scheme, which considers black hole attacks in smart grid communication structure and also considers traffic balance, route configuration and power control for reliable routing. We propose a mechanism to detect black hole attacks and also a method is employed to combine the routing objectives into a single target function. Randomized route selection strategy is adopted for traffic balance. The simulation results demonstrate that the proposed scheme improves the communication reliability and packet delivery rate in smart grid.**

***Index Terms*—black hole attack, cognitive sensor network, security, smart grid, spectrum aware routing**

I. Introduction

Current electrical power grid for improving future demand growth is being reconstructed [1]. It has many issues which must be resolved, including more voltage sags, blackouts, overloads, increased population size and finally, the current electrical network contributes greatly to carbon emissions [2]. As noticed in [3], there are two driving forces to move toward Smart Grid (SG): (1) the aging, inadequate, and outdated current electricity grid which needs to be improved to meet the future demand challenges, (2) the benefits of the SG in consequence of the improvements in six key value areas: reliability, economics, efficiency, environmental, security, and safety. The essential concept of the smart grid is the integration of advanced information technology, digital communications, sensing, and measurement and control technologies into the power system in order to achieve its benefits [4]. The major difference between telecommunication networks and the electric grid is that communication networks route packets of information, while the electric grid routes power flows [5]. One of the issues that must be considered in the smart grid is routing capability to all network endpoints device for a wide range of applications with different requirements.

Reliable and efficient management of smart grid can be accomplished with the installation of wireless sensor nodes on critical power grid equipment [6]. Obtained information from sensors can be used to diagnose arising problems rapidly, and hence, autonomous and reliable operation can be achieved in smart grid. However, the realization of smart grid literally depends on the communication capabilities of sensor networks in harsh and complex electricity network environments that bring out great challenges for reliability and energy efficiency in WSN. To this end, the dynamic and opportunistic spectrum access capabilities of cognitive radio can be benefited to address many of the unique requirements and challenges of smart grid for WSN [7]. Spectrum-aware and cognitive sensor nodes in smart have many promising advantages.

Security is also another critical component of SG and has to be considered in communication structure. Security includes the protection from unauthorized accesses and malicious attacks. It also covers the protection of compromised control units from harming the system. Joint design of security and routing together is needed for better efficiency. Routing data through the public SG communications network is considered one of the weakest

Manuscript received June 29, 2014; revised December 24, 2014.

doi: 10.12720/ijoee.2.4.337-342

points in the system and significant work is required in order to overcome this vulnerability [5]. Security aspects have not yet been fully explored for CSN. The security paradigms are often inherited from WSN and do not fit with the specifications of CR networks. Security researchers have seen that CR has special characteristics. This make CR security an interesting research field, since more chances are given to attackers by CR technology compared to general wireless networks [8].

In this paper, we propose a secure spectrum-aware routing scheme that detect black hole attacks in smart grid environment and simultaneously consider delay, energy efficiency and reliability. In Section II, we explain node and network model and also describe the attack. In Section III, we establish a secure spectrum-aware routing framework for local household data to reach a super data concentrator. In Section IV, we analyze our simulation data and finally we conclude in Section V with future work and challenges.

II. Network and Node Model

A. Network Model

SG has a hierarchical structure that is built upon the current hierarchical power grid architecture. The end-users, such as households, communicate their power usage and pricing data with a local area substation which collects and processes data from smart meters. In SG, the path for the measurement data may not be predetermined. The data can be relayed from smaller scale data concentrators to some super data concentrators (SDCs). Here we consider a self-organized CSN in a planar architecture as it shown in Fig. 1. There is a data center (i.e. data concentrator) in the network, which is responsible for network management. The data center is the destination of all packets.

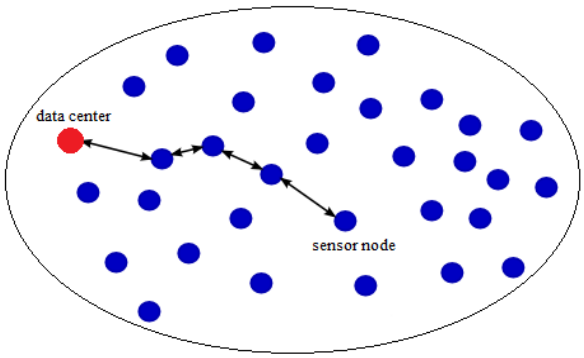

Figure 1. Network model.

B. Node Model

We consider two node types: (1) Primary Users (PUs, i.e. licensed users); (2) Secondary Users (SUs, i.e. unlicensed users and they are cognitive sensor node). Each SU (i.e., cognitive sensor node) periodically senses the channels and acquires the number of in-use PU channels *i* and in-use SU channels *j*. The parametric pair *(i, j)* is used to characterize the channel availability, and called Channel Usage Information (CUI). The total channel number of SUs is N. PUs and SUs are allowed to be mobile or quasi-static (i.e., moving slowly) in the network.

C. Interference Model

We should consider an interference model for transmitting data in SUs and PUs nodes. We have two region of interference, one region is for SUs transmitting data. In this region SUs may compete for spectrum resource, if one SU lies in the interference radii of two other SUs. In the other region SU is not allowed to use the channels occupied by PUs located within distance a constant distance that is defined by receiver interference threshold. This is shown in Fig. 2.

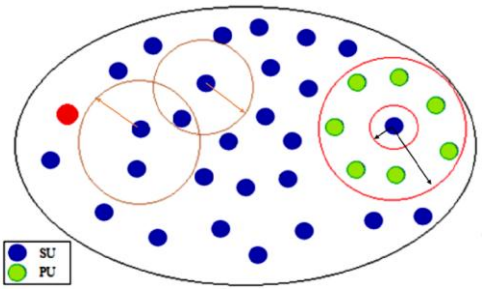

Figure 2. Interference model: for PU to SU and for SUs.

D. Attack Model

Here we consider a black hole attack. With the introduction of advanced metering and pricing capabilities, the reliability of the communication link between a consumer and the utilities becomes a prime concern. Consequently, a denial of service (DoS) attack geared towards the smart grid communication network poses a huge threat. DoS attacks can generally be classified into two distinct categories, i.e., protocol compliant and non-compliant attacks. While detection of the non-compliant attacks such as jamming is still a challenging task, attacks which comply with the protocol operation are more difficult to detect and counter. Black hole attack is one of the most popular protocol compliant DoS attacks. In such an attack, malicious users not only impersonate legitimate users but also pose as the nodes that will maximize the network utility. Both the spatial scale and the broadcast nature of the information dissemination (such as pricing information) further elevate the relevance of the black hole attack to smart grid communication. An accurate quantification of the impact of the black hole attack is an important step towards a secure design of smart grid communication network [9]. We consider two different mechanisms for packet dropping attacks employed by the malicious users to deteriorate the legitimate user utility (will be defined later in Section).

III. Secure Spectrum-Aware Routing Scheme

A. Routing Framework

The number of neighboring PUs and surrounding SU flows provides crucial information for decision-making in the spectrum-aware routing. The routing scheme has the following phases.

- SUs broadcast their channel usage information for neighbor nodes, so each node is aware of in use spectrum PUs and SUs number.

- Source node checks CUI and number of hopes to the sink node.
- According to the CUI and consider the secure route (no black hole attack exist), the source node performs route configuration. In addition, a target function is explained that consider energy efficiency, delay and reliability.
- Whenever a black hole attack route was detected and the channel CUI is changed route to be updated.

B. Routing Objectives

Spectrum-aware routing aims at by considering black hole attack selecting the optimal route according to the available spectrum resource and optimize the QoS issues including reliability, energy efficiency and path delay, which are discussed as follows.

- Security

We consider two different mechanisms for black hole attacks. In the first mechanism, we assume that the malicious node place near the source node, therefore it can destroy more data. To deal with black hole attacks, when the destination node receives route reply, the source node must perform following assessments.

First in each path that the number of its hop is less than or equal 2 consider as malicious node. To ensure that malicious node is a real black hole attack, we send a test packet. If we don't receive confirm packet consider it as an attacker, this mechanism is shown in Fig. 3.

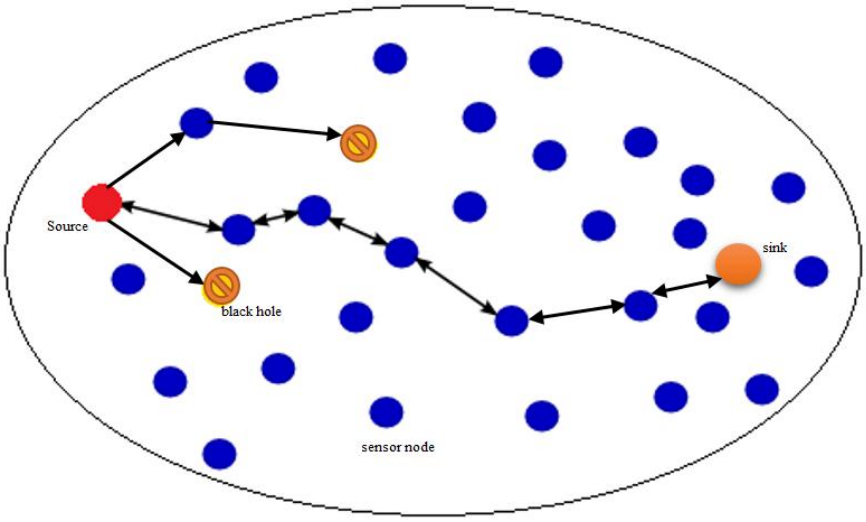

Figure 3. Black-Hole attack in routing scheme.

The second method to detect attack is a time-based mechanism. Malicious node always responds quickly to route reply and operating node doesn't have correct information about their distance to the sink node, thus they respond to these malicious nodes quickly. To avoid this, we calculate round trip time of all nodes so correct time between source and destination nodes are identified then the right decision is made to send data. To this end, after obtaining all round trip time (RTT) we calculate their average. A path has closer value to the average value is considered as a secure path.

- Reliability

A reliable routing means ability of providing reliable end-to-end communications regardless the variation of the PU activities. This means that the routing scheme is insensitive to the variation of the number available channels. Reliability is important because the main challenge in cognitive radio networks is the unpredictability of the PUs activities. CUI is an effective metric to reflect the reliability of the route. It is obvious that the larger the value of *(N−i−j)*, the better the reliability. Thus, we represent the one-hop reliability as

$$r_h = N - i - j \tag{1}$$

- Delay

The end-to-end delay equals to the sum of the delay along all hops. Let d_h denote the one-hop link delay. Let d_f and d_t denote the forwarding delay and transmission delay, respectively. The link delay can be written as

$$d_h = d_f + d_t \tag{2}$$

Generally, the transmission latency d_t is small enough that it can be neglected. Meanwhile, because each sensor node has the same processing capability, the forwarding delay is almost the same to different sensor nodes. Let d_p and n_h denote the entire path delay and the number of hops in the path, respectively. The path delay is given by $d_p = d_f \cdot n_h$, where the forwarding delay d_f is treated as a constant.

- Energy consumption

When power control is adopted, the energy consumption is related to the link distance. We consider a path of U hops. Let e_p denote the energy consumption of the entire path, and e_h the energy consumption of the h-th hop. Then we have $e_p = \sum_{h=1}^{U} e_h$. Note that, if the link distance of the h-th hop is l_h, the energy consumption of the h-th hop is represented by

$$e_h = c_1 l_h^a + c_2 \tag{3}$$

where c_1 and c_2 are constants that are determined according to the actual energy mode.

C. Formulate Routing Objectives

To achieve the above multiple objectives, we formulate the problem to a target function using the methodology of Multiple Attribution Decision Making (MADM) [10]. Without loss of generality, we consider the scenario as shown in Fig. 4, where there are three candidate routes between the source node and the destination node. The source node S is going to select the relays from the three candidate routes. The performance issues like reliability, end-to-end delay and energy consumption are taken into account. Let *g(r, d, e)* denote the total target function, called score, to numerically evaluate the total performance of a route, where r, d and e represent the metrics of reliability, end-to-end delay and energy consumption, respectively. From the point of view of MADM, the target of route selection is to find the route which has the highest score. To define the form of the target function *g( )*, we consider the score with respect to different attributes. The decision-making characteristic matrix can be written as

$$Y = (y_{m,k})_{3\times 3} = \begin{bmatrix} y_{11} & y_{12} & y_{13} \\ y_{21} & y_{22} & y_{23} \\ y_{31} & y_{32} & y_{33} \end{bmatrix} \quad (4)$$

We must normalize scores, after normalization of matrix we have:

$$Z = (z_{m,k})_{3\times 3} = \begin{bmatrix} z_{11} & z_{12} & z_{13} \\ z_{21} & z_{22} & z_{23} \\ z_{31} & z_{32} & z_{33} \end{bmatrix} \quad (5)$$

Using Entropy weighting method [10], we can obtain the weight coefficient of each attribute. Let

$$p_{m,k} = \frac{z_{m,k}}{\sum_{m\in M} z_{m,k}}, m \in M, k = R \quad (6)$$

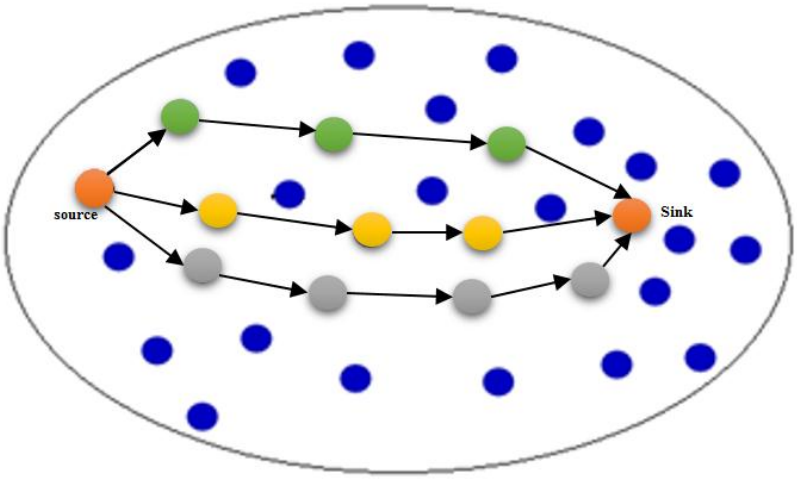

Figure 4. Routing scenario after detecting black-hole nodes.

Let *M* denote the size of *M*. The entropy of the *k-th* attribute is represented by

$$\xi_k = -\frac{1}{\ln M}\sum_{m=1}^{M} p_{m,k} \ln p_{m,k} \quad (7)$$

If $p_{m,k}=0$, let $p_{m,k}1np_{m,k}=0$. Let w_k denote the weight of the *k-th* attribute, which is given by

$$w_k = \frac{1-\xi_k}{\sum_{l\in k}(1-\xi_l)}, w_k \succ 0, k \in R \quad (8)$$

Note that, we have $\sum_{k\in R^{wk}} = 1$. Finally, the optimized route is obtained by

$$m^* = \arg\max_{m\in M} \sum_{k\in R} w_k z_{m,k} \quad (9)$$

D. Randomized Route Selection

If we always select routes according to the objectives described above, the SU flows will tend to go through the area where there is fewer PUs and SUs, which may lead to overuse of some specific nodes, and more severely, cause traffic congestion. Therefore, traffic balance should be taken into account. We solve this by randomizing the route selection.

IV. Simulation Result

In this section, we evaluate the proposed routing scheme in the NS2 network simulator. In the simulation, we consider a square field with area 1000×1000 m^2. PU and SU nodes are uniformly deployed at random in the region. Our node are considered to be smart meter, mobile enforces, vehicle and etc. in smart grid. PUs and SUs are movable following the Random Waypoint model with speeds 10 and 1m/s, respectively. The arrival and departure rates of PU services are 0.1 and 0.5m/s, respectively. The parameters in interference model the PU interference radius is 30 m, SU interference radius is 10 m. The number of wireless channels N = 13. The parameters in energy model c_1 = 1.5×106, c_2 = 1.2×103 and α = 3.

For comparison, we consider the SP-power [11] routing scheme, which applies Dijkstra's single source shortest weighted path algorithm to optimize the power cost and

SP-MADM scheme [12]. As shown in Fig. 5, the proposed spectrum aware routing scheme (labeled by Secure-MADM) clearly outperforms the other two schemes in packet loss. More specifically, the enhancement of reliability is better than two other so we configure a high security path. Besides the results in Fig. 5, we also observe that the loss of optimality in energy efficiency compared to SP-power and SP-MADM over time, and the loss of optimality in path delay because we are not force to retransmit lost packet in network. All these results indicate that the proposed scheme is able to find out the end-to-end secure routes while those routes are also with satisfying performance in reliability, energy efficiency and delay.

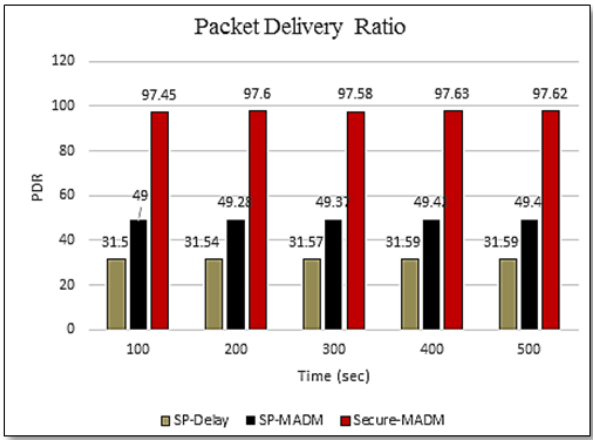

Figure 5. Performance comparison.

V. Conclusion

In this paper, we developed a secure spectrum-aware routing framework to quantify end-to-end performance of a smart grid communication network. The proposed framework is adopted to detect the black hole attackers. It is shown the difference between end-to-end packet delivery ratio in the presence and absence of attacker in comparison with two others algorithm. Two mechanism of attacks are considered, i.e., black hole attack near source node and time-based mechanism. Our results also indicate that in the presence of malicious users there exists high packet loss for the smart grid communication link. Importantly, we consider security in smart grid communication networks as an important issue. Secure routing is a pivotal problem in smart grids as the power infrastructure is migrating to new communication technologies.

In addition to security issue in smart grid, we jointly consider reliability, energy efficiency, and path delay. Firstly, the conditions of spectrum usage of PUs and SUs are obtained by sensing channels and send its data to neighbor nodes. Secondly, the method of MADM is employed to combine the metrics of reliability, energy consumption and path delay. The simulation results demonstrate that the proposed scheme achieves better performance while having satisfying performances in energy consumption, reliability, packet loss and path delay. Future work will be aimed at the implementation of the routing algorithm on a small test-bed as well as the study of a more refined and more comprehensive security metric that incorporates potential threats and attacks in cognitive sensor networks for smart grid.

References

[1] U.S. NIST. (Jan. 2010). NIST framework and roadmap for smart grid interoperability standards, release 1.0. *NIST Special Publication 1108* [Online]. Available: http://www.smartgrid.gov/standards/roadmap.

[2] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. L. P. Chen, "A survey of communication/networking in smart grids," *Future Generation Computer Systems*, vol. 28, no. 2, pp. 391-404, Feb. 2012.

[3] S. Lohani, "Communication network analysis in smart grid," Student Thesis, School of Computer Sciene, Phisics and Mathematics, 2012.

[4] G. Arnold, "Challenges and opportunities in smart grid: A position article," *Proceeding of the IEEE*, vol. 99, no. 6, pp. 922-927, Jun. 2011.

[5] A. Sabbah, A. El Mougy, and M. Ibnkahla, "A survey of networking challenges and routing protocols in smart grids," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 210-221, 2014.

[6] Y. Yang, D. Divan, R. G. Harley, and T. G. Habetler, "Power line sensornet—A new concept for power grid monitoring," in *Proc. IEEE Power Eng. Soc. Gen. Meeting*, Jun. 2006, pp. 1-8.

[7] A. Bicen, O. Akan, and V. Gungor, "Spectrum-Aware and cognitive sensor networks for smart grid applications," *IEEE Communications Magazine*, vol. 50, pp. 158-165, May 2012.

[8] A. Araujo, J. Blesa, E. Romero, and D. Villanueva, "Security in cognitive wireless sensor networks, challenges and open problems," *EURASIP Journal on Wireless Communications and Networking*, vol. 48, pp. 1-8, Feb. 2012.

[9] S. A R. Zaidi and M. Ghogho, "Stochastic geometric analysis of black hole attack on smart grid communication networks," presented at 2012 IEEE Third International Conference on Smart Grid Communications, Tainan, Nov. 5-8, 2012.

[10] C. L. Hwang and K. Yoon, *Multiple Attribute Decision Making: Methods and Applications*, Berlin/Heidelberg/New-York: Springer Verlag, 1981.

[11] I. Stojmenovic and X. Lin, "Power-Aware localized routing in wireless networks," *IEEE Trans. Parallel Dist. Sys.*, vol. 12, no. 11, pp. 22-33, 2001.

[12] R. Yu, Y. Zhang, W. Yao, L. Song, and S. Xie, "Spectrum-Aware routing for reliable end-to-end communications in cognitive sensor network," presented at 2010 IEEE Global Telecommunications Conference, Miami, FL, Dec. 6-10, 2010.

Azadeh Jafarinezhad was born in Shiraz, Fars, Iran on 5 May 1987. She received the B.S. degree in Communication Electrical Engineering from Fars Science and Research Azad University of Fars, Iran in 2012. She is M.S. in telecommunication engineering in Imam Reza International University, Mashhad, Iran. Her research interests include Computer Networks, Wireless Sensor Networks, Cognitive Radio, Cognitive Sensor Network and Smart Grids.

Mohsen Dorsetan was born in Fouman, Gilan, Iran on 19 October 1987. He received the B.S. degree in Electrical Engineering from Lahijan Azad University of Lahijan, Iran in 2011. He is M.S. in telecommunication engineering in Imam Reza International University, Mashhad, Iran. His research interests include Computer Networks, Wireless Sensor Networks, Smart Grids and Image Processing

Sayyed Majid Mazinani was born in Mashhad, Iran on 28 January 1971. He received his Bachelor degree in Electronics from Ferdowsi University, Mashhad, Iran in 1994 and his Master degree in Remote Sensing and Image Processing from Tarbiat Modarres University, Tehran, Iran in 1997. He worked in IRIB from 1999 to 2004. He also received his phD in Wireless Sensor Networks from Ferdowsi University, Mashhad, Iran in 2009. He is currently assistant professor at the faculty of Engineering in Imam Reza International University, Mashhad, Iran. He was the head of Department of Electrical and Computer Engineering from 2009 to 2012. His research interests include Computer Networks, Wireless Sensor Networks and Smart Grids.

Masoud Shirkhani was born in Ilam, Iran on 29 November 1987. He received the B.S. degree in Electrical Engineering from Sepahan University of Isfahan, Iran in 2012. He is M.S. in Power electrical engineering student in Ilam Science and Research Islamic Azad University, Iran. His research interests include Smart Grid, Renewable Energy and Micro Grids.