Detection of Replay Attacks in Smart Grid Systems

Thien-Toan Tran, Oh-Soon Shin
School of Electronic Engineering
Soongsil University, Korea
E-mail: {tttoan, osshin}@ssu.ac.kr

Jong-Ho Lee
Department of Electronic Engineering
Gachon University, Korea
E-mail: jongho.lee@gachon.ac.kr

Abstract—Smart grid has many advantages compared with the traditional power grid, and will soon become new infrastructure for power generation, delivery, and management. However, beside those positive promising, security for smart grid has been emerging as an important issue, since the smart grid will be a combination of many kinds of systems and security protocols that cover the whole system are still not complete. In this paper, we focus on replay attacks, which could be one of the most popular security attacks in smart grid systems. In particular, we propose a new detection scheme for replay attacks based on a solution originally developed for a control system.

Keywords—cyber-physical security, replay attack, smart grid.

I. INTRODUCTION

Today almost all activities in our society rely on the electric power system. While computer, wireless communication, and many other aspects have dramatically changed our lives, the electric power system still operates based on the infrastructure that was designed decades ago. This aged system now becomes overloaded, especially during high-peak hours. Traditional power grid cannot predict the power demand efficiently. Therefore, it needs to use additional power sources, when the demand grows high. This solution is expensive and exacerbates pollution problem.

As the next generation power grid, smart grid is being designed to have the ability to solve the problem of the traditional approach. By combining communication networks together with the power grid, smart grid is capable of providing many powerful functions. Instead of following centralized power plant architecture, smart grid will be established on various kinds of plants and will connect them together. We can count in wind power, solar power, tidal power, hydropower, geothermal power, biomass fuel power, etc. With variety of green energy sources, smart grid shall have enough backup power to bring online whenever customer needs.

The power transmission will be put under the management with the help of communication networks established across the power line, as depicted in Fig. 1. All the failures can be detected and fixed as soon as possible to avoid any corruption of power delivery. Power distribution in smart grid includes distribution between several power stations and between a power station and customers. The most important thing in this part is responding to customers’ demand and to power outage.

978-1-4673-2088-7/13/$31.00 ©2013 IEEE 298
by the utility company. The attacker can hijack the smart meters to observe the reported data for a certain amount of time, and replay the data while carrying out the attack. Furthermore, attacker can make customers’ smart meters out of order by injecting incorrect data to the system, which may lead to incorrect energy price or inaccurate prediction. The replay attacks can easily be realized when the utility company cannot manage every smart meter distributed in a large area. We develop an efficient detection scheme for replay attacks based on a periodic injection of artificial noise to the system.

This paper is organized as follow. Section II describes the system model for a smart grid and presents replay attack scenarios. In Section III, we propose a detection scheme for replay attacks after reviewing the conventional detection scheme. Section IV provides numerical results that validate the performance of the proposed detection scheme. Finally, conclusions are drawn in Section V.

II. REPLAY ATTACKS IN SMART GRID SYSTEMS

In this section, we first describe the system model for smart grid systems in Section II-A, and then present scenarios of replay attacks and their impact on the whole smart grid system in Section II-B.

A. System Model

As depicted in Fig. 2, the smart grid system considered in this paper is comprised of the customer equipment, smart meter, estimator, detector, and controller. The customer equipment, which corresponds to the control object, is modeled as a linear time invariant (LTI) system that can be described as

\[ x_{k+1} = Ax_k + Bu_k + w_k, \]  

where \( x_k \), \( u_k \) and \( w_k \), respectively, denote the state variable of the equipment representing the power consumption, control signal, and system noise at time \( k \). The system noise is assumed to follow Gaussian distribution with zero mean and variance \( Q \). The smart meter monitors the equipment and measures the output \( y_k \) as

\[ y_k = Cx_k + v_k, \]

where \( v_k \) denotes the measurement noise, which is assumed to follow Gaussian distribution with zero mean and variance \( R \).

The state estimator employs a Kalman filter, which is the optimal estimator for an LTI system. Kalman filter can provide the minimum variance unbiased estimate of \( x_k \) given the observations \( y_0, y_1, \ldots, y_k \) through recursive updates. The update process of Kalman filter can be written as

\[
\begin{align*}
\hat{x}_{k+1} &= A\hat{x}_k + Bu_k, \\
P_{k+1|k} &= A^2P_{k|k} + Q, \\
K_{k+1} &= P_{k+1|k}C^T\left(C^TP_{k+1|k}C + R\right)^{-1}, \\
\hat{x}_{k+1|k+1} &= \hat{x}_{k+1|k} + K_k(y_{k+1} - \hat{x}_{k+1|k}), \\
P_{k+1|k+1} &= P_{k+1|k} - K_kP_{k+1|k}C_k,
\end{align*}
\]

where \( K_k \) denotes the Kalman gain and \( P_k \) is an estimate of the state variance.

The controller is assumed to employ the linear quadratic Gaussian (LQG) optimal control [5]. Correspondingly, the optimal control signal is generated as

\[ u^*_k = L\hat{x}_{k+1|k}, \]

where \( L \) is the optimal control gain calculated from the Riccati equation with objective of minimizing the control cost. According to [5], the residues \( y_k - C\hat{x}_{k+1|k} \) of the Kalman filter follow independent and identically distributed (i.i.d.) Gaussian distribution with zero mean and variance \( \mathcal{P} = C^2P + R \).

Based on the residues obtained from the estimator, the detector makes a decision whether the system is in abnormal state or not. Assuming that the system employs a \( \chi^2 \) detector [6], the decision variable \( g_k \) at time \( k \) is formed as

\[ g_k = \sum_{i=k-W+1}^{k} \frac{(y_i - C\hat{x}_{i+1|i})^2}{\mathcal{P}}. \]

Note that \( g_k \) is a chi-square distributed random variable with \( W \) degrees of freedom, and \( W \) denotes the window size of detection. If the decision variable \( g_k \) exceeds a certain threshold, the detector will make an alarm that the system is out of the normal state. The threshold can be determined to ensure that the false alarm probability, which is the probability that \( g_k \) is greater than the threshold when the system is actually in normal state, is less than a certain target value.

It should be noted that the system model of Fig. 2 can easily be extended to the case of multiple subscribers, as illustrated in Fig. 3. In this case, for economic and security purposes, one estimator and detector may cover a group of customers, while smart meters are deployed at every customer’s house.
Replay Attacks and their Impact

Replay attacks can be launched when an attacker can gain access privilege to smart meters and can inject control signal to the system. The attacker first needs to record data transmitted from customer equipment to smart meters and analyze them to achieve customer’s characteristics of power usage. After analyzing, the attacker may fudge the data and inject corresponding control signal to the system. The replay attacks can be carried out for two purposes. One purpose is to steal energy; replay attacks could change idle equipments’ status to busy state in order to reroute the power to another place. Another is to cause physical damage to the system. Stuxnet is another case of smart grid systems. Specifically, the random signal is added periodically only for small time duration with the period T. Customer equipment will operate normally in the remaining time. This operation should be accomplished in turn for every equipment in working state. The advantage of the proposed solution is that customer equipment works normally if the system is not under attack. This can greatly reduce system management burden and can decrease waste of power due to mismatch. Moreover, the addition of a random signal to the control signal makes the control signal not optimal any more, causing mismatch between actual power usage and data measured by the smart meters. The power mismatch may also lead to waste of power.

III. DETECTION OF REPLAY ATTACKS

A. Conventional Scheme

In order to help the detector recognize replay attacks, a simple technique has been developed for a control system [5]. The basic idea is to add an additional random signal to the control signal as

$$u_i = u_i^* + \Delta u$$

where $\Delta u$ is chosen to follow Gaussian distribution with zero mean and variance $Q$. Note that $\Delta u$ plays as an authenticator for the system: whenever the system does not respond to $\Delta u$, it is thought that the system is under attack. When $\Delta u$ is added, the system residue is modified as

$$y_i' = C\hat{x}_{i,k-1} = y_i^* - C\hat{x}_{i,k-1}^* + C\mathcal{A}x^*(\hat{x}_{i,k-1} - \hat{x}_{i,k-1}^*) + C\sum_{i=1}^{k-1}\mathcal{A}^{-1}B(\Delta u_i - \Delta u_i^*)$$

Hence, with the help of $\Delta u$, the $\chi^2$ detector can differentiate between the normal and attacked situations. From the side of detector, the larger the variance of $\Delta u$ is, the greater the probability of detecting attacks is. From the side of controller, on the contrary, the control accuracy will degrade as the variance grows.

B. Proposed Scheme

A smart grid system has some characteristics quite similar to those of the traditional control system, in that the system needs to manage working status of the equipments, to predict and control customers’ usage, and to detect system failures. However, the smart grid system also has some unique features differentiated from the control system. The detection scheme in [5] against replay attacks has been developed for a core control system, where increased burden is not so problematic. For the case of smart grid, however, we need to protect the customer equipment rather than the core system. The difference here is about quantity; the conventional scheme may cause huge burden on the management system for the smart grid. Moreover, the addition of a random signal to the control signal makes the control signal not optimal any more, causing mismatch between actual power usage and data measured by the smart meters. The power mismatch may also lead to waste of power.

Based on above reasons, we propose to modify the original solution in [5] so that it can efficiently detect replay attacks in smart grid systems. Specifically, the random signal $\Delta u$ is added periodically only for small time duration with the period T. Customer equipment will operate normally in the remaining time. This operation should be accomplished in turn for every equipment in working state. The advantage of the proposed solution is that customer equipment works normally if the system is not under attack. This can greatly reduce system management burden and can decrease waste of power due to mismatch. Although the proposed solution can give less chance of detecting the attacks, the period T of adding $\Delta u$ can be adjusted to guarantee sufficiently frequent detection capability of the detector.
IV. Simulation Results

In this section, we examine the detection characteristics and power usage of the proposed scheme and compare with that of the conventional scheme. The system constants $A$, $B$, $C$, and $D$ are set to one. The random signal $\Delta u$ is assumed to have the variance $Q = 1V$. From the theory of Kalman filter and LQG optimal controller, Kalman gain $K$ and feedback $L$ are set to $0.9161$ and $-0.6180$, respectively. The window size $W$ of the detector is set to 6. In each simulation, we observe two sets of data: one associated to normally operating condition and the other to the attacked condition. The duration of observation for each case is set to 120 sec. The control signal is assumed to be equal to 5V during the first 80 sec, and 0 during the remaining period. According to the characteristic of the control system, the state variable $x_k$ will become 8V in the steady state, when the control signal is turned on.

Fig. 3 illustrates the system behavior against a replay attack, when the conventional detection scheme is employed. Two dashed lines in Fig. 3(a) represent the variation of state variable $x_k$ with and without $\Delta u$, respectively, under normally operating condition. The attacker is assumed to have snitched the data and launch a replay attack using the recorded data. The red line in Fig. 3(a) denotes the output $\hat{x}_{k+\Delta}$ of the estimator, when the data associated with $\Delta u$ are injected as a replay attack rendering the system under attacked condition. Fig. 3(b) shows the detection process based on the estimates in Fig. 3(a). The red line represents the decision variable $g_k$ of the $\chi^2$ detector, while the blue horizontal line denotes the decision threshold. The decision threshold is set such that the false alarm probability is equal to 0.05. We can observe that the detector is able to detect the attack over most of the time, since most of $g_k$ are above the threshold.

Fig. 4 illustrates the system behavior against a replay attack, when the proposed detection scheme is employed. Note that $\Delta u$ is added to the control signal sporadically for the proposed scheme, while it is added continuously for the conventional scheme. The period $T$ of adding $\Delta u$ is set to 60 sec, and $\Delta u$ is assumed to last for 10 sec whenever added. Under normally operating condition without attacks, $\Delta u$ is assumed to be added during 10-20 sec and 70-80 sec in Fig. 4(a). The time intervals are changed to 30-40 sec and 90-100 sec under the attack condition, as indicated in the estimates. From Fig. 4(a), we can observe mismatch between the replayed signal and estimated value due to random nature of $\Delta u$. Note that the mismatch is seen for the entire duration in the conventional

301
scheme in Fig. 3(a). In the proposed scheme, however, remarkable mismatch happens only at the points when the $\Delta u$ was added for replayed data and when a new $\Delta u$ is added. From Fig. 4(b), it is observed that the proposed scheme can detect the attack only at the points when $\Delta u$ is added. If $\Delta u$ is added more frequently, the detection chance will grow accordingly.

When the system is not under attack, it is important not to waste power especially for smart grid systems. From the response of the systems using conventional and proposed schemes, we can easily calculate different power usage. Fig. 5 illustrates the amount of mismatch power and the percentage of wasted power due to mismatch out of the total power consumption. The proposed scheme is shown to yield much smaller power waste than the conventional scheme due to the sporadic addition of the random signal.

V. CONCLUSIONS

We have investigated efficient detection of replay attacks in smart grid systems. By adding an artificially generated random signal to the control signal, the detector can recognize whether the system responds to the random signal or not. A solution originally designed for protecting the core control system has been modified to be suitable for smart grid systems. In the proposed scheme, the random signal is added sporadically instead of continuously. Due to this modification, the proposed scheme can greatly reduce the waste of power when the system is under normal condition. When the system is under replay attacks, the system is still capable of detecting the attack using the periodically added random signal. Through computer simulations, the proposed scheme has been compared with the conventional scheme, in terms of the detection capability and power saving. The proposed scheme has been shown to substantially reduce the waste of power, while providing adjustable detection capability.

ACKNOWLEDGMENTS

This work was supported in part by the Human Resources Development program (No. 20114010203110) of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government Ministry of Knowledge Economy, and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 20110020262).

REFERENCES