Denial-of-Service (DoS) Attacks on Load Frequency Control in Smart Grids

Shichao Liu, Xiaoping P. Liu,
Department of Systems and Computer Engineering
Carleton University, Ottawa ON, K1S 5B6, Canada
Email:{xpliu,lshchao}@sce.carleton.ca

Abdulmotaleb El Saddik,
School of Electrical Engineering and Computer Science (EECS)
University of Ottawa, Ottawa ON K1N 6N5, Canada
Email:abed@mcrlab.uottawa.ca

***Abstract*—While open communication infrastructures are embedded into smart grids to support vast amounts of data exchange, it makes smart grids vulnerable to cyber attacks. In this paper, we investigate the effects of Denial-of-Service (DoS) attacks on load frequency control (LFC) of smart grids. In contrast with existing works, we consider the problem that how DoS attacks affect the dynamic performance of a power system. The state space model of power systems under DoS attacks is formulated as a switched system. By applying switched system theories, the existence of DoS attacks that make the dynamics of a power system unstable is proved. A two-area power system is used to conduct case studies. The dynamic performance of the power system, such as convergence and steady-state errors, is compared under different DoS attack scenarios. It is shown that the dynamic performance of the power system is affected strongly if the adversaries launch DoS attacks before the dynamics of the power system converge.**

***Index Terms*—Smart grids, denial-of-service (DoS) attacks, load frequency control (LFC), switched systems, power system dynamics.**

I. Introduction

Several large blackouts recently, such as 2003 North American and 2012 Indian blackouts, highlight the importance of improving the capability of real-time situational awareness for power systems. Therefore, future smart grids will use advanced two-way communication and intelligent computation technologies to provide better situational awareness to utilities in terms of power grid states. While these technologies facilitate the aggregation and communication of both system-wide information and local measurement data in selected locations, they introduce new cyber-physical security challenges for keeping smart grids operate safely and reliably [1]. There are already several reported attacks on power grids in U.S. [2], [3].

The importance of securing current and future power grids has attracted more and more attentions from both the academia and industry communities. In [4], the authors pointed out that replacing proprietary network by open communication standards exposes process control and SCADA systems to cyber security risks. A class of false data attacks on state estimation in power SCADA system, bypassing the bad data detection, were firstly presented in [5]. In [6], adversaries were assumed to only know the perturbed model of power systems when they are designing false data attacks against state estimations. In [7], the smallest set of adversary-controlled meters were identified to perform an unobservable attacks.

Although these works are very promising, they considered only static state estimation in power systems without noticing the impacts of attacks on dynamics of power systems. Regarding cyber attacks on SCADA control systems, a lot of challenges were identified by A. A. Cardenas et al in [8], [9]. In [10], Y. Mo et al., studied false data attacks on a control system equipped with Kalman filter. As one of the few automatic control loops in SCADA power systems, Load Frequency Control (LFC) under cyber attacks is considered in Viking projects conducted in [11], [12]. They performed the analysis of the impacts of cyber attacks on control centers in power system, by using reachability methods. However, they only considered the scenario that control center is attacked and controlled by adversaries. In fact, it is harder to attack the control center than to compromise the communication channels in the sensing loop of a power system.

In this paper, we consider DoS attacks on the communication channels in the sensing loop (measurements telemetered in remote terminal units (RTUs) are sent to control center) of power systems. We show that adversaries may make power systems unstable by properly designing DoS attack sequences. To launch a DoS attack on the communication channels, the adversaries can jam the communication channels, attack networking protocols, and flood the network traffic etc. [13], [14]. If attacked, measurement packets sent from sensors through this channel will be lost. Thus, it is reasonable to model the power system under DoS attacks as a switched system, by formulating DoS attacks as an switch (on/off) action in the sensing loop of the power system. The existence of DoS attacks that are able to destabilize power systems is proved by using switched system theories. Case studies are conducted to evaluate the effects of DoS attacks on the dynamics of a power system.

The remainder of this paper is organized as follows. In Section II, the power system with DoS attacks is modeled as a switched system. Then, the existence of DoS attacks that can make the power system unstable is proved in section III. A two-area LFC model is used to evaluate the effects of DoS attacks on the power system in section IV. Finally, conclusions are made in section V.

Notation : $\mathbb{R}^n$, $\mathbb{R}^m$ denotes the n dimensional and m

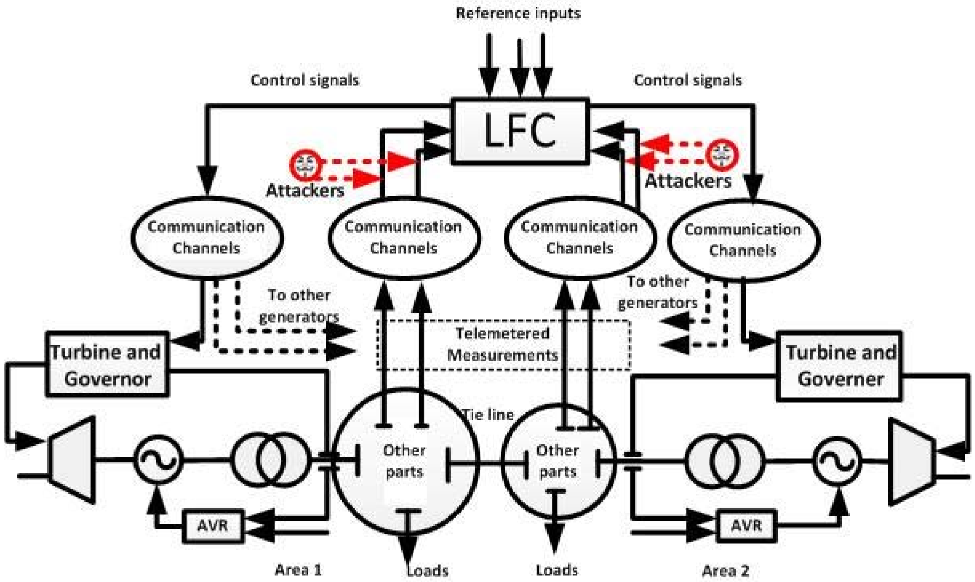

Fig. 1 Two-area Load Frequency Control (LFC) under DoS attacks

dimensional Euclidean space, respectively. The superscript 'T' denotes the transposition of vectors or matrix. Notation $P > 0$ means positive definite.

II. Model of power systems with switching DoS attacks

In this section, the classical model of LFC [15], [16] is extended to include DoS attacks existing in sensing channels for the multi-area interconnected power system, shown in Fig.1. In Fig.1, the telemetered measurements for RTUs are sent back to the control center of LFC through communication channels (either wired or wireless networks). The adversaries launch DoS attacks by jamming the communication channels or flooding network traffics to cause congestions in networks. Thus, the telemetered measurements are lost. Without feedback measurements, the control center can not update its control commands in time and the dynamic performance of the power system will be influenced. For LFC studies, all the generators in each area are represented equivalently by one single machine. In the following models in this paper, we omit the time t in every variable for convenience, such as $x(t)$ is written as x.

For area i, the dynamics of LFC are described by:

$$\begin{aligned}
\Delta\dot{f}_i &= -\frac{D_i}{M_i}\Delta f_i + \frac{1}{M_i}\Delta P_{m_i} - \frac{1}{M_i}\Delta P_{tie}^{ij} - \frac{1}{M_i}\Delta P_{L_i} \\
\Delta\dot{P_{m_i}} &= -\frac{1}{T_{ch_i}}\Delta P_{m_i} + \frac{1}{T_{ch_i}}\Delta P_{v_i} \\
\Delta\dot{P_{v_i}} &= -\frac{1}{R_i T_{g_i}}\Delta f_i - \frac{1}{T_{g_i}}\Delta P_{v_i} + \frac{1}{T_{g_i}}\Delta P_{c_i} \qquad (1) \\
\Delta\dot{P_{tie}^i} &= \sum_{j=1,j\neq i}^{N} 2\pi T_{ij}(\Delta f_i - \Delta f_j) \\
\dot{E_i} &= \beta_i \Delta f_i + \Delta P_{tie}^i
\end{aligned}$$

where
Δf_i frequency deviation;
ΔP_{m_i} generator mechanical power deviation;
ΔP_{v_i} turbine valve position deviation;
ΔP_{c_i} load reference set-point;
ΔP_{tie}^i tie-line power flow in area i;
ΔP_{L_i} load deviation
M_i moment of inertia of generator i;
D_i damping coefficient of generator i;
T_{g_i} time constant of governor i;
T_{ch_i} time constant of turbine i;
T_{ij} stiffness constant;
β_i frequency bias factor of area i;
$E_i = \int ACE_i$, ACE_i is ith area control error;
R_i speed droop coefficient.

Furthermore, we can write the state space model of the above dynamics for LFC in area i as follows:

$$\dot{x_i} = A_{ii}x_i + B_i u_i + \sum_{j=1,j\neq i}^{N} A_{ij}x_j + F_i \Delta P_{L_i} \qquad (2)$$

where
$x_i = \left[\begin{array}{ccccc} \Delta f_i & \Delta P_{m_i} & \Delta P_{v_i} & \Delta P_{tie}^i & \Delta E_i \end{array}\right]^T$;
$u_i = \Delta P_{c_i}$;

$$A_{ii} = \left[\begin{array}{ccccc} -\frac{D_i}{M_i} & \frac{1}{M_i} & 0 & -\frac{1}{M_i} & 0 \\ 0 & -\frac{1}{T_{ch_i}} & \frac{1}{T_{ch_i}} & 0 & 0 \\ -\frac{1}{R_i T_{g_i}} & 0 & -\frac{1}{T_{g_i}} & 0 & 0 \\ \sum_{j=1,j\neq i}^{N} 2\pi T_{ij} & 0 & 0 & 0 & 0 \\ \beta_i & 0 & 0 & 0 & 1 \end{array}\right];$$

$$A_{ij} = \left[\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -2\pi T_{ij} & 0 & 0 & 0 & 0 \end{array}\right];$$

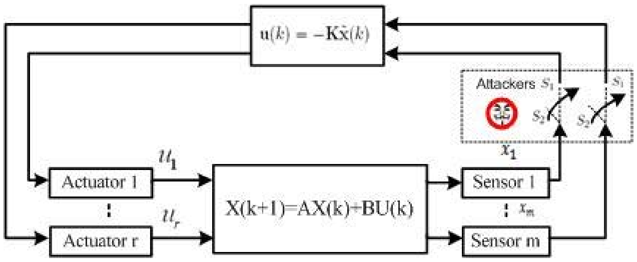

Fig. 2 The model of the power system under DoS attacks

$B_i = \left[\begin{array}{ccccc} 0 & 0 & \frac{1}{T_{g_i}} & 0 & 0 \end{array} \right]^T;$
$F_i = \left[\begin{array}{ccccc} -\frac{1}{M_i} & 0 & 0 & 0 & 0 \end{array} \right]^T.$

Remark 1: Here, we only consider $\Delta P_{L_i} = constant$ cases. For a sufficient duration following a step load change, it does not influent the stability of power system.

For the whole multi-area power system, an linear time invariant(LTI) interconnected model is given by:

$$\dot{\mathbf{x}} = \mathbf{A_c}\mathbf{x} + \mathbf{B_c}\mathbf{u} \tag{3}$$

where
$\mathbf{x} = \left[\begin{array}{cccc} x_1 & x_2 & \cdots & x_n \end{array} \right]^T;$
$\mathbf{u} = \left[\begin{array}{cccc} u_1 & u_2 & \cdots & u_n \end{array} \right]^T;$
$\mathbf{A_c} = \left[\begin{array}{cccc} A_{11} & A_{12} & \cdots & A_{1N} \\ A_{21} & A_{22} & \cdots & A_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ A_{N1} & A_{N2} & \cdots & A_N \end{array} \right];$
$\mathbf{B_c} = diag \left\{ \begin{array}{cccc} B_1 & B_2 & \cdots & B_N \end{array} \right\}^T;$
The sampled discrete-time model is:

$$\mathbf{x}(k+1) = \mathbf{A}\mathbf{x}(k) + \mathbf{B}\mathbf{u}(k) \tag{4}$$

where, $\mathbf{A} = e^{\mathbf{A_c}h}$, $\mathbf{B} = \int_0^h e^{\mathbf{A_c}\tau}\mathbf{B_c}d\tau$, h is the sampling period.

We consider the optimal state feedback controller

$$\mathbf{u} = -\mathbf{K}\mathbf{x} \tag{5}$$

for the power system.

However, the communication channels are assumed to be attacked and the following DoS attacks are conducted. The adversaries attack the communication channels, by preventing the sensed measurements in RTUs to be transmitted successfully to the control center. We can model DoS attacks as an switching on/off event of states $\mathbf{x}$ as shown in Fig.2. We denote the equivalent controller by

$$\mathbf{u}(k) = -\mathbf{K}\tilde{\mathbf{x}}(k). \tag{6}$$

Since we consider the controller equipped with zero-order-hold (ZOH), DoS attacks on $\mathbf{x}$ can be modeled as the following:

$$\left\{ \begin{array}{ll} \tilde{\mathbf{x}}(k) = \mathbf{x}(k) & if, S_1; \\ \tilde{\mathbf{x}}(k) = \tilde{\mathbf{x}}(k-1) & if, S_2 \end{array} \right. \tag{7}$$

Define the augmented state $\mathbf{z}(k) = [\mathbf{x}^T(k), \tilde{\mathbf{x}}^T(k-1)]^T$. By integrating the (6) into (4). We get the closed-loop form:

$$\mathbf{z}(k+1) = \Phi_{\sigma_i}\mathbf{z}(k) \tag{8}$$

where σ_i represents the switch position, $\sigma_i = 1$ for position S_1, $\sigma_i = 2$ for position S_2.
$\Phi_1 = \left[\begin{array}{cc} \mathbf{A}-\mathbf{BK} & \mathbf{0} \\ \mathbf{I} & \mathbf{0} \end{array} \right]^T$; $\Phi_2 = \left[\begin{array}{cc} \mathbf{A} & -\mathbf{BK} \\ \mathbf{0} & \mathbf{I} \end{array} \right]^T$;

Remark 2: DoS attacks are performed or not, according to intentionally designed ith sequential time interval $[t_{si}, t_{fi})$. For example, the switch position is in S_1 for time interval $[k, k+10)$, then S_2 for $[k+11, k+30)$.

III. Existence of successful DoS attacks in smart grids

In this section, it will be shown that DoS attacks can make the power system unstable by carefully designing the sequential attacking time intervals of DoS attacks. In the previous section, the power system with DoS attacks is modeled as a linear switched system. The problems of the stability of switched systems has been extensively addressed, such as [17], [18]. On the one hand, the whole system which comprises of several unstable subsystem can be stable by properly designing switching strategy among these subsystems. On the other hand, it can be made unstable too, by improperly switching among even stable subsystems. From the adversaries point of view, they may be able to make the whole power system unstable by choosing proper switching strategies.

At first, we will show the necessary and sufficient conditions for the stability of switched systems.

Theorem 1. *[18] A switched linear system (8) where $\Phi_{\sigma_i} \in \{\Phi_1, \Phi_2, \cdots, \Phi_N\}$, is asymptotically stable under arbitrary switching if and only if there exists a finite integer* $\mathbf{n}$ *such that*

$$||\Phi_{i1}\Phi_{i2}\cdots\Phi_{in}|| < 1 \tag{9}$$

for all $\mathbf{n}-tuple$ $\Phi_{ij} \in \{\Phi_1, \Phi_2, \cdots, \Phi_N\}$, where $j = 1, 2, \ldots, \mathbf{n}$

According to the above Theorem 1, it may be possible for adversaries to find switching rules to make power systems unstable as long as these switching rules make $||\Phi_{i1}\Phi_{i2}\cdots\Phi_{i\mathbf{n}}|| \geq 1$ happen. In fact, we can equivalently see the switched system (8) in this paper as an average system

$$\Phi_\alpha = \alpha\Phi_1 + (1-\alpha)\Phi_2 \tag{10}$$

where $0 < \alpha < 1$.

Then, we can get the following theorem to show there might exist some switching DoS attacks make the power system (8) unstable.

Theorem 2. *The switched linear system (8) where $\Phi_{\sigma_i} \in \{\Phi_1, \Phi_2\}$, is unstable, if there exists a constant $0 < \alpha < 1$ such that the average system $\Phi_\alpha = \alpha\Phi_1 + (1-\alpha)\Phi_2$ has an eigenvalue with magnitude outside the unity circle.*

Proof: Consider the time interval $[t_s, t_f)$, $\eta = t_f - t_s$ for the switched linear system (8) where $\Phi_{\sigma_i} \in \{\Phi_1, \Phi_2\}$. We assume, without attacks, the switched linear system (8) stays at Φ_1 for $\alpha\eta$ seconds. Then, the adversary starts the DoS attacks. That means the switched linear system (8) stays at Φ_2 for $(1-\alpha)\eta$ seconds. The state of system (8) at time instant t_f will be

$$\mathbf{x}(t_f) = e^{\Phi_1 \alpha\eta} e^{\Phi_2(1-\alpha)\eta} \mathbf{x}(t_s) \tag{11}$$

Let $\Phi(t_f) = e^{\Phi_1\alpha\eta}e^{\Phi_2(1-\alpha)\eta}$. The system (8) is unstable, if $\Phi(t_f)$ has eigenvalues which are outside the unity circle. For some commutable and Hurwitz matrices Φ_1 and Φ_2,

$$\Phi(t_f) = e^{\Phi_1\alpha\eta}e^{\Phi_2(1-\alpha)\eta} = e^{\Phi_1\alpha\eta+\Phi_2(1-\alpha)\eta} = e^{(\Phi_1\alpha+\Phi_2(1-\alpha))\eta} \tag{12}$$

Thus, the system (8) is unstable, if its equivalent average system matrix $\Phi_1\alpha + \Phi_2(1-\alpha)$ has eigenvalues with magnitude outside the unity circle. ■

Remark 3: In this paper, our main objective is to analyze how DoS attacks on communication channels could disturb the operations of the power grid. Thus, the defense mechanisms at the control center are not included in this work. However, it will definitely be our future work on this project. To defend the DoS attacks, there are mainly two different categories of defense strategies in smart grids, either to apply intrusion detection and remove attacks in the cyber layer or to correspondingly adjust demands and generations in physical layer to stabilize the frequencies of power systems again.

IV. Case studies

In this section, a two-area model shown in Fig.1 is used to evaluate the impacts of DoS attacks on power systems. The generators in each area are modeled as a single equivalent generator. Matlab/Simulink is chosen as the simulation environment. In this paper, we consider DoS attacks existing in communication channels in the sensing loop of the power system. That is the feed-back channel (measurements which are sent from remote terminal units (RTUs) to control center) in the power system.

All the parameters of the two-area power system are given in Appendices. In this study, we use 100 MVA as the base unit for per unit (p.u.) calculations.

The original linear quadratic optimal controller is $\mathbf{u} = \mathbf{K}\mathbf{x}$. By using the command *dlqr* in Matlab 2012 and setting $Q = 100 * diag([1111111111])$,$R = 100 * diag([11])$, we get the controller gain. We consider the adversary will launch the DoS attacks according to the proposed switching sequence method in Theorem 2. We will see how the dynamics change according to different DoS attacks launching time, indexing by $0 \leq \alpha < 1$. The time duration is set to be $[0, 300]$. Four cases are considered in this paper:
Case 1: $\alpha = 0$, the power system operates normally.
Case 2: $\alpha = 0.1$, the power system operates under DoS attacks which start at $T = 300 * 0.1 = 30$.
Case 3: $\alpha = 0.2$, the power system operates under DoS attacks which start at $T = 300 * 0.2 = 60$.
Case 4: $\alpha = 0.5$, the power system operates under DoS attacks which start at $T = 300 * 0.5 = 150$.

The dynamics of the two-area power system are shown in Fig.3 and Fig.4. These figures illustrate the effects of the proposed DoS attacks on the two-area dynamic power system. On the one hand, from Fig.1 and Fig.2, it is shown that DoS attacks affect the dynamics of the power system seriously when $\alpha = 0.1$. Thus, it is reasonable for the adversary to launch DoS attacks as early as the dynamic power system does not converge. As long as the dynamics of the power system converge, the DoS attacks might not work any more, such as the case when $\alpha = 0.5$. On the other hand, the convergence of frequencies and tie-line powers in both area 1 and area 2 are affected by the DoS attacks much more seriously than other two elements of the state of the power system. Because frequencies and tie-line powers are mainly telemetered from measurement devices in RTUs, they are sent through communication channels which might be under DoS attacks. In general, the dynamics of the power system under DoS attacks are worse than it runs normally.

V. Conclusion

This paper considered the problem that how DoS attacks in the cyber layer of smart grids can affect the dynamic performance of physical power systems. The power system under DoS attacks was modeled as a switched system, by formulating DoS attacks as an switch (on/off) action on sensing channels. We identified the existence of DoS attacks that can destabilize power systems, by using switched system theories. In case studies, a two-area LFC model was built to evaluate the effects of DoS attacks with different attack-launching instants. It shows that DoS attacks can affect the dynamic performance of the power system badly if they are launched early before the dynamics of the power system converge. Its dynamics are weakly influenced when adversaries enable DoS attacks after the dynamics of the power system converge.

Appendix A

Two-area power system parameters are shown as follows [16].
Area 1:
$T_{ch_1} = 0.3s$, $T_{g_1} = 0.1s$, $R_1 = 0.05$, $D_1 = 1$,
$M_1 = 10$, $\beta = 21$.
Area 2:
$T_{ch_2} = 0.4s$, $T_{g_2} = 0.17s$, $R_2 = 0.05$, $D_2 = 1.5$
$M_2 = 12$, $\beta = 21.5$.
$T_12 = 0.1986pu/rad$

Acknowledgment

The authors thank the reviewers for their valuable comments and suggestions on how to improve this paper. This work was partially supported by the Natural Sciences and Engineering Research Council of Canada and Carleton University President 2010 PhD Fellowship.

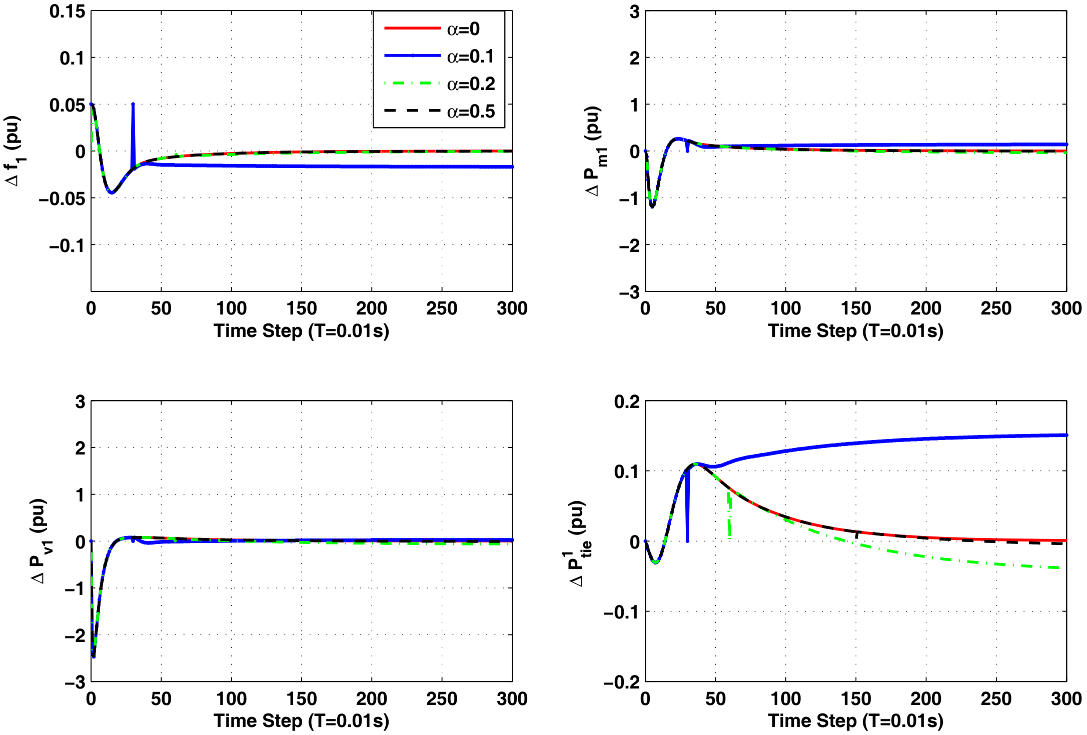

Fig. 3 The dynamics of area 1 under different DoS attacks initial times

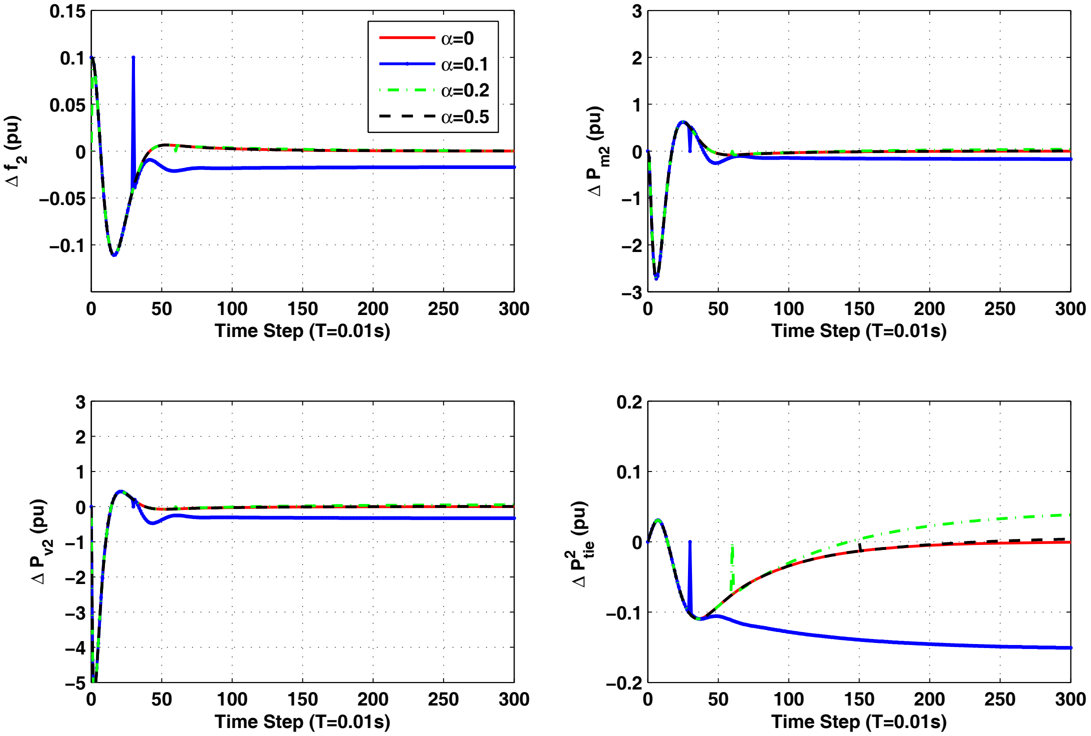

Fig. 4 The dynamics of area 2 under different DoS attacks initial times

References

[1] Y. Mo, T.H.-J. Kim et al., "Cyberphysical security of a smart grid infrastructure," *Proceedings of The IEEE*, vol. 100, no. 1, pp. 195 - 209, 2012.

[2] "Electricity grid in U.S. penetrated by spies" the Wall street Journal, P. A1, April 8th, 2009.

[3] J. Vijayan, "Stuxnet renews power grid security concerns," Computer world, Jul. 26, 2010.

[4] E. Byres and J. Lowe, "The myths and facts behind cyber security risks for industrial control systems, presented at the VDE Kongress, Berlin, Germany, 2004.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proceedings of the 16th ACM conference on Computer and communications security, ser. CCS 09. New York, NY, USA: ACM, 2009, pp. 21 - 32.

[6] A. Teixeira, S. Amin et al., "Cyber security analysis of state estimators in electric power systems," 49th IEEE Conference on Decision and Control, December 15 - 17, 2010, Atlanta, GA, USA, pp. 5991 - 5998.

[7] O. Kosut, L. Jia, R. J. Thomas , Tang Long, " Malicious data attacks on the smart grid," *IEEE Transactions on smart grid*, vol. 2, no. 4, pp. 645 - 658, 2011.

[8] A. A. Cardenas, S. Amin, and S. Sastry, " Research challenges for the security of control systems, in HOT-SEC08: Proceedings of the 3rd conference on Hot topics in security. Berkeley, CA, USA: USENIX Association, 2008, pp. 1 - 6.

[9] S. Amin, A. Cardenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks. in Hybrid Systems: Computation and Control. Lecture Notes in Computer Science. Springer, Berlin / Heidelberg, April 2009, pp. 31 - 45.

[10] Y. Mo and B. Sinopoli, "False data injection attacks in cyber physical systems," in Proceedings of the 1st Workshop on Secure Control Systems, Stockholm, Sweden, April 2010.

[11] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in Proceeding of 49th IEEE Conference on Decision and Control, December 15 - 17, 2010, Atlanta, GA, USA, pp. 5973 - 5978.

[12] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Cyber attack in a two area power system Impact identification using reachability," 2010 American Control Conference, Baltimore, MD, USA, June 30-July 02, 2010, pp. 962 - 967.

[13] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41 - 47, 2006.

[14] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy"Denial of Service attacks in wireless network: the case of jammers," *IEEE Communications surveys and Turorials*, vol. 13, no. 2, pp. 245 - 257, 2011.

[15] J. Machovski, J. W. Blalek, and J. R. Bumby, "Power system dynamics and stability," John Wiley and Sons, 1998.

[16] L. Jiang, W. Yao, Q. H. Wu et. al, "Delay-dependent stability for load frequency control with constant and time-varying delays," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 932 - 941, 2012.

[17] Daniel Liberzon, "switching in systems and control," 2003, Boston, Birkhauser.

[18] H. Lin, and P. J. Antsaklis, "Stability and stabilizability of switched linear systems: A survey of recent results," *IEEE Transactions on Autom. Control*, vol. 54, no. 2, pp. 308 - 322, 2009.