Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 720416, 7 pages
http://dx.doi.org/10.1155/2013/720416

Research Article

A Distributed Intrusion Detection Scheme about Communication Optimization in Smart Grid

Yunfa Li and Qili Zhou

School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China

Correspondence should be addressed to Yunfa Li; yunfali@hust.edu.cn

Received 1 September 2013; Accepted 26 November 2013

Academic Editor: Yuxin Mao

We first propose an efficient communication optimization algorithm in smart grid. Based on the optimization algorithm, we propose an intrusion detection algorithm to detect malicious data and possible cyberattacks. In this scheme, each node acts independently when it processes communication flows or cybersecurity threats. And neither special hardware nor nodes cooperation is needed. In order to justify the feasibility and the availability of this scheme, a series of experiments have been done. The results show that it is feasible and efficient to detect malicious data and possible cyberattacks with less computation and communication cost.

1. Introduction

Smart grid, which is composed of some sensors, digital smart meters, and digital controls, can efficiently and intelligently manage energy supply and consumption. Based on this characteristic, each consumer or energy supplier can monitor and control two-way energy flow. And each consumer or energy supplier can real time manage energy supply and consumption by using smart gird. In fact, the factor that each consumer or energy supplier can monitor and manage energy supply and consumption is that it can get the information of energy supply and consumption by using some management and communication tools in smart grid. In general, a smart grid communication network includes home area network (HAN), neighborhood area network (NAN), and wide area network (WAN). NAN is a network of multiple HANs to deliver metering data to the data concentrator and deliver control date to corresponding HANs. WAN is the largest network for communication to/from data center. In a HAN, each appliance (such as electricity, gas, water, heat, solar panels, etc.) is equipped with a smart meter. And these smart meters connect corresponding smart appliances. Finally, these meters connect a metering gateway. In a NAN, many metering gateways of different home areas connect each other to form a possible wireless mesh network. A WAN connects smart metering gateways with utility and the distribution control system.

Based on the description above, we can find that the smart grid is a hybrid of the power system and the communication network. Therefore, there are a lot of security problems which need people to resolve. These problems include unauthorized smart metering data access, distributed turning off of all devices by an attacker, smart metering data repudiation, stealing power without notice, and attacking the infrastructure of smart grid to cause power outage. Although there are a lot of traditional computer network security mechanisms and methods which can be used in a smart grid, these mechanisms and methods do not take into account the real-time nature of the smart grid and lack of the risk management function when the smart grid is attacked. As a matter of fact, these traditional security mechanisms and methods do not meet the security requirement of smart grid.

Based on the security requirement of smart grid, we will propose an optimization routing algorithm of communication and build an intrusion detection scheme for smart grid in this paper. In the scheme, we will integrate a lot of cybersecurity into the communication of smart grid. This paper is organized as follows. In the next section, we review some related work. In Section 3, we first propose an efficient communication optimization algorithm. Then, we present

an intrusion detection algorithm for smart grid. The two part algorithms compose a distributed intrusion detection scheme about communication optimization in smart grid. In Section 4, we describe a series of experiments and analyze the results of experiments in detail. The time complexity of this distributed intrusion detection scheme is analyzed in Section 5. Finally, the conclusions are drawn in Section 6.

2. Related Works

With the growth of the application of smart grid, the security of communication has widely been concerned. More and more people begin to present some methods and mechanisms for protecting the security of communication in smart grid. These methods and mechanisms can be simply shown as follows.

In [1], Ren et al. proposed a provable secure scheme PASS for privacy-protected yet accountable communications between smart meters and smart grid control center. In the PASS scheme, some formal definitions and requirement analysis of privacy and accountability are provided in smart grids. Corresponding data can be hidden and the privacy of customer can be protected by using the PASS scheme. In [2], a wireless communication architecture is first proposed for a smart distribution grid (SDG) based on wireless mesh networks (WMNs). Then, the security framework under this communication architecture is analyzed and potential security attacks and possible counterattack measures are studied. In order to demonstrate the effectiveness of the security framework, a smart tracking firewall was developed to address the intrusion detection and response issue in a WMN-based SDG system. In [3], Wei et al. first discussed the major challenges and strategies to protect smart grid against cyberattacks. Then, they proposed a conceptual layered framework for protecting power grid automation systems against cyberattacks.

In [4], Li and Cao first introduce multicast communications in the smart grid, analyze the requirements on multicast authentication, and review related work. Then, they describe their one-time signature scheme. At last, they present the multicast authentication protocol. In [5], Luo et al. first described the background of smart grid. Then, they analyzed some key technologies, like wide-area measurement system and wide-area communication system. These technologies accelerate the development of wide-area protection. Finally, they prospected the development trends of wide-area protection in smart grid. In [6], Xia and Wang first analyze Wu-Zhou's key management scheme for the smart grid and show it is easily broken by man-in-the-middle attacks. Then, they consider the communication model used by Wu-Zhou and give a detailed description of the components in the model. With the components, they propose a new secure key distribution scheme for the smart grid with high efficiency as well as high security.

In [7], Yan et al. present the background and requirements for smart grid communication security. After discussing the challenge of smart grid communication security, the current research and solutions are surveyed. This paper gives an insight into smart grid communication security in architecture features, system designs, and technical development. In [8], Li et al. discussed the design of a secure access gateway (SAG) for home area network and provided a framework on how to improve the system security, capacity, flexibility, and scalability through cognitive networking.

In [9], Wang and Lu presented a comprehensive survey of cybersecurity issues for the smart grid. Specifically, they focused on reviewing and discussing security requirements, network vulnerabilities, attack countermeasures, secure communication protocols, and architectures in the smart grid. They aim to provide a deep understanding of security vulnerabilities and solutions in the smart grid and shed light on future research directions for smart grid security. In [10], Knapp and Samani explained how to secure the smart grid by using the security methodologies and practices described in earlier chapters. Many methods were explained, including end-point protection, securing individual "zones" within the smart grid architecture, data and application security, and situational awareness.

In [11], Huang et al. first discuss the important security problem of bad data injection in smart grid. Then, from the defenders' point of view, the authors study the quickest detection techniques to detect the bad data injection attack as quickly as possible. And they also demonstrate that the proposed attack can be accomplished by learning the topology structure of the power system and is difficult to detect. In [12], Bou-Harb et al. discuss the security and feasibility aspects of possible communication mechanisms that could be adopted on that subpart of the grid. By accomplishing this, the correlated vulnerabilities in these systems could be remediated, and associated risks may be mitigated for the purpose of enhancing the cybersecurity of the future electric grid.

Though these security methods for smart grid are derived from theoretical analyzing and deducing, they do not take into account the real-time nature of smart grid and lack of the risk management function when the smart grid is attacked. Therefore, these methods are limited in practical application. In order to solve this problem, we propose a new intrusion detection scheme for smart grid, which is based on our proposed communication optimization algorithm.

3. Intrusion Detection Scheme

As mentioned above, a typical communication network infrastructure consists of home area network, neighborhood area network, and wide area network in a smart grid. In order to describe the network infrastructure, we define

$$G = (V, E, D), \tag{1}$$

where G is a directed graph used to describe a multihop multichannel network. V is a smart grid component, which denotes some nodes and can measure electricity consumption and manage communications with higher layer components. E is the wireless links between the nodes. D denotes the information flow which can be transmitted in different channels smoothly.

In order to enhance the security of smart grid, the intrusion detection technology is usually used. The fundamentals of intrusion detection is to gather and analyze communication information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). If an obvious deviation between monitored information values is found, an alarm will be issued and the corresponding outlier should be identified and segregated from the communication network of smart grid. If the transmission of communication is not constrained or optimized in the smart grid, the instruction system may achieve a higher false alarm rate because the power requirement of system is dynamic. Therefore, it is necessary to consider how to control and optimize the transmission of communication information in the smart grid. Since the smart grid network is a hybrid of the power system and a communication network, intrusions should be detected that concern either the power system or the communication network or both. Because there are three different layer communication networks (HAN, NAN, and WAN), our proposed intrusion detection algorithm should have the distributed characteristics which can be applied in the three different layer communication networks.

3.1. Communication Optimization Algorithm. In order to describe the communication optimization algorithm conveniently, all the notation and definitions used in the rest of this paper are summarized in Table 1, respectively.

In the multihop multichannel network G, the links or channels and all flows should be set appropriately when the data flow can be transmitted in the channels smoothly. Here, we let the Boolean variable $v_i(e \mid t) = 1$ when data is transmitted on link channel i of link $e$during time slot t. Thus, we can get the following inequality because the number of active channels of link e during time slot t is less than the maximum number of all channels of the link e:

$$\sum_{i \in C} v_i(e \mid t) \leq C(e). \tag{2}$$

Because S_i is the constraining set belonging to channel i of link e and $H(S_j)$ is the right hand side constant of the pair which includes the set S_j, we can get the following inequality:

$$\frac{1}{H\left(S_j\right)} \sum_{(e,j) \in S_j} \frac{d_j(e)}{C_j(e)} \leq 1. \tag{3}$$

Because $p_i(e \mid m)$ is the number of information flow m allowed on channel i of link e and $r(m)$ is the total number of information flows m allowed on the link, we can get $\sum_{e=s(m)} \sum_{i \in C} p_i(e \mid m) = r(m)$. As we all know, the flow allowed on a channel is smaller than the total flow transmitted on this channel, and we can get the following inequality:

$$\frac{1}{H\left(S_j\right)} \sum_{S_j} \frac{\sum_{m \in M} p_j(e \mid m)}{C_j(e)} \leq 1. \tag{4}$$

The basic method of the communication optimization algorithm is to find the optimal path for communication flows. Based on this method, the collector first counts all the routes from the source node to the destination node. Then, it begins to calculate the accumulation of the constraining pairs' weights. In the following step, it will label the route which has the lowest value of weight accumulations as the shortest path. Based on these shortest paths, the desired information flow $r(m)$ is distributed to the corresponding node. Thus, the source destination pair, which is also called a commodity pair, can find the optimal route with the shortest distances and link weights.

Table 1: The notation and definitions used in the rest of this paper.

Notation	Definition
e	A link of the network
$C(e)$	All channels of a link e
$C(a \mid e)$	The maximum number of active channels that can be activated on the link e
$C_i(e)$	The transmission capacity of the ith channel in data link e
$d_i(e)$	The information flow currently transmitting on channel i of link e
$v_i(e \mid t)$	The Boolean variable when information is transmitted on channel i of link e during time slot t
S_i	The constraining set belongs to channel i of link e
n	The number of sets of link and channel constraining pairs $(S_1, S_2, S_3, \ldots, S_n)$ between each pair of nodes which are allowed to communicate with each other directly
$(s(m), d(m))$	The communication pair of information m between source node and destination node
$H(S_j)$	The right hand side constant of the pair which includes the set S_j
M	The number of communication pairs
$p_i(e\|m)$	The number of information flow m allowed on channel i of link e
$r(m)$	The total number of information flows m allowed on a link
$w(j)$	The weight of the constraining pair of channel i of link e
$b(j)$	The weight of each set S_i whose value is calculated by the distance between two nodes
F	The maximum scaling factor where its value denotes the total slack capacity needed in the network

Based on the above constraints and optimization method, we propose a communication optimization algorithm in smart grid. The shortest path of communication can be found by using the communication optimization algorithm. The communication optimization algorithm is described as follows.

Algorithm 1 (communication optimization algorithm). Consider the following.

Step 1. Initialize $G = (V, E, D)$, and detect whether there is some source information in certain node. If there is some

source information in the node, it will be labeled as a source node.

Step 2. Detect the destination node of the source information and find out all adjacent links of the source node.

Step 3. If link e is one of all adjacent links of the source node, the collector counts all the possible transmission routes from the source node to the destination node by the depth-first search method which includes link e.

Step 4. Count all sets of link and channel constraining pairs $(S_1, S_2, S_3, \ldots, S_n)$ between each pair of nodes which are allowed to communicate with each other directly.

Step 5. Initialize $W(j) \leftarrow \delta$, $j \in \{1, 2, 3, \ldots n\}$.

Step 6. Initialize $a \leftarrow 0$.

Step 7. Judge whether all information flows transmitted on channel i of link e are smaller than the allowed maximum (namely, $\sum_{j=1} w(j) < 1$). **If** $\{\sum_{j=1} w(j) < 1\}$, **Then** {the collector begins to calculate the lowest value of weight of the route in terms of the following computation process:

{ For $m = 1$ To M

$\{r \leftarrow r(m)$.

/* assign the total number of information flows m allowed on a link to the variable r */:

While $(r > 0)$

$\{\Delta w(j) \leftarrow (\sum_{j \in S_i} (b(j)/H(S_j)))/C_i(e)$

$P_{\min}(s(m), d(m)) \leftarrow \min \sum_{m \in M} \Delta w(j)$.

/* calculate the lowest value of weight accumulations about the communication pair of information m between source node and destination node */:

$\xi \leftarrow \min(d(P_{\min}))$.

/* assign the lowest value of weight accumulations to the variable ξ */:

$\eta \leftarrow \min\{r, \xi\}$.

/* the route which has the lowest value of weight accumulations will be labeled as the shortest path */:

$r \leftarrow r - \eta$.

/* the total number of the variable r should minus the route of information flow which has the lowest value of weight accumulations */:

$d_i(e) \leftarrow d_i(e) + \eta$.

/* the information flow currently transmitted on channel i of link e should append the route of information flow which has the lowest value of weight accumulations */:

$w(j) = w(j) * (1 + (\varepsilon\eta/d(P_{\min})))\}\}$.

/* calculate the current weight of the constraining pair of channel i of link e */:

$a = a + 1\}$

$\}$

Else {go to Step 8}.

Step 8. $\rho \leftarrow \max(\sum_{j \in S}(d_i(e)/C_i(e)))$.

Step 9. $F \leftarrow a/\rho$.

/* calculate the maximum scaling factor */

Step 10. End.

3.2. Intrusion Detection Algorithm. Based on the communication optimization algorithm, we will design an intrusion detection algorithm to detect malicious data and possible cyberattacks which have considerable influence on the communication flow. In the intrusion detection algorithm, we let the smart grid be completely safe during its deployment phase. And the existing security agreement of different layers holds the same assumptions, which include HAN, NAN, and WAN. Moreover, the monitor can detect the following information, which is shown in Table 2, to collect the malicious network attack behavior.

In the smart grid, there is HAN, NAN, and WAN. Each area network may have multiple links and each link may have multiple channels. Each channel has its communication flow for a link. These communication flows form different monitoring attributes of link. Here, let the multiple monitoring attributes of link e_i in certain area network form a multiple dimension vector $A(e_i) = \{A_1(e_i), A_2(e_i), A_3(e_i), \ldots, A_k(e_i)\}$, where k is the number of the monitoring attributes. And all the monitoring vectors of link $e_1, e_2, e_3, \ldots, e_n$ form a matrix $A(e) = \{A(e_1), A(e_2), A(e_3), \ldots, A(e_n)\}$, where n is the number of links in the area network.

In order to detect any possible intrusion and maintain the security of each area network, we let the information flow sent from the source node to the destination node keep to a normal distribution in each channel during intrusion detection. Thus, all $A(e_i)$ ($e_i \in \{e_1, e_2, e_3, \ldots e_n\}$) in certain area network form a sample of a multivariate normal distribution. And $A(e_i)$ is distributed as $N_k(\mu, \sigma)$, following a multivariate normal distribution with mean vector μ and variance-covariance matrix σ. Therefore, the probability that $A(e_i)$ satisfies $(A(e_i) - \mu)^T \sigma^{-1} (A(e_i) - \mu) \succ \chi_k^2(\alpha)$ is α, where $\chi_k^2(\alpha)$ is the upper (100α)th percentile of a chi-square distribution with k degrees of freedom.

If we assume that the estimate of μ is $\widehat{\mu}$ and the estimate of σ is $\widehat{\sigma}$, then, we can get the probability that $A(e_i)$ satisfies $(A(e_i) - \widehat{\mu})^T \widehat{\sigma}^{-1} (A(e_i) - \widehat{\mu}) \succ \chi_k^2(\alpha)$, which is expected to be roughly α. Let $\phi(e_i) = ((A(e_i) - \widehat{\mu})^T \widehat{\sigma}^{-1} (A(e_i) - \widehat{\mu}))^{1/2}$. Link e_i will be regarded as an outlier if $\phi(e_i)$ or $\phi^2(e_i)$ is unusually large. In our algorithm, link e_i is regarded as an abnormal link if $\phi^2(e_i) \succ \chi_k^2(\alpha)$.

Table 2: The detected information.

Detected information	Collected attack behavior
Sensor sensed data	Fabricate information attack
Information sending rate	Energy exhausting attack
Information mismatch rate	Message alter attack
Information receiving rate	Sink hole attack
Information dropping rate	Black hole attack, select forward attack
Information sending power	Worm hole attack, hello attack

Rather than estimating μ and σ by the simple mean and the simple variance-covariance matrix:

$$\widehat{\mu} = \frac{1}{n}\sum_{i=1}^{n} A(e_i),$$
$$\widehat{\sigma} = \frac{1}{n-1}\sum_{i=1}^{n} (A(e_i) - \widehat{\mu})(A(e_i) - \widehat{\mu})^T \quad (5)$$

in which the values from outlying links can easily distort the estimates of μ and σ and the detection via Mahalanobis distances may fail to identify true abnormal links, we adopt the orthogonalized Gnanadesikan-Kettenring estimators $\widehat{\mu}$ and $\widehat{\sigma}$ [13]. Therefore, the intrusion detection algorithm can be described as follows.

Algorithm 2 (the intrusion detection algorithm). Consider the following.

Step 1. The system sends a "detect" command to the controller of HAN, the controller of NAN, and the controller of WAN, respectively.

Step 2. After each controller receives the "detect" command, it begins to execute our proposed communication optimization algorithm and finds the shortest path of communication from the source node to the destination node, respectively.

Step 3. The controller of each area network, respectively, controls the information flow of corresponding channel and lets the information flow sent from the source node to the destination node keep to a normal distribution in the channel during intrusion detection.

Step 4. After the destination node receives the information flow sent from the source node, corresponding controller begins to calculate $\widehat{\mu}$ and $\widehat{\sigma}$ in terms of the following computation process.

(1) Compute $B(e) = \{b(e_1), b(e_2), \ldots, b(e_n)\}$, where $b(e_1) = P^{-1}A(e_1)$, $P = \mathrm{diag}(\lambda(\widetilde{A}_1(e)), \lambda(\widetilde{A}_2(e)), \ldots, \lambda(\widetilde{A}_k(e)))$, and $\lambda(\widetilde{A}_j(e))$ is the j row of $A(e)$.

(2) Calculate $k \times k$ matrix R, where $\psi_{i,j} = \begin{cases} (1/4)\widehat{\lambda}^2(B_i+B_j) - \widehat{\lambda}^2(B_i-B_j) & j \neq k \\ 1 & j = k \end{cases}$

(3) Apply the spectral decomposition to obtain $\psi = \theta\Lambda\theta^T$, where θ is ψ's eigenmatrix and Λ is the diagonal matrix composed of ψ's eigenvalues.

(4) Compute $H = \{h(e_i) \mid h(e_i) = \theta^T A(e_i)\}$. Then calculate $\Delta = (\widehat{\mu}(H_1(e)), \widehat{\mu}(H_2(e)), \ldots, \widehat{\mu}(H_k(e)))$ and $\Phi = \mathrm{diag}(\widehat{\lambda}^2(H_1(e)), \widehat{\lambda}^2(H_2(e)), \ldots, \widehat{\lambda}^2(H_k(e)))$.

(5) Let $V = P\theta$. Then the robust multivariate estimates are $\widehat{\mu} = V\Delta$ and $\widehat{\sigma} = V\Phi V^T$.

Step 5. If the controller finds obvious deviation between the information data sent by the source node and its monitored data, it will raise the alarm and show corresponding warning information.

Step 6. The controller of each area network, respectively, judges that the information data of each source node has completely been transmitted or not within its own jurisdiction. **If** {there is some information data which has not completely been transmitted}, **Then** {go to Step 3}; **Else** {go to Step 7}.

Step 7. End.

In fact, we choose the Mahalanobis distance measurement because it includes the interattribute dependencies. Thus, we can compare the attribute combinations and get more precise results [14]. The reason why we decide to choose the orthogonalized Gnanadesikan-Kettenring estimator is because it ensures a high breakdown point with some missing data and can compute quickly with a lower computational cost [15].

4. Experiments and Results Analysis

In this section, we first introduce our experiments. Then, we analyze the results. The specific process can be described as follows.

4.1. Experiments. In our experiments, IEC 61850, ZigBee, and IEEE 802.11s are used to build a complex communication system for smart grid. In the complex communication system, there are three layers which include HAN, NAN, and WAN. Moreover, there are 20 nodes in HAN, 3 nodes in NAN, and 1 node in WAN. In order to ensure the security of each component, every node has an intrusion detection system belonging to its corresponding network, which can use our proposed intrusion detection scheme and the inside r attacker detection scheme [15]. By a series of experiments, we can get the false alarm ratio, the detection accuracy ratio, and the power consumption in the intrusion detection system belonging to WAN when the intrusion detection system uses the two different detection schemes, respectively. The results are shown in Figures 1, 2, and 3.

The similar situation can also get in another node's intrusion detection system by using the above two different detection schemes, respectively.

4.2. Results Analysis. Figure 1 shows the false alarm ratio between our proposed intrusion detection scheme and the

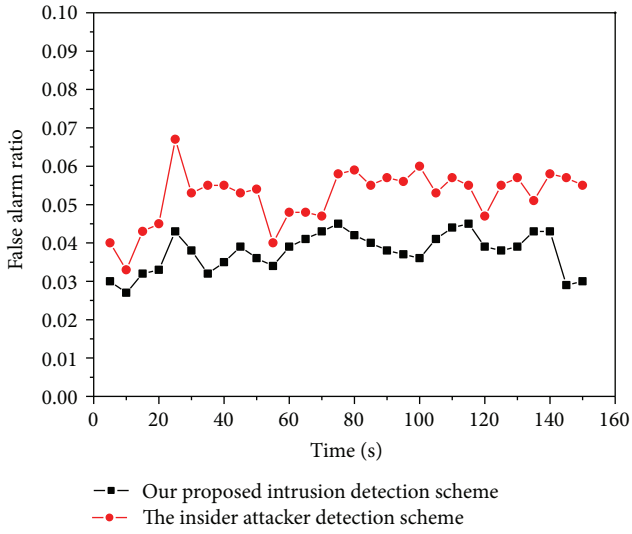

Figure 1: Comparison of false alarm ratio between our proposed intrusion detection scheme and the insider attacker detection scheme.

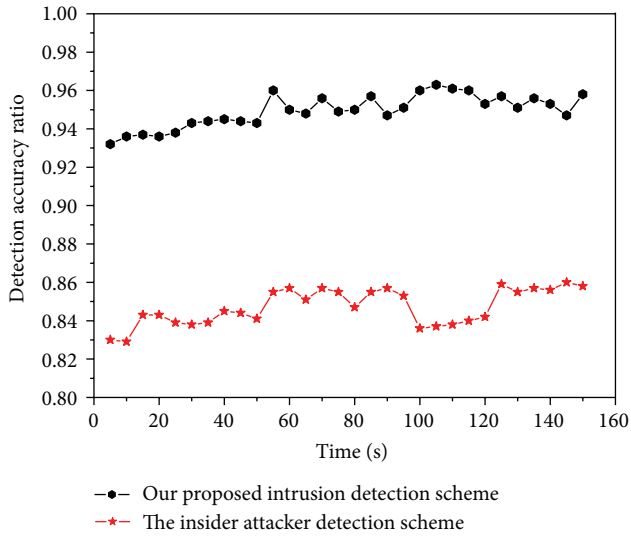

Figure 2: Comparison of detection accuracy ratio between our proposed intrusion detection scheme and the insider attacker detection scheme.

insider attacker detection scheme. According to the results of Figure 1, we will find that our proposed intrusion detection scheme produces less number of false alarm alerts than that of the insider attacker detection scheme.

Figure 2 shows the detection accuracy ratio between our proposed intrusion detection scheme and the insider attacker detection scheme. According to the results of Figure 2, we will find that the detection accuracy of our proposed intrusion detection scheme is much higher than that of the insider attacker detection scheme.

Figure 3 is the comparison of power consumption between our proposed intrusion detection scheme and the insider attacker detection scheme. According to the results

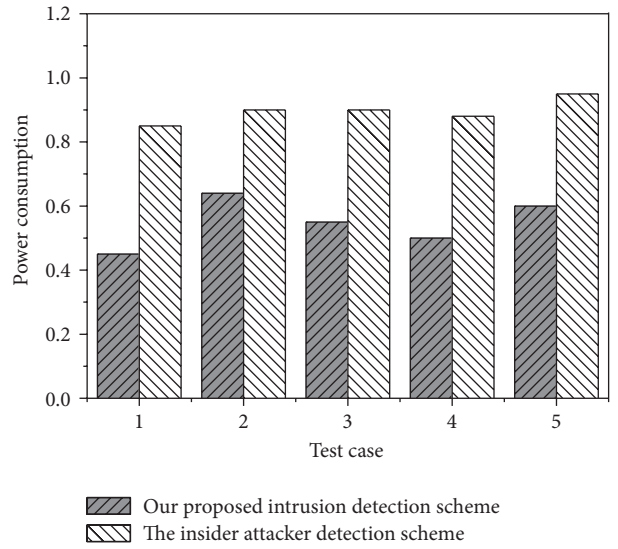

Figure 3: Comparison of power consumption between our proposed intrusion detection scheme and the insider attacker detection scheme.

of Figure 2, we find that the power consumption of our proposed intrusion detection scheme is much less than that of the insider attacker detection scheme.

The main reason generating the three situations is that the detection results are less influenced in our proposed intrusion detection scheme than those in the insider attacker detection scheme.

Because the similar situation can also get in another node's intrusion detection system by using the different detection schemes, respectively, our proposed intrusion detection scheme is feasible and available.

5. Complexity Analysis

In this section, we will analyze the time complexity of our proposed distributed intrusion detection scheme about communication optimization in smart grid. The analysis processes are described as follows.

There are two main algorithms in the distributed intrusion detection scheme. One is the communication optimization algorithm and the other is the intrusion detection algorithm. The time complexity of our proposed distributed intrusion detection scheme mainly focuses on the two algorithms.

(1) In the communication optimization algorithm, we have the following.

(a) In order to detect whether there is some source information in certain node, this algorithm takes $O(|V|)$ time to find out all the nodes, where $|V|$ denotes the total number of nodes in V.

(b) In order to count all the possible transmission routes from the source node to the destination node, this algorithm takes $O(|V| + |E|)$ time

to realize the goal, where $|E|$ denotes the total number of nodes in E.

(c) In order to calculate the lowest value of weight of the route, this algorithm takes $O(n * M)$ time to realize the goal, where n denotes the set total number of link and channel constraining pairs and M denotes the total number of information flows.

Hence, the total time complexity in the communication optimization algorithm is $O((|V| + |E|) * |V| * n * M)$.

(2) In the intrusion detection algorithm, we have the following.

(a) In order to calculate $\widehat{\mu}$ and $\widehat{\sigma}$, this algorithm takes $O(n_1^3 * K)$ time to realize the goal, where n_1 denotes the set total number of links and K denotes the total number of all monitoring attributes in an information flow. Therefore, it will take $O(n_1^3 * K * M)$ time to calculate all $\widehat{\mu}$ and $\widehat{\sigma}$ when the total number of information flows is M.

Thus, the time complexity of our proposed distributed intrusion detection scheme is $O((|V| + |E|) * |V| * n * M^2 * n_1^3 * K)$, where $|V|$ denotes the total number of nodes in V,$|E|$ denotes the total number of nodes in E, n denotes the set total number of link and channel constraining pairs, M denotes the total number of information flows, n_1 denotes the set total number of links, and K denotes the total number of all monitoring attributes in an information flow.

6. Conclusion

In this paper, we proposed an intrusion detection scheme for smart grid which is based on our proposed communication optimization algorithm. In the scheme, each node acts independently when it processes the communication flows and handles cybersecurity threats. And neither special hardware nor nodes cooperation is needed. Our experiment results show that our scheme can achieve a lower false alarm rate and a higher detection accuracy rate than the existing detection schemes. At the same time, it can also reduce the monitoring power consumption with the requirement of grouping the nodes in the network.

Acknowledgments

This paper is supported by Zhejiang Provincial Natural Science Foundation of China under Grant nos. Y14F020186 and Y14F020194 and Startup Foundation of School Grant no. KYS055608103.

References

[1] W. Ren, J. Song, Y. Yang, and Y. Ren, "Lightweight privacy-aware yet accountable secure scheme for SM-SGCC communications in smart grid," *Tsinghua Science and Technology*, vol. 16, no. 6, pp. 640–647, 2011.

[2] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 809–818, 2011.

[3] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde, "Protecting smart grid automation systems against cyberattacks," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 782–795, 2011.

[4] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 686–696, 2011.

[5] L. Luo, N. Tai, and G. Yang, "Wide-area protection research in the smart grid," *Energy Procedia*, vol. 16, pp. 1601–1606, 2012.

[6] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2012.

[7] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[8] T. Li, J. Ren, and X. Tang, "Secure wireless monitoring and control systems for smart grid and smart home," *IEEE Wireless Communications*, vol. 19, no. 3, pp. 66–73, 2012.

[9] W. Wang and Z. Lu, "Cyber security in the smart grid: survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, 2013.

[10] E. D. Knapp and R. Samani, "securing the smart grid," in *Applied Cyber Security and the Smart Grid*, pp. 125–145, 2013.

[11] Y. Huang, M. Esmalifalak, H. Nguyen et al., "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 27–33, 2013.

[12] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42–49, 2013.

[13] R. A. Maronna, R. D. Martin, and V. J. Yohai, *Robust Statistics: Theory and Methods*, John Wiley & Sons, Chichester, UK, 2006.

[14] V. J. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artificial Intelligence Review*, vol. 22, no. 2, pp. 85–126, 2004.

[15] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks," in *Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM '07)*, pp. 1937–1945, May 2007.