Event-Oriented Dynamic Security Service for Demand Response in Smart Grid Employing Mobile Networks

Event-Oriented Dynamic Security Service for Demand Response in Smart Grid employing Mobile Networks

Guo Longhua[1], Dong Mianxiong*[2], Kaoru Ota[2], Wu Jun[1], Li Jianhua[1]
[1] School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[2] Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan

Abstract: Equipped with millions of sensors and smart meters in smart gird, a reliable and resilient wireless communication technology is badly needed. Mobile networks are among the major energy communication networks which contribute to global energy consumption increase rapidly. As one of core technologies of smart grid employing mobile networks, Demand Response (DR) helps improving efficiency, reliability and security for electric power grid infrastructure. Security of DR events is one of the most important issues in DR. However, the security requirements of different DR events are dynamic for various actual demands. To address this, an event-oriented dynamic security service mechanism is proposed for DR. Three kinds of security services including security access service, security communication service and security analysis service for DR event are composited dynamically by the fine-grained sub services. An experiment prototype of the network of State Grid Corporation of China (SGCC) is established. Experiment and evaluations shows the feasibility and effectiveness of the proposed scheme in smart grid employing mobile network.

Key words: mobile network, event-oriented, security service, Demand Response (DR), publish/subscribe (pub/sub)

I. INTRODUCTION

With the development of automated control and modern communications technologies, the smart grid brings improved efficiency, reliability and safety for electric power grid infrastructure [1-3]. As a distributed architecture, smart grid controls a large number of distributed energy devices including sensors and smart meters through the communication network. The employment of mobile networks provides global and flexible communication with reliability and resiliency [4-6]. As one of core technologies of smart grid employing mobile network, Demand Response (DR) can assist users to optimize power use and help reducing peak demand [7-8]. Smart grid employing mobile networks are able to buy electricity from different power generators according to energy market information and optimize their BS operation to minimize their operating expenses. Using DR, power systems contribute to CO_2 emission reduction through reducing the rating of generators which is required to provide peak demand and spinning reserve [9-10].

As a distributed architecture, DR controls a large number of distributed energy resource through the mobile communication network. Mobile network communication technology is utilized for gathering, assembling and synthesizing data provided by various related hardware and software. The messages transferred using mobile network contain power network run data, device state data, measurement data, control data and so on, which set a significant foundation for DR. However, the increased use of smart devices and commercial software render DR communication employing mobile network vulnerable to diverse cyber-attacks. Security service for communication in DR is badly needed to fight against the increased cyber-attacks which impacts on the performance of DR [11]. Assuming that DR controller controls the electrical end devices through the control commands, the security of communication affects both the normal running and the effectiveness of DR performance. Meanwhile, DR programs typically have limits on the number and timing of events that may be triggered for a selected group of customers [12]. A lot of existing works focused on DR events [13-15]. In addition, the consumers and security requirements of different DR program are various according to the actual demand. Thus static security services cannot deal with the requirements of dynamic service of DR. When the service is requested, it is very important to composite the security services dynamically according to the security requirements of the DR event.

In area of smart grid, many researchers have worked on solving the security problems. The works in [5, 16] propose an Efficient Privacy Preserving Demand Response scheme with adaptive key evolution which achieves forward secrecy against privacy attacks. The work in [17] proposed a random spread spectrum based scheme to solve physical security which can achieve both fast and robust data transmission. The work in [18] identifies a variety of practical loads to avoid grid device from device attack which comprise devices to abruptly increase load to cause circuit overflow. The works in [19-21] concentrate on the security problem existing in the communication of smart grid. As for DR in smart grid,

some existing works have focused on the design and implementation of DR communication to pursue better performance in energy efficiency [22], communication cost [18], reliability [23] and so on. However, the security service of DR has not attracted enough attentions in the previous work which can't meet the security requirements against the evolving cyber-attack.

In this paper, event-oriented dynamic security service for smart grid employing mobile network is proposed to enhance the security of DR event. Three kinds of security services including security access service, security communication service and security analysis service for DR event are provided to protect the system composited dynamically by the fine-grained sub services. The composition services deliver appropriate services to electricity suppliers and users according to actual security condition. Experiment and evaluations show the feasibility and effectiveness of the proposed scheme. The remainder of the paper is organized as follows. Section II describes the background related to this paper. Section III presents proposed security service mechanism architecture for DR event. In section IV, the details of proposed security service are given, followed by the implementation system in section V as well as evaluation in section VI respectively. Finally, we draw our conclusion in section VII.

II. BACKGROUND

2.1 DR program architecture employing mobile network

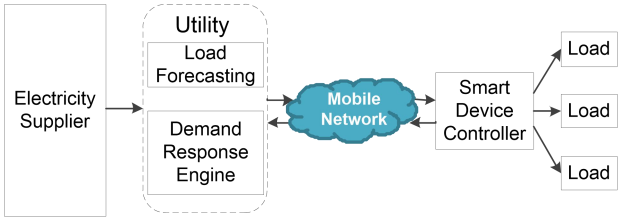

Fig.1: .Schematic diagram of DR program

Figure 1 illustrates the schematic diagram of the DR communication employing mobile network. The electricity customers participate in the DR program through the utilization of smart device controller which controls the electrical devices. The utility works as DR engine and forecasts electricity load according to the network model, regulator/market and operator workstation. According to the electricity supplier, the DR engine may provide the output containing the control commands for directly controllable loads, demand reduction signals for interruptible loads and/or update electricity rates for voluntary demand reduction depending on the various program types the customers are subscribed to [24]. The DR engine works with the help of the load forecast module which forecasts the future demand globally. The devices are connected using mobile networks for gathering, assembling and synthesizing data provided by various related hardware and software.

2.2 Security risks

With the evolvement of cyber-attacks, DR faces serious security risks. The security risks of DR communication are subject to several factors, such as eavesdropping, launching security attacks and so on [25-26]. For example, the malicious or pseudo nodes may acquire and analysis the electricity usage information to expose customers' habits and behaviors, which invades customers' privacy. As for the malicious nodes inside DR program, they may be the legitimate nodes who have access to the network. However, they eavesdrop passively rather than conducting active attacks. As for the pseudo nodes outside the DR program that aren't authorized to access the network, they eavesdrop and decrypt the packets to steal useful information of the program. When launching security attacks, malicious or pseudo nodes are actively involved in networking protocols. They may launch various attacks such as dropping, redirecting or changing the contents of packets. As a result, the DR communication is confronted with security challenges which deserve security protection.

2.3 Security requirements

With the development of DR technology, communication systems with better network connectivity are demanded, which consequently leads to the increasing complexity. To fight against the evolving cyber-attacks, protection is required to secure the DR communication.

The security requirements mainly focus on authentication, integrity, confidentiality, non-repudiation, access control, authorization, etc. Authentication is related to the identification of the communication participators. Integrity is concerned with protecting messages against modification or destruction. Confidentiality refers to the protection of information sent to the appropriate entity. Nonrepudiation helps preventing deny of message senders afterward. Access control deals with the management and allocation of the entities' permission. Authorization ensures that only authorized nodes have access to the resource.

III. PROPOSED SECURITY SERVICE MECHANISM

In the DR program, different DR event demands for different security requirements. Event-oriented dynamic security service is provided to enhance the security of DR event. A comprehensive set on the

basis of DR Service Bus is utilized in the proposed mechanism as shown in Fig.2. In addition to the original Applications (APPs), Business Activity Monitoring (BAM), Rules and Tasks, security service protects the DR event with Service Manager and Service Composition. Security management towards DR event relies on the three major security services including Security Access service (SA), Secure Communication service (SC) and DR event analysis service (EA). Service Manager provides centralized management of original service and additional security service such as versioned, private and public service types in the DR. It includes a Service Registry and a Service Repository which enables versioning and reuse of service types, and a Service Dispatcher providing publish/subscribe (pub/sub) communication framework.

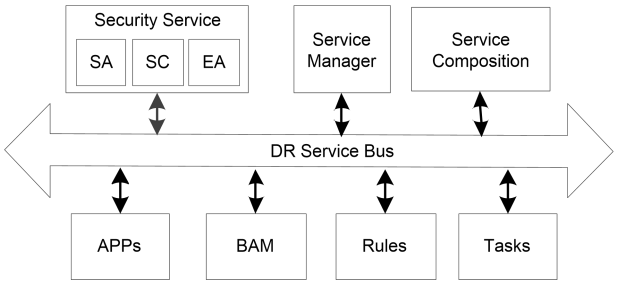

Fig.2: Proposed security service mechanism for DR program.

Security service extends original services with the capability to enhance the DR program from DR event to information communication. The three major security services are provided to protect the system achieved by the fine-grained sub services under the dispatch of service manager, service composition and service selection as shown in Fig.3. Considering the security requirements of the proposed mechanism, Security Access service towards demand side probes the security related data from the electricity supplier. Access control method is utilized to allocate permission based on the probed data. The communication between utility and smart device controller is transferred based on pub/sub pattern using encryption algorithm. The mechanism requires mutual authentication and generates a group of keys acknowledged by both sides of communication. Username/password token with help of dynamic password provides a more secure authentication. In addition, DR event analysis service towards response side is concerned with the truthfulness of decrypted DR event information. Rough set theory based SVM algorithm is utilized to identify the truthfulness of DR event. The electricity loads will run according to the analysis result in case the malicious or pseudo nodes disarrange the DR program.

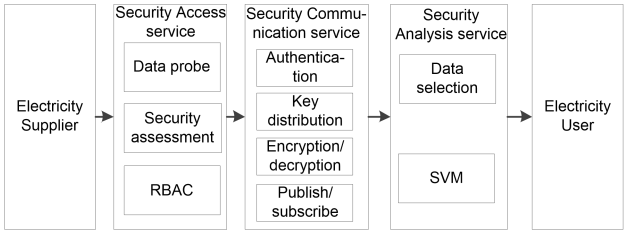

Fig.3: Basic idea of proposed security service.

IV. DESIGN OF PROPOSED SECURITY

4.1 Security Access service

With the development of information technology equipment in DR, it faces increasing vulnerable risks. In the proposed mechanism, Security Access service allocates and manages permissions of creating DR event according to the security condition. As shown in Fig.4, security assessment service is integrated into RBAC service to control the access efficiently. As a secure access control mechanism, RBAC has been widely applied for the concept "role" which makes it convenient to allocate and manage permission. Security Assessment service calculates the threat value which provides the basis for mapping electricity supplier to the executable role.

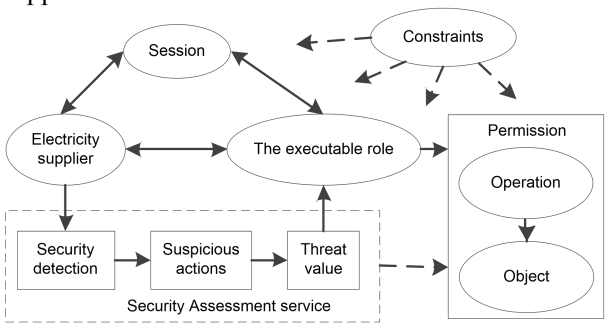

Fig.4: Proposed DR Security Access Service.

In order to assess the security of electricity supplier, security detection is launched to detect the suspicious actions which may cause cyber-attack to the DR project. Suspicious actions in process operation, file operation, registry operation, network operation and vulnerability exploitation are taken into consideration to calculate the threat value. Vulnerabilities of the service, weights and ages of the vulnerabilities are taken into consideration when measuring the risk level of threat. The Equation (1)-(4) are referred to the DRAFT CVSS v2.10 Equations [27] defined in National Vulnerability Database organized by National Institute of Standards and Technology (NIST). As shown in Equation (1), the threat value V of each suspicious action is related to the Impact metric I and the Exploitability metric E.

$$V = 0.1 \times (0.6 \times I + 0.4 \times E - 1.5) \times f(I) \quad (1)$$

The impact metric I is decided by the following three

elements：Confidentiality Impact *CI*, Integrity Impact *II* and Availability Impact *AI*. The exploitability metric can be calculated using three elements including Access Vector *AV*, Access Complexity *AC* and Authentication *A*.

$$I = 10.41 \times \left[1 - (1 - CI) \times (1 - II) \times (1 - AI)\right] \quad (2)$$

$$E = 20 \times AC \times A \times AV \quad (3)$$

What's more, *f(I)* equals to 0 if *I* is 0; otherwise, *f(I)* equals to 1.176.

$$f(I) = \begin{cases} 0, I = 0 \\ 1.176, otherwise \end{cases} \quad (4)$$

A combination of *V* for all *n* suspicious actions existed in the electricity supplier es is defined in Equation (5) [28]. *S(es)* calculates the vulnerability threats for all suspicious actions a_i existed in *es*.

$$S(es) = \ln\left(\frac{1}{n}\sum_{i=1}^{n} \exp(V(a_i))\right) \quad (5)$$

Based on the threat value calculated in Equation (5), an executable role is assigned to the electricity supplier. Assignment between the electricity supplier and role is a many-to-one relationship. Permissions are divided into two dimensions: data permission and functional permission. Permission indicates the authorization of executing the operation in the protected system and data resource. Operation means various command executed in the data resource, such as reading, writing, adding, deleting and so on. Session is a dynamic concept and it's established when the electricity supplier activates some or all the granted roles. Constraint with the separation of duty is used to control assignment operation and avoid conflict.

4.2 Security Communication service

As a distributed architecture, DR system controls a large number of distributed energy resource through the mobile communication network. DR event is transferred under the protection of security communication service. The communication service based on pub/sub service is shown as Fig.5.

Pub/sub pattern is used in the communication to acquire greater network scalability and a more dynamic network topology. In the security association, the mutual authentication service towards demand side and response side is designed based on username/password in addition of dynamic password. The purpose of key distribution service is to initialize communication and update secret key distributed to the participators. The content is encrypted by secret key and exchanged in the form of ciphertext until release. The subscribers who are the members of targeted role can decrypt the ciphertext with privatekey and acquire the content. Electricity suppliers and electricity users are severed as publishers or subscribers respectively.

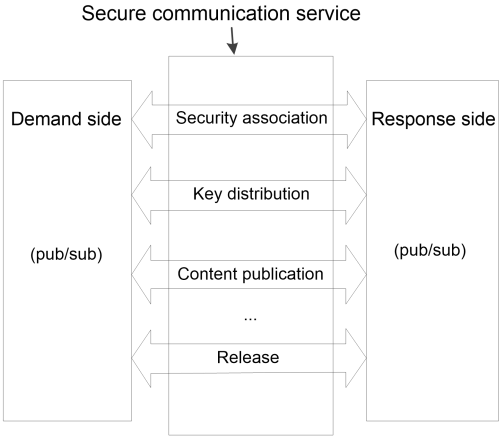

Fig.5: Proposed security communication service

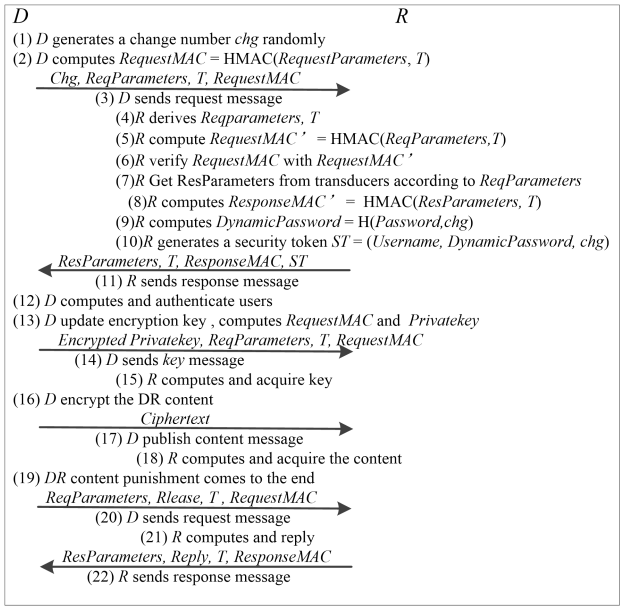

Fig.6: Proposed security communication protocol

The secure communication protocol is shown in Fig.6. The symbols used in the protocol are explained in Table I. In the security association, a *chg* is a challenge number that created randomly. *Chg* is created and distributed to DR participators. The new password is calculated using hash function towards a combination of original password and *chg*. In order to realize the goal of making the information communication secure in the public Internet, the created time of message *T* is added to resist against the replay attack. Publisher computes the digital digest for request parameters with created time message based on hash based message authentication code (HMAC). Original message *M* together with *T* and *HMAC (M)* are sent to subscribers. Subscribers derives *M* as well as *T* and computes *HMAC (M)'*

using HMAC algorithm and verify *HMAC (M)* and *HMAC(M)'*.

In the secure communication, a group-wise key distribution service based on KCT (Key-Chain Tree) is adopted with self-healing ability [29-30]. Initialization phase, broadcast phase and key recovery phase is the three major parts to realize the basic function in the scheme. When participators roles are changed after DR Security Access Service, key updating phase is implemented. Self-healing phase works in case of broadcast packets loss to some participators.

In the initialization phase, maximum number of participators is denoted by *N*. Group manager construct a KCT and *N-1* two-way hash chains. Under the assumption that there are *s* logical participators in the network when initialization, group manager puts all s participators in the first s leave in the tree. The participators from leaf to root are associated with *logN* two-way hash chain. The keys in the associated two-way hash chain are treated as the participators private key and sent to them by group manager. The remaining *N-s* leave are distributed to the initiate members in the future. In the broadcast phase, session keys need to be updated. Logical participators calculate the encryption key using existing private key through hash function. Group manager find out the encryption keys from the *N-1* two-way hash chains. The broadcast packet is constructed in consideration of revoked and illegal participators. In the key recovery phase, the participators acquire the location of encryption session key in the KCT and get the encryption key through hash chain. The key will be recovered after decryption.

When the group of participator changes, it is treated as an initiate member of the new role group. Group manager put it in the position of the first remaining leaf and distribute corresponding private key. A new round of session starts with group manager's reselection of session key and encryption session key. In case of broadcast packets loss to some participators, self-healing phase can recover the session key according to the previous and after broadcast packet. Participator can acquire the position of encryption session key in the KCT and encryption key. Associated with the previous and after broadcast packet, the session key can be recovered.

4.3 Security Analysis service for DR event

In the DR program, DR event entity contains a series of related DR information. An examination towards decrypted DR event is necessary in the security service. In the proposed scheme, rough set theory based SVM service is utilized to identify the truthfulness of DR event.

In a DR event, there is detailed information to describe the DR program. Utility Program describes the information about DR program including name, time, participant, executing level and so on describe how to management and execute the program from the point of electricity company and user. Event Info Type, a part of Utility Program, describes information type in detail such as real-time electricity price, load reduction or transfer and so on. Participant Account describes all the information related to the participant. The attributes include participant name, qualification certificate, reference group and participant program.

One of the most important and typical information for electricity users is the changed electricity load. The number of changed load power is related to DR event, such as time, executing level, real-time electricity price and so on. The proposed scheme calculates linear correlation coefficient to measure the degree of correlation to select the appropriate data. The calculate equation is shown in Equation (6).

$$C = \frac{\sum_{i=1}^{N}(P_i - \bar{P})(X_i - \bar{X})}{\sqrt{\sum_{i=1}^{N}(P_i - \bar{P})^2}\sqrt{\sum_{i=1}^{N}(X_i - \bar{X})^2}} \tag{6}$$

Where C donates the correlation coefficient, P_i, X_i donates the power and feature X of the i_{th} DR event respectively. $\bar{P}$ and $\bar{X}$ donates the average of the N times DR events. The training data is selected according to the correlation coefficient. The higher numbers indicate improved performance.

Avoiding the traditional process from induction to deduction, SVM realize transduced inference from the training examples to the prediction examples efficiently, which greatly simplify the general classification and regression. Extracting features from training examples is the first step. Without deriving weights of networks from the training data, security analysis service captures the geometric characteristics of feature space. What's more, it is capable of extracting the optimal solution with small training data. According to the calculation of correlation coefficient, several suitable dimensions of data are chosen. Hyperplane represents the division boundary with which we can classify the DR events according to these chosen attributes [31]. Hyperplane can be defined as follows:

$$F(x) = W \bullet X + b \tag{7}$$

Where W denotes the weight vector, W= $\{w_1, w_2, \cdots, w_m\}$, b is bias scalar. The training data is a set of m-dimensions data defined as follows: $X = (x_1, x_2, \cdots, x_m)$. $x_1, x_2, \cdots, x_m$ represents the actual value of the m attributes. b can be treated as an extra weight w_0.

The hyperplane can be rewritten as follows:

$$F(x) = w_0 + \sum_{i=1}^{m} w_i x_i \quad (8)$$

Convex quadratic optimization algorithm is adopted to search the Maximum Marginal Hyperplane (MMH). A division boundary can be written according to the MMH as follows:

$$d(X^T) = \sum_{i=1}^{m} y_i \alpha_i X_i^T + b_0 \quad (9)$$

Where α_i and b_0 is determined in the process of optimization. To classify all the training data, the margin of separation (2 /||w||) needs maximum. In the proposed scheme, the training data makes a difference to the training process due to over fitting. Each data point is assigned in the dataset with a membership to decrease the influence of outlier noises. Besides, the deviations are summed. The data point will be assigned with a low membership if it is detected as an outlier. As a result, it makes less contribution to total error term. Different from the equal treatment in standard SVM, the proposed scheme fuzzifies the penalty term for the purpose of reducing the sensitivity of less significant data points.

According to the classification of rough set theory based SVM, the smart device control distinguish the decrypted DR event's truthfulness. Avoiding the fake DR event's attack, the DR participators can protect their system using the rough set theory based SVM.

4.4 Dynamic security service composition

Service composition is one of central part resides the architecture as shown in Fig.7. The event-oriented dynamic compositive services realize and deliver appropriate services to electricity suppliers and users based on the security condition. Regardless of the hosting device, hardware and operating system, the service discovers module detects and communicates with each device including network devices, electricity devices and meters universally. The information of each device is collected and analyzed in the additional security service [32].

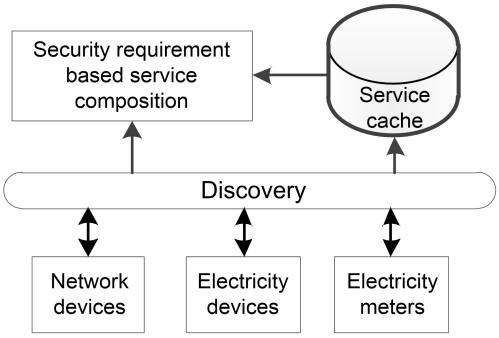

Fig.7: Security requirement based service composition

Excepting satisfying the demand of system in the composition service, security attributes are also taken into consideration. The security information is applied in the process of service composition. The security information can be treated as constraint to search for the optimal service composition.

The security requirement of different DR program is various according to the actual demand. Security requirement based service composition strategy helps providing different service towards various security requirements. When the service is requested, the most appropriate service composition template is searched according to the request and security requirements. If the template can't satisfy the request, the service composition changes based on the template. Small change of service composition will satisfy the different security requirements. The decrease of service searching time and matching calculation will improve the algorithm efficiency. The generated template will add to the template database. The appropriate service composition will be searched in the database if the request faces similar security requirements, which avoids repetitive execution of the service composition logic.

V. IMPLEMENTATION OF THE SECURITY SYSTEM

To bring out the security service between demand side and response side, the structure of the implementation is designed as shown in Fig.8. In addition to the original electricity service like electricity production and consumption, Security Access service is achieved based on the sub services including data probe service, Security Assessment service and RBAC service. RBAC granted roles as publisher or subscriber with proper permission. As a commonly used method in power system, username password token provides a practical and secure authentication with the help of dynamic password in Security Communication service. Encryption and decryption algorithm contributes to the implementation of integration required in DR. Key distribution set a foundation to the secure communication. Pub/sub pattern adopt in the communication acquires greater network scalability and a more dynamic network topology. Cryptographic algorithm ensures the communication security. After data selection service, SVM acquire the classified result through analyzing the features extracted from the examples.

The service layer is the core part in the DR program service implementation which provides services for smart client and achieves business service as well as

business process logic. The original electricity services provide functional services such as electricity production, electricity consumption, etc. The additional security services protect the DR program. The data layer acquires and processes data to support upper layers in database or data collection section.

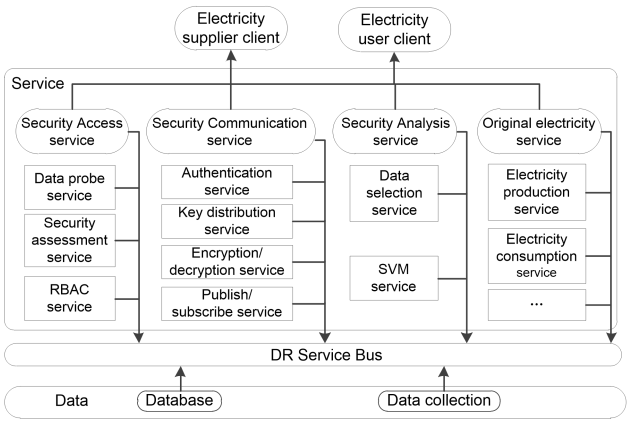

Fig.8: Proposed structure of the implementation

VI. EXPERIMENT AND EVALUATIONS

As required in section II, username password with the help of dynamic password contributes to authentication service identifying electricity suppliers and users. As a classical access control algorithm, RBAC service ensures entities with proper permissions. Security assessment works as the basis for granting electricity supplier permissions. In the communication, HMAC algorithm helps achieving integrity and nonrepudiation of the messages. Security association helps achieving the function of dynamic password and meets the requirements of authentication, integrity, confidentiality and nonrepudiation. Key distribution set a foundation for decryptionalgorithm to achieve the confidentiality authorization of messages. The content is published with the requirements ofintegrity, confidentiality and nonrepudiation until release.

6.1 Security access service

To evaluate the performance of the proposed security access service for DR, we performed experiments in the network of State Grid Corporation of China (SGCC). The network topology in SGCC is shown in Fig.9. Intranet office section is critically dominated for it supports the company's management information business including DR. Intranet production section achieves the basic electricity production, consumption and so on. Although the network security isolation device and firewall examine the information flow between Internet and intranet, there still exists risk of flow with malicious code transported into the intranet. Therefore, it's necessary to monitor and analysis the network flow in the data exchange interface between intranet and Internet. Security management device connects to the core switch and analysis the mirror network flow. Security management device reorganizes the abnormal behavior and restores the potential threats in the network.

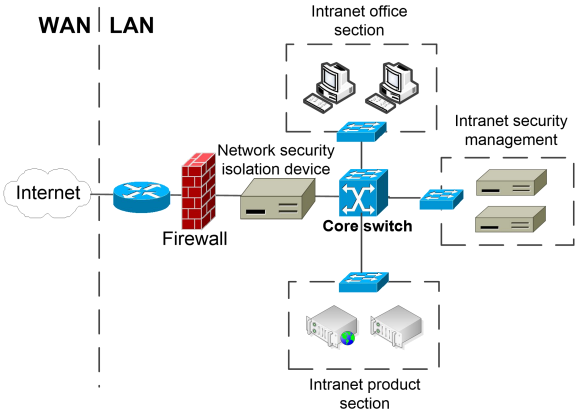

Fig.9: The experiment network topology

In the security management, File Transfer Protocol (FTP) is utilized to transfer the sample test file. The core switch set up a mirror port as the monitor port. IP address, subnet mask and gate way are set to 0.0.0.0 while the interface type is set to "Monitor". The security management device connects to the mirror port. IP address, subnet mask and gate way are set to 193.168.2.1, 255.255.255.0 and 192.168.2.254 respectively. The interface type is set to "Management". Three methods are used to detect security threat including virus detection, static detection and dynamic detection.Virus detection compares the features between the system files and the virus file. Static detection detects the malicious file with unknown features and the encoded shellcode. The dynamic detection finds out the suspicious action through the virtual execution technology.

In the experiment, the dynamic detection result is shown as Table II. Five types of suspicious dynamic actions are detected including process operation, file operation, registry operation, network operation and vulnerability. According to the computing method in Equation (1), the threat score is listed. $S(es)$=0.223 as calculated using Equation (5). Based on the threat value, a corresponding executable role is assigned to the electricity supplier. Permission is assigned to the electricity supplier. Permission indicates the authorization of executing the operation in the protected system and data resource. For the existed security threat, data permission and functional permission are limited. Operation means various command executed in the data resource, such as

reading, writing, adding, deleting and so on. As for production data collecting operation, the permissions contain read, write, save and so on. The permissions in project management operation include read, write, upload, check, examine and approve. Corresponding executable role and permissions differ along with the change of threat value.

Table II
Result of dynamic detection

Dynamic action	Number of suspicious actions	Threat score
Process operation	41	0.45
File operation	26	0.37
Registry operation	58	0.53
Network operation	1	0.12
Vulnerabilityexploitation	2510	0.68

6.2 Complexity evaluation and comparison of secure communication service

Besides the security requirements, complexity evaluation including communication, computation and storage overhead is discussed. The comparison of our work with others is shown in Table III. Communication overhead is composed of broadcast packets in each session. Broadcast packets B_i consists of B_{i1} and B_{i2}. B_{i1} donatestheciphertext of the session key. The length of B_{i1} equals to the key length of the encryption algorithm. B_{i2} marks the position of encryption key in the KCT which occupies just a few bits. The overhead of B_{i2} is negligible comparing with the overhead of B_{i1}. The communication overhead of our work is $O(m)$ where m donates the amount of the subscribers. Calculating times of hash function are used to evaluate the computation overhead. The computation overhead of our work is $O(m)$. In the initialization of the communication, the group manager maps the nodes to the leaves of KCT. Each node is associated with $logN$ two-way hash chains from leaves to root, which works as the private keys of the nodes. The number of private keys stored in each node is $2logN$. As a result, the storage overhead of our work is $O(m\log N)$.

The work in [33] and [34] proposed a security key management and data aggregation in smart grid and wireless sensor networks respectively. In [33], a novel key management scheme which combines symmetric key technique and elliptic curve public key technique are proposed based on the Needham-Schroeder authentication protocol. Communication, computation and storage overhead are $O(N)$ where N donates all the nodes in the network including sensors, collectors and aggregators. In [34], a node X has to compute $O(uv_x)$ hash functions to acquire u synopses, where v_x is X's sensed value. A node X randomly selects these k MACs from the pool received from its c child nodes or generated by itself. The communication overhead is $O(uk)$.

Table III
Comparison of our work with others

Mechanisms	Communication overhead	Computation overhead	Storage overhead
Our work	$O(m)$	$O(m)$	$O(m\log N)$
[33]	$O(N)$	$O(N)$	$O(N)$
[34]	$O(uk)$	$O(uv_x)$	$O(kc)$

Compared with other works, our work provides a complete security mechanism from association to release while others work on securing data aggregation for verification. Publishers who broadcast information don't concern about who subscribes to their information in the content exchange step. The former steps which authenticate and grant access to each subscriber make the content exchange easier and more flexible. The security mechanism designed for the pub/sub based communication simplifies the content publication at a price of implementation complexity and extra overhead. The more content exchanged each time, the less average extra overhead the mechanism will cost. The flexibility and security of communication is achieved at the cost of extra storage overhead.

6.3 Security Analysis of DR event

In the DR event analysis service, rough set theory based SVM service is utilized to classify the pseudo DR event. Optimal margin hyperplane H which is constructed in the sample space achieves the maximum distance between the hyperplane and sample sets. Therefore, SVM has global optimality and good generalization with simple structure. Rough set theory applied in the data classification can efficiently process the uncertainty sample like noise.

Rough set theory based SVM uses upper approximate set, lower approximate set and boundary region represent two types of sample set. Because boundary region allow classification error in the certain degree, the algorithm provides good semantic interpretation and efficiently process the uncertainty sample. Two types of sample found in the boundary region make the absolute value of discriminant minimum. DR event analysis dispenses the category of searching for the optimal penalty coefficient, which avoids excessive regression. The utilization of loop iteration algorithm to search for proper parameter b achieves better performance of SVM. Therefore, the application of rough set theory based SVM in DR event analysis is efficient and feasible.

VII. CONCLUSIONS

In this paper, an event-oriented dynamic security service mechanism for smart grid employing mobile network was proposed to extend original services with the capability to enhance the DR program. The three kinds of security services which includes security access service, security communication service and security analysis service for DR event are provided to protect the system achieved by the fine-grained sub services. Security Access service utilizes RBAC algorithm on the basis of threat analysis result to allocate and manage permission. Security Communication service based on pub/sub pattern contains the following parts: security association, key distribution, content publication and release. In addition, DR Event Analysis service deals with the truthfulness issue of decrypted DR event information. The composition services to DR based on the security condition deliver appropriate services to electricity suppliers and users. Experiment and evaluations shows the feasiblity and effectiveness of the proposed scheme.

Acknowledgements

This work is supported by National Natural Science Foundation of China (Grant No. 61401273 and 61431008), Doctoral Scientific Fund Project of the Ministry of Education of China (No. 20130073130006).

References

[1] V. C. GUNGOR, B. LU, G.P. HANCKE. Opportunities and Challenges of Wireless Sensor Networks in Smart Grid[J]. IEEE Trans. Ind. Electron., 2010, 57(10): 3557-3564.

[2] P. SIANO, C. CECATI, C. CITRO, P. SIANO. Smart Operation of Wind Turbines and Diesel Generators According to Economic Criteria[J]. IEEE Trans. Ind. Electron., 2011, 58(10): 4514-4525.

[3] V. GUNGOR, D. SAHIN, T. KOCAK, S. ERGUT, C. BUCCELLA, C. CECATI, G.HANCKE. Smart Grid Technologies: Communications Technologies and Standards[J]. IEEE Trans. Ind. Informat., 2011, 7(4): 529-539.

[4] S. BU, F. R. YU. Green Cognitive Mobile Networks With Small Cells for Multimedia Communications in the Smart Grid Environment[J]. IEEE Transactions on Vehicular Technology, 2014, 63(5): 2115-2126.

[5] S. HORSMANHEIMO, N. MASKEY, L.TUOMIMAKI. Feasibility Study of Utilizing Mobile Communications for Smart Grid Applications in Urban Area[C]// Proceedings of International Conference on Smart Grid Communications (SmartGridComm'14). Venice: IEEE Press, 2014:440-445.

[6] T. HAN, N. ANSARI. Smart Grid Enabled Mobile Networks: Jointly Optimizing BS Operation and Power Distribution[C]// Proceedings of International Conference on Communications (ICC'14). Sydney, NSW: IEEE Press, 2014:2624-2629.

[7] A.J. ROSCOE, G. AULT. Supporting High Penetrations Of Renewable Generation via Implementation Of Real-Time Electricity Pricing And Demand Response[J]. IET Renewable Power Gener.2010, 4(4): 369-382.

[8] S. LI, D. ZHANG, A.B. ROGET, Z. O'NEILL. Integrating Home Energy Simulation and Dynamic Electricity Price for Demand Response Study[J]. IEEE Trans. Smart Grid, 2014, 5(2): 779-788.

[9] D.T. NGUYEN, M. NEGNEVITSKY, M. DE GROOT. Pool-based Demand Response Exchange Concept and Modeling[J]. IEEE Trans. Power Syst. 2011, 26(3): 1677-1685.

[10] P. FARIA, Z. VALE, J. SOARES, J. FERREIRA. Demand Response Management in Power Systems using a Particle Swarm Optimization Approach[J]. IEEE Intell. Syst. 2013, 28(4): 43-51.

[11] L. ZHENG, N. LU, AND L. CAI. Reliable Wireless Communication Networks for Demand Response Control[J]. IEEE Trans. Smart Grid, 2013, 4(1): 133–140.

[12] W. CHEN, X. WANG, J. PETERSEN, R. TYAGI, AND J. BLACK. Optimal Scheduling of Demand Response Events for Electric Utilities[J]. IEEE Trans. Smart Grid. 2014, 4(4): 2309-2319.

[13] Z. DARABI, M. FERDOWSI. An Event-Based Simulation Framework to Examine the Response of Power Grid to the Charging Demand of Plug-In Hybrid Electric Vehicles[J]. IEEE Trans. Industrial Informatics. 2014,10(1): 313-322.

[14] P. FARIA, Z. VALE, H. MORAIS. Study of Distribution Network Demand Response Events in the Portuguese System[C] // Proceedings of Power and Energy Society General Meeting, San Diego, CA: IEEE Press, 2012: 1-8.

[15] Y. WANG, I. R. PORDANJANI, W. XU. An Event-Driven Demand Response Scheme for Power System Security Enhancement[J]. IEEE Trans. Smart Grid,2014, 2(1): 23-29.

[16] J. XIA, Y. WANG. Secure Key Distribution for the Smart Grid[J]. IEEE Trans. Smart Grid. 2012, 3(3): 1437-1443.

[17] EUN-KYU LEE, MARIO GERLA, SOON Y. OH. Physical Layer Security in Wireless Smart Grid[J]. IEEE Comm.,2012, 50(8): 46-52.

[18] A.H. MOHSENIAN-RAD and A. LEON GARCIA. Distributed Internet Based Load Altering Attacks Against Smart Power Grids[J]. IEEE Trans. Smart Grid, 2011, 2(4): 667-74.

[19] X. LI, X. LIANG, R. LU, H. ZHU, X. LIN, X. SHEN. Securing Smart Grid: Cyber Attacks, Counter measures and Challenges[J]. IEEE Commun., 2012, 50(8).

[20] K.J. ROSS, K.M. HOPKINSON, M. PACHTER. Using a Distributed Agent Based Communication Enabled Special Protection System to Enhance Smart Grid Security[J]. IEEE Trans. Smart Grid, 2013, 4(2): 1216-1224.

[21] E. LEE, M. GERLA, S.Y. OH. Physical Layer Security in Wireless Smart Grid[J]. IEEE Commun., 2012, 50(8): 46-52.

[22] L. ZHENG, S. PARKINSON, D. WANG, L.CAI, C. CRAWFORD. Energy Efficient Communication Networks Design for Demand Response in Smart Grid[C]// Proceedings of International Conference on Wireless Commun. Signal Process. (WCSP'11), Nanjing, China: IEEE Press, 2011, pp. 1–6.

[23] L. ZHENG, N. LU, L. CAI. Reliable Wireless Communication Networks for Demand Response Control[J]. IEEE Trans. Smart Grid, 2013, 4(1): 133–140.

[24] S. MOHAGHEGHI, J. STOUPIS, W. ZHENYUAN, L. ZHAO, H.KAZEMZADEH, "Demand response architecture: Integration intothe distribution management system," in Proc. 1st IEEE Int. Conf. Smart Grid Commun. (Smart Grid Comm), Oct. 2010, pp. 501–506.

[25] X.WANG and P. YI. Security Framework for Wireless Communications in Smart Distribution Grid[J]. IEEE Trans. Smart Grid,2011, 2(4): 809–818.

[26] E. BOU-HARB, C. FACHKHA, M. POURZANDI, M. DEBBABI, C. ASSI. Communication Security for Smart Grid Distribution Networks[J]. IEEE Comm., 2013, 51(1): 42–49.

[27] [Online] Available: http://nvd.nist.gov/cvss.cfm?calcu- lator & version=2

[28] H. Y. TSAI, Y. L. HUANG. An Analytic Hierarchy Process-Based Risk Assessment Method for Wireless Networks[J]. IEEE Trans. Reliability, 2011, 60(4): 801-816.

[29] J. Han , M. Kamber, J. Pei, Data Mining Concepts and Techniques, 3rd ed. Waltham, Elsevier, 2009, pp. 408-415.

[30] M. SHI, Y. JIANG, X. SHEN, C. LIN. Self-Healing Group-Wise Key Distribution Schemes with Time-Limited Node Revocation for Wireless Sensor Networks[J]. IEEE Wireless Commun. 2007,14(5): 38-46.

[31] W. RAO; L. CHEN; S. TARKOMA. Toward Efficient Filter Privacy-Aware Content-Based Pub/Sub Systems[J]. IEEE Trans. Knowledge and Data Engineering. 2013, 25(11): 2644-2657.

[32] S. N. HAN, GYU MYOUNG LEE, N. CRESPI. Semantic Context-Aware Service Composition for Building Automation System[J]. IEEE Trans. Industrial Informatics, 2014, 10(1): 752-761.
[33] D. WU, C. ZHOU. Fault-Tolerant and Scalable Key Management for Smart Grid[J]. IEEE Trans. Smart Grid. 2011, 2(2): 375–381.
[34] S. ROY, M. CONTI, S. SETIA, S. JAJODIA. Secure Data Aggregation in Wireless Sensor Networks[J]. IEEE Trans. Inf. Forensics Security. 2012, 7(3).

Biographies

Guo Longhua, received the B.S. degree in electronic information engineering from Tianjin University, Tianjin, China, in 2013 and is currently pursuing the Ph.D. degree in Shanghai Jiao Tong University, Shanghai, China. He participates in many national projects, such as National Natural Science Foundation of China, National "973" Planning of the Ministry of Science and Technology, China, etc. His research interests include sensor network security, smart grid security, etc.

Dong Mianxiong**,** received the B.S., M.S., and Ph.D. degrees in computer science and engineering from The University of Aizu, Japan. He was a Researcher with the National Institute of Information and Communications Technology, Japan. He was also a Japan Society for the Promotion of Sciences (JSPS) Research Fellow with The University of Aizu, and a Visiting Scholar with the BBCR Group, University of Waterloo, Canada, supported by the JSPS Excellent Young Researcher Overseas Visit Program, from 2010 to 2011. He was selected as a Foreigner Research Fellow (a total of three recipients all over Japan) by the NEC C&C Foundation in 2011. He is currently an Assistant Professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. He is a Research Scientist with the A3 Foresight Program funded by the Japan Society for the Promotion of Sciences, the National Natural Science Foundation of China, and the National Research Foundation of Korea (2011–2016). His research interests include wireless sensor networks, vehicular ad-hoc networks, and wireless security. He was the Best Paper Award Winner of the IEEE HPCC 2008, the IEEE ICESS 2008, and ICA3PP 2014. *The corresponding author. Email: mx.dong@ieee.org.

Kaoru Ota, received the M.S. degree in computer science from Oklahoma State University, USA, in 2008, and the Ph.D. degree in computer science and engineering from The University of Aizu, Japan, in 2012. From 2010 to 2011, she was a Visiting Scholar with the BBCR Group, University of Waterloo, Canada. She was also a Japan Society of the Promotion of Science (JSPS) Research Fellow with the Kato-Nishiyama Laboratory, Graduate School of Information Sciences, Tohoku University, Japan, from 2012 to 2013. She has been with the JSPS A3 Foresight Program as one of primary researchers since 2011, which is supported by the Japanese, Chinese, and Korean Governments. She is currently an Assistant Professor with the Department of Information and Electronic Engineering, Muroran Institute of Technology, Japan. Her research interests include wireless sensor networks, vehicular ad hoc networks, and ubiquitous computing. She was a Guest Editor of *IEEE Wireless Communications* and *IEICE Transactions on Information and Systems*, and serves as an Editor of *Peer-to-Peer Networking and Applications* (Springer), *Ad Hoc & Sensor Wireless Networks*, *the International Journal of Embedded Systems (Inderscience)*, and *the Journal of Cyber-Physical Systems.*

Wu Jun, is an Associate Professor of School of Information Security Engineering, Shanghai Jiao Tong University, China. He got his PH.D. Degree in Information and Telecommunication Studies at Waseda University, Japan. He was a postdoctoral researcher of Postdoctoral researcher of Research Institute for Secure System (RISEC), National Institute of Advanced Industrial Science and Technology (AIST), Japan, from 2011 to 2012. He was a researcher of Global Information and Telecommunication Institute (GITI), Waseda University, Japan, from 2011 to 2013. His research interests include the advanced computations and communications techniques of smart sensors, wireless communication systems, industrial control systems, wireless sensor networks, smart grids, etc.

Li Jianhua, is a professor/Ph.D. supervisor and the vice dean of School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai, China. He got his BS, MS and Ph.D. degrees from Shanghai Jiao Tong University, in 1986, 1991 and 1998, respectively. He was the chief expert in the information security committee experts of National High Technology Research and Development Program of China (863 Program) of China. He is the member of the committee of information security area of the state 10th five-year plan of China. Also, he is a committee expert of China State Secrecy Bureau and Shanghai Secrecy Bureau. He is also a committee expert of Information Technique Standardization Committee of Shanghai, China. He was the leader of more than 30 state/province projects of China, and published more than 200 papers. He published 6 books and has about 20 patents. He made 3 standards and has 5 software copyrights. He got the Second Prize of National Technology Progress Award of China in 2005. He got the First Prize of National Technology Progress Award of Shanghai in 2003 and 2004, and he got two First Prize of National Technology Progress Awards of Shanghai in 2004. His research interests include information security, signal process, computer network communication, etc.