Fuzzy Logic Controller based Automatic Generation Control of Multi-Area Power System

Lakshmikar Reddy Depuru
M.Tech Student, Department of Electrical and Electronics Engineering
S.V.U. College of Engineering, S.V. University, Tirupati, Andhra Pradesh, India.
Smt.V. Usha Reddy
Assistant Professor, Department of Electrical and Electronics Engineering
S.V.U. College of Engineering, S.V. University, Tirupati, Andhra Pradesh, India.

Abstract— The design of Automatic Generation Control (AGC) system plays a vital role in the automation of power system. A game-theoretic approach to smart grid security by joining quantitative risk management with decision making on defensive measures. The quantified risks are used as an input to stochastic security game model. Security game provides the framework for choosing the best response strategies against attackers in order to minimize potential risks. Defensive measures are usually based on a cost-benefit analysis balancing available defensive resources with perceived security risks. Conditional Value-at-Risk (CVaR) measure provides an estimate of the defender's loss due to load shed in simulated situations. In this paper, the proposed Fuzzy Logic Controller can generate best dynamic performance.

Keywords -- Automatic Generation Control (AGC), Security Games, Fuzzy Logic Controller (FLC), Smart Grid.

I. INTRODUCTION

A power grid is a critical infrastructure that must be protected against potential threats. AGC or Load Frequency Control is an important issue in power system for delivering sufficient and reliable power. The main objective of AGC is to establish a normal operating state and optimum scheduling of generation with good quality of power. AGC also controls the frequency of larger interconnected power system. The main purpose of designing FLC based AGC is to ensure stable and reliable power system operation. Risk means, the probability and magnitude of a loss, disaster or other undesirable events. Security games provide an analytical framework for modeling the interaction between malicious attackers to compromise a smart grid, and operators defending it. The rich mathematical basis provided by the field of game theory facilitates formalizing the strategic struggle between attackers and defenders for the control of the smart grid [1]. As a complex system, smart grid presents a number of security challenges. Risk assessment is an important research imperative in smart grid security. Risk assessment is an important research imperative in smart grid security. We note that some authors erroneously refer to risk assessment as vulnerability assessment, which is a different concept [2]. [3], [4] use two-player zero-sum stochastic games for assessing security risks and optimal defenses for the smart grid. In comparison to these work, our current work 1) provides a more intuitive definition of risk states, 2) studies concrete clustering-based intrusion detection algorithms instead of hypothetical ones, and 3) provides alternative definitions of the players' payoffs, one of which is based on the financial risk measure of "conditional value-at-risk Game theory provides the basis for generalizing decision making methods such as Markov decision processes [6]. The main contributions of this paper include, 1) Assessment and identification of risks faced by the automatic generation control system, which constitute an important part of smart grid, due to false data injection attacks. 2) A discussion of the security threat model, potential attacks, and counter-measures. 3) A stochastic (Markov) security game for analysis of best defensive actions building upon the risk analysis conducted and under resource limitations.

The rest of the paper is organized as follows. Section II Proposed FLC based AGC, an essential power system component and presents our game and risk model. Section III Simulation results and discussions. Section IV concludes this paper.

II. PROPOSED SYSTEM

A. Automatic Generation Control

The most critical aspect of a power system is stability, and one of the most important parameters to stabilize is frequency. This is because the frequency of a power system rises/falls with decreased/increased loading. Failure to stabilize frequency may lead to damage to equipment (utility's or end users'), harm to human safety, reduction of or interruption to electricity supply. Violation of frequency stability criteria is one of the main reasons for numerous power blackouts. Less tangible secondary impacts, including loss of data or information and damage to reputation, are equally undesirable. The frequency control system operates at three levels [7]. In an electrical power system, AGC is a system for adjusting the power output of multiple generators at different power plants in response to changes in the load. AGC consist of load frequency control, economic dispatch and interchange scheduling. The main objective AGC are

- To regulate the frequency (using both primary and secondary controls).
- To maintain the scheduled tie-line flows.
- To obtain least operating costs.

When system frequency deviates from the nominal frequency (60Hz for the Americas, 50Hz for most other parts of the world) by a certain threshold, overfrequency and underfrequency protection relays execute tripping logic defined by a protection plan that varies from operator to operator. Assuming a nominal frequency of 60 Hz, overfrequency relays start tripping thermal plants when frequency rise exceeds 1.5 Hz [8], [9]but these relays are usually set to tolerate deviations due to post-fault transients for short periods of time. Underfrequency relays perform underfrequency load shedding (UFLS), which is the sole concern of our study because it results in directly measurable revenue loss. Mullen's UFLS scheme [10]. When the system frequency drops by more than 0.35 Hz below the nominal frequency, to shed this much load:

$$\Delta P_m - \Delta P_e - 0.3/R \qquad (1)$$

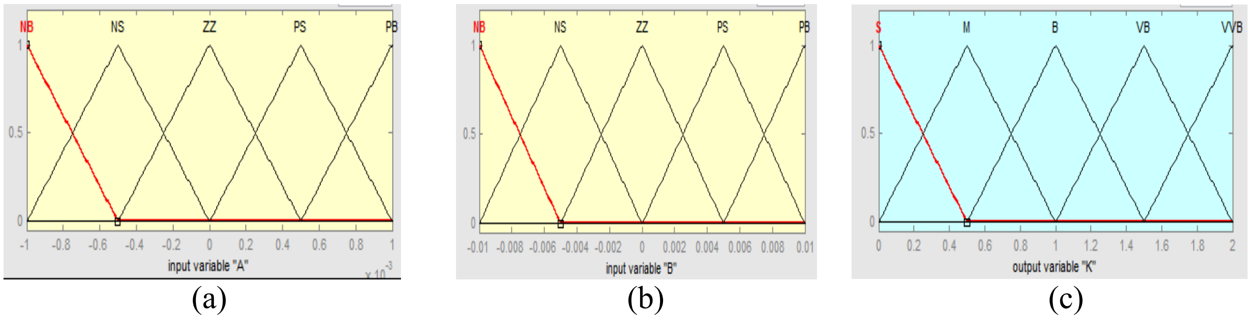
Where ΔP_m is the change in generator's mechanical power, ΔP_e is the change in generator's electrical power, and R is the droop characteristic. Our aim is to model and quantify the risks posed by an attacker who aims to inflict revenue loss on the electricity provider by injecting false data to the automatic generation controller in the hope of triggering load shedding.

B. Fuzzy Logic Controller

Fuzzy Logic Controllers can be more useful in solving a wide range of control problems. Fuzzy Logic controller is used for automatic generation control in a two area power system. The methodology of fuzzy logic controller is very useful when the systems are too complex for analysis by using conventional methods. Fuzzy logic controller mainly consists of four components

(1) Fuzzification Interface
(2) Knowledge Base
(3) Decision Making Logic
(4) Defuzzification Interface

The fuzzification interface measures the values of input variables and converts the input data into suitable linguistic values. The Knowledge Base provides necessary definitions that are used to define the linguistic control rules. The Decision Making logic has the capability of simulating human decision- making based on fuzzy concepts. The defuzzification Interface converts the output variables into corresponding universe of discourse. Membership functions used for designing of fuzzy logic controller for automatic generation control of two area power system are shown below.



(a) (b) (c)

Fig.1. Fuzzy Inference system for FLC:
(a) Membership functions of input1, (b) Membership functions of input2, (c) Membership functions of output

The error (e) and change in error ($\dot{e}$) are inputs of FLC. Two inputs signals are converted to fuzzy numbers first in fuzzifier using five membership functions. Positive Big (PB), Positive Small(PS), Zero (ZZ),Negative Small(NS),Negative Big (NB), Small (S), Medium (M), Big (B), very Big (VB), Very Very Big (VVB).

		Change in Error ($\dot{e}$)				
		NB	**NS**	**ZZ**	**PS**	**PB**
Error (e)	**NB**	**S**	**S**	**M**	**M**	**B**
	NS	**S**	**M**	**M**	**B**	**VB**
	ZZ	**M**	**M**	**B**	**VB**	**VB**
	PS	**M**	**B**	**VB**	**VB**	**VVB**
	PB	**B**	**VB**	**VB**	**VVB**	**VVB**

Table I Fuzzy Rule Base

C. Security Game Model

The decision maker's objective is to maximize its cumulative reward by deciding on the optimal policy d[t], for all t.The effect of an attack manifests as a change to M and r_d this is equivalent to modeling attacks as the actions of an "attacker" agent that at every stage, takes an action from a set of actions. In other words, the attacker comes into the picture as another decision maker. While the theory of multiagent MDP deals with cooperative agents [6], the theory of stochastic games (equivalently, Markov games) is applicable here. A stochastic game is a "competitive MDP" where the agents/players execute their actions simultaneously to maximize their own reward. Define a security game as a stochastic game with a finite state space, and two players (attacker versus defender) that choose their actions from their respective finite action space; or more formally, as a 6-tuple (S, A^A,A^D,M,G^A,G^D), where

- $S \overset{\text{def}}{=} \{s1, \dots s^{Ns}\}$ is the system's state space;
- $A^A \overset{\text{def}}{=} \{a_1, \dots, a_{NA}\}$ is the attacker's action space;
- $A^D \overset{\text{def}}{=} \{d_1, \dots, d_{ND}\}$ is the defender's action space;
- $M(a,d)=[M_{si,sj}(a,d)]_{Ns}\times_{Ns}$ is the system's state transition matrix corresponding to attack action a ∈ A^A and d ∈ A^D;
- $G^A(s)_{=[}G^A_{a,d}(s)_{]NA}\times_{ND}$ is the attacker's expected payoff for playing action a ∈ A^A against defense action d ∈ A^D in system state s ∈ S;
- $G^D(s)=[G^D_{a,d}(s)]_{NA}\times_{ND}$ is the defender's expected payoff for playing action d ∈ A^D against attack action a ∈ A^A in system state s ∈ S;

Let $p^s[t]$ be the stage-t probability distribution on the state space S:

$p^s[t] \overset{\text{def}}{=} [\Pr\{s[t]=s_1\},\Pr\{s[t]=s_2\},\dots.., \Pr\{s[t]=s_{Ns}\}]^T$

then $p^s[t+1]=M(a,d)p^s[t]$. The matrix entry M $s_{i,}$ $s_j(a,d)$ represents the probability of state s_i transitioning to state s_j under attack action *a* and defense action *d.* a different level of risk with each state. In this work, define a risk state as a tuple $(\Delta f_{1,}\Delta f_2)$ i.e., a tuple consisting of area 1's frequency deviation and area 2's frequency deviation. Four risk states are defined by partitioning $(\Delta f_{1,}\Delta f_2)$)

State S_{00}: -0.35 < Δf_1 and -0.35 < Δf_2;
State S_{01}: -0.35 < Δf_1 and $\Delta f_2 \leq$ -0.35;
State S_{10}: $\Delta f_1 \leq$ -0.35 and -0.35 < Δf_2;
State S_{11}: $\Delta f_1 \leq$ -0.35 and $\Delta f_2 \leq$ -0.35;

The definition follows the intuition that S_{00} is the least underfrequency (least risky) state while S_{11} is the most underfrequency (most risky) state.

1. *Attacker's and Defender's payoff's*

For each state s ∈ S, the attacker (defender) incurs a net gain (net loss):

$$Attacker's\ net\ gain = Attacker's\ gain - Attacker's\ cost,$$

$$Defender's\ net\ loss = Defender's\ loss - Defender's\ gain$$

$$= Defender's\ loss$$

Above, the defender's gain is taken to be zero, because no profit is made by merely countering attacks. There are many ways to model the remaining variables, namely the attacker's gain, the attacker's cost and the defender's loss, by making different assumptions about the attacker and defender. For example, can assume the attacker to be a corporate adversary or a nation-state attacker—either way, need to make very specific assumptions about the nature of the attacker. Depending on the assumptions, the attacker's net gain may be much larger, much smaller, or close to the defender's net loss. In this work, we assume the attacker's net gain to be close to the defender's net loss, and hence the security games to be *zero-sum*, i.e.,

$$Attacker's\ gain - Attacker's\ cost = Defender's\ loss.$$

By estimating the defender's loss, which is more readily quantifiable from a power system perspective, essentially also estimate the attacker's net gain. Our zero-sum formulation is a simplification that 1) is based on the loose principle: “what-ever the defender loses the attacker gains”, 2) absolves us from making very specific assumptions about the attacker, 3) guarantees convergence, and 4) provides an accessible demonstration of the utility of our security game framework. The defender’s loss has multiple cost components, including primarily 1) the cost of load shed, 2) the development and run-time costs of the defense actions, and 3) the costs of false positives. We discuss each of these cost components [7]. Based on the discussion above, provide two alternative definitions of $G_{a,d}(s)$:

$$G_{a,d}^{mean}(s) \overset{\text{def}}{=} E\{P_{shed}(a,d,s)\} + c_{fp}p_{f_p}(a,d,s), \qquad (2)$$

$$G_{a,d}^{CVaR}(s) \overset{\text{def}}{=} CVaR_{\alpha}\big(P_{shed}(a,d,s)\big) + c_{f_p}\, p_{f_p}(a,d,s). \qquad (3)$$

Note both P_{shed} and c_{f_p} depend on the actions and state. Summarizing this subsection, $G(s) = G^A(s) = -G^D(s)$. $G_{a,d}$(s)represents the defender’s loss (attacker’s net gain) in risk state s by taking action d against attack action a . In game-theoretic terms, given a stage- t state of $s[t]$, the attacker and defender play a zero-sum matrix game represented by $G(s[t])$.

2. Optimal Attack and Defense Strategies

The objective of a rational attacker (defender) is to maximize (minimize) its expected cumulative payoff $\bar{Q}$. For a game played in a sufficiently long time, we can adopt the *future-discounted reward* model [13] and write $\bar{Q}$ as

$$\bar{Q} \overset{\text{def}}{=} \sum_{t=0}^{\infty} \gamma^t\ G_{a[t],d[t]}(s[t]) \qquad (4)$$

Where, $a[t] \in A^A$, $d[t] \in A^D$, $s[t] \in S, \forall t \in \mathbb{N}, and\ \gamma \in [0,1]$ is the *discount factor*. The discount factor γ is a logical construct for de-emphasizing the payoff at future stages (a smaller γ leads to lower future payoffs). As per game theory, the attacker’s *strategy* is defined as a probability distribution on A^A for a given state $s[t]$, i.e.,
$p^A(s[t]) \overset{\text{def}}{=} [\Pr\{a(s[t]) = a_1\}, \ldots\ldots, \Pr\{a(s[t]) = a_{N_A}\}]^T$.
$p^A(s[t])$ is a $mixed\ strategy$ when none of the entries of $p^A(s[t])$ is 1. When implementing a mixed strategy, for state $s[t]$, the attacker adopts action a_i at probability $\Pr\{a(s[t]) = a_i\}$, for i=1,….N_A. A *pure strategy* is where one and only one entry of $p^A\ (s)$is 1, and the attacker always adopts the action corresponding to this entry for state $s[t]$. The defender’s strategy $P^D(s[t])$, is similarly defined. The (optimal) $P^D(s[t])$ that minimizes $\bar{Q}$ depends on $p^A(s[t]), \forall t \in \mathbb{N}$. For this “reference” attack strategy to be meaningful, we adopt the notion of *Nash equilibrium*, where the equilibrium attack strategy and equilibrium defense strategy are the *best responses* to each other. The question is: are these equilibrium strategies stationary (same for all t). In this paper [11] proved that any n-player $(n \geq 2)$discounted stochastic game has at least one Nash equilibrium in stationary strategies. For two-player zero-sum discounted stochastic games, Shapley [12] proved that there exists a unique Nash equilibrium in stationary strategies. Hence there is no need to compute a separate optimal attack/defense strategy for each t. Furthermore, the problem can be solved recursively using *dynamic programming* to obtain the stationary optimal strategy (solving a zero-sum matrix game at each stage) [9]. At stage , the optimal cost $Q_t(a,d,s)$ (the dependency of s, a and d on t is omitted for notational brevity) can be computed iteratively using the dynamic programming recursion

$$Q_{t+1}(a,d,s) = G_{a,d}(s) + \gamma \sum_{s' \in S} M_{s,s'}\ (a,d) \cdot \min_{p^D(s')} \max_{a} \sum_{s' \in S} Q_t(a,d,s')\ \ p^D(s') \qquad (5)$$

For $t \in \mathbb{N}$ and a given initial condition Q_0. In (5), $p_d^D(s')$ is the element of $p^D(s')$ that corresponds to d . converges to the optimal Q^* as $t \to \infty$. There are multiple ways to implement (5). The algorithm called *value iteration* is prescribed here due to its scalability. To describe the algorithm, we first split (5) into the two-part mutually recursive Bellman equations:

$$V(s) = \min_{p^D(s')} \max_{a} \sum_{s' \in S} Q_t(a,d,s)\ \ p^D(s) \qquad (6)$$

$$Q_{t+1}(a,d,s) = G_{a,d}(s) + \gamma \sum_{s' \in S} M_{s,s'}\ (a,d) V(s'') \qquad (7)$$

For $t \in \mathbb{N}$. We can formulate (5) as a linear program:

$$\min_{p^D(s')} V(s)$$

$$s.t. V(s) \geq \sum_{\mathrm{d} \in \mathrm{AD}} Q_t(a,d,s)\, p_d^D(s), \forall a \in A^A, \tag{8}$$

$$p_d^D \geq 0, \sum_d p_d^D = 1, \forall d \in A^D.$$

The strategy $p^D(s), \forall s \in S$ computed from (8) is the *minimax* strategy w.r.t. Q. The fixed points of equations (6) and (7), V^* and Q^*, lead to the optimal minimax solution for the defender. the optimal attack strategy $p^A(s), \forall s \in S$ can be obtained by solving the dual of linear program (8). Pseudocode for the value iteration algorithm, using (8) and (7) to find V^* and Q^*, can be found in [1].

III. SIMULATION RESULTS AND DISCUSSIONS

A two area system consists of two single area systems, connected through a power line called tie-line. If the system robustness and reliability are more important, Fuzzy Logic Controllers can be more useful in solving a wide range of control problems since conventional controllers are slower and also less efficient in nonlinear system applications. The Mamdani-type fuzzy inference system has been used and the defuzzification technique used is centre of gravity.

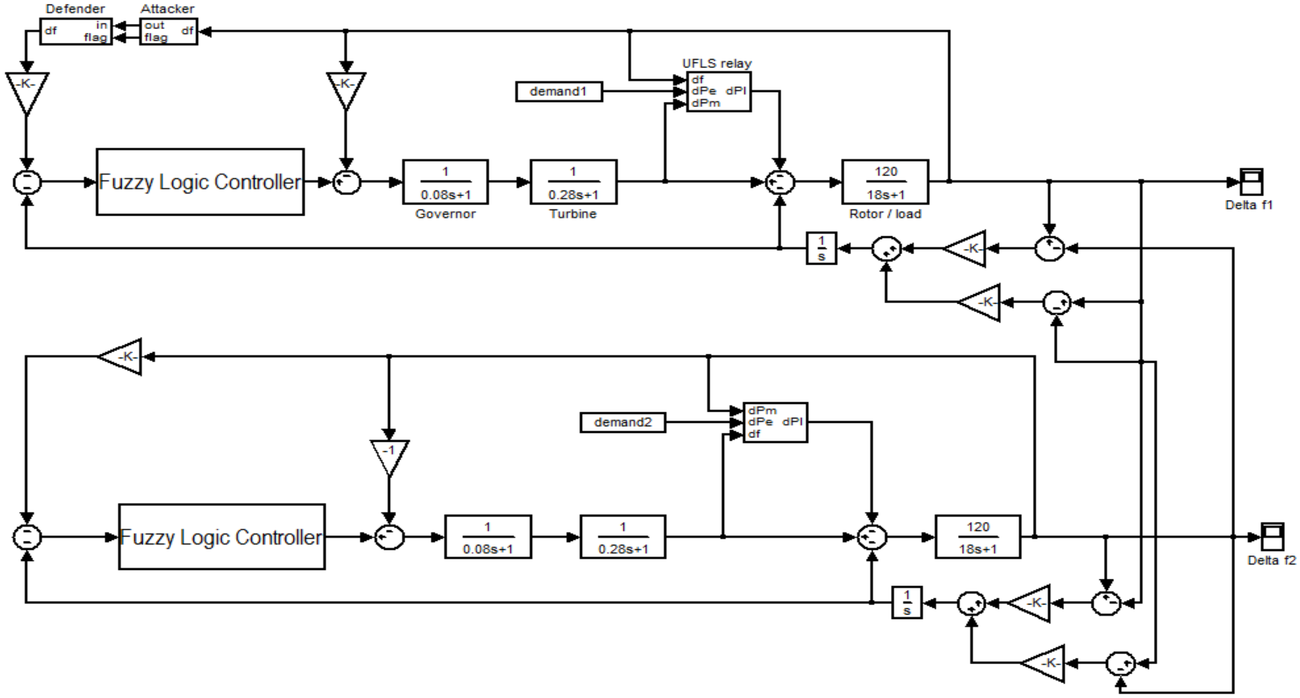


Fig.2. Simulink representation and simulation parameters for a two-area AGC system model based on FLC.

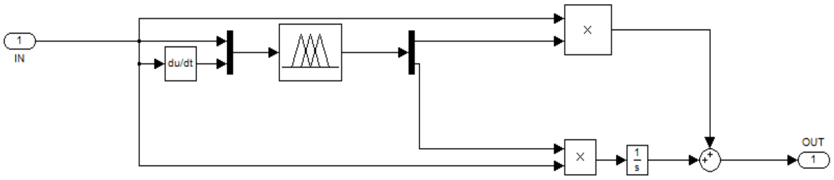


Fig.3. Simulink Structure of Fuzzy Logic Controller

Fuzzy logic controller is used in AGC modeling of the two area power system. The results obtained by using fuzzy logic controller are compared with the results obtained by using conventional controller. Figs show the resulting responses of the simulation model. Fig 3 and 4 shows the frequency responses of the two area power system using Fuzzy Logic Controller plus AGC and Simple AGC.

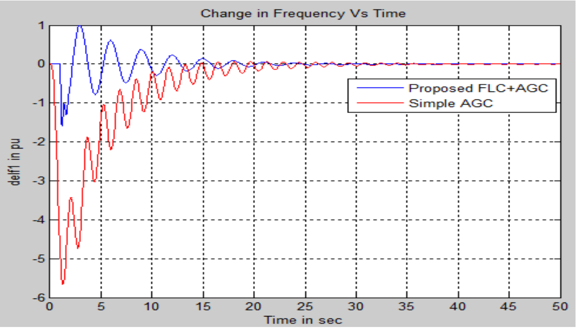


Fig.4. The deviation of the frequency at area-1

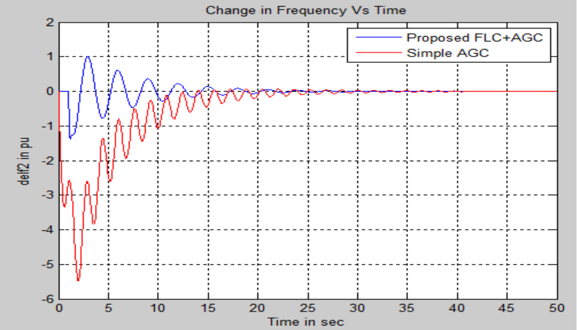


Fig. 5. The deviation of the frequency at area-2

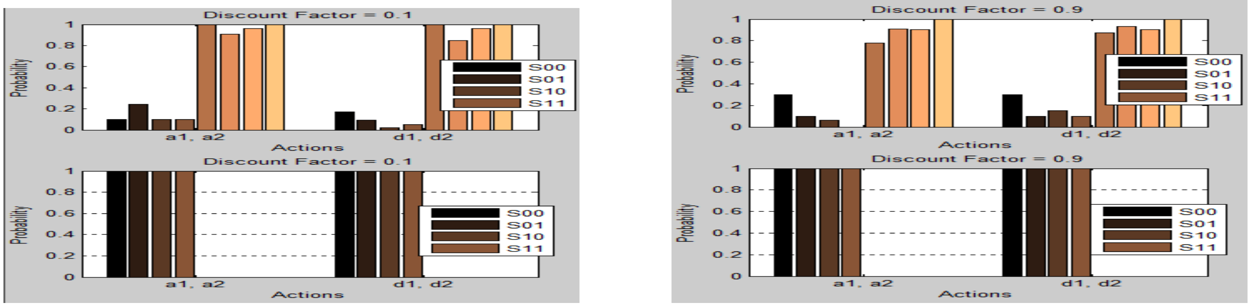


Fig.6. Optimal attack and defense strategies when the game matrix is defined using Simple AGC and FLC+AGC load reconnection delay are set to 30 s.

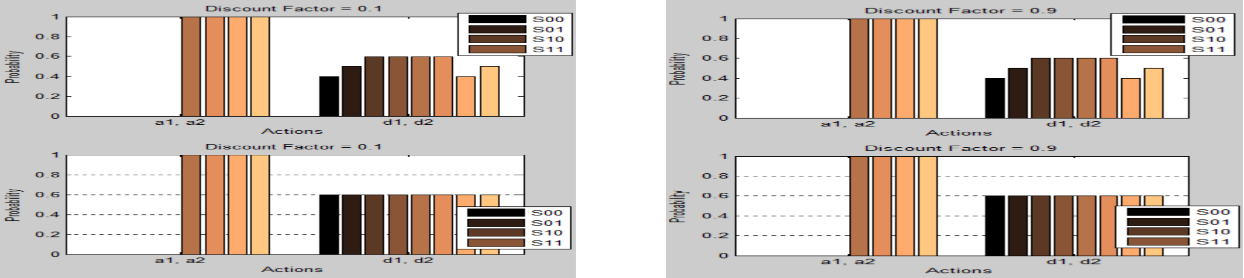


Fig. 7. Optimal attack and defense strategies when the game matrix is defined using Simple AGC and FLC+AGC load reconnection delay is set to 60 s.

Comparisons for two different controllers are shown in table II, which indicates that FLC+AGC have better performance.

Table II Comparison of Different Controllers

Frequency Deviation in	**Controllers**	
	AGC	**FLC+AGC**
Area 1	**44 sec**	**35 sec**
Area 2	**40 sec**	**30 sec**

IV. CONCLUSION

In this paper a fuzzy logic controller is designed for automatic generation control of two area interconnected power system. It mainly controls the frequency deviation and tie-line power deviation of two area system and increases the dynamic performance. A method of the quantitative risk measure CVaR capturing the probability and magnitude of security threats faced by the AGC system due to false data injection attacks. The model attacker-defender interactions using stochastic (Markov) security games to analyze the best defensive actions under resource constraints. The performance of fuzzy logic controller better than other controllers.

APPENDIX

Parameters	Area - 1	Area - 2
Governer Time Constant (Tg)	**0.08**	**0.08**
Turbine Time Constant (Tt)	**0.28**	**0.28**
Power System Equivalent Gain Constant (Kp)	**120**	**120**
Power System Equivalent Time Constant (Tp)	**18**	**18**
Droop Characteristic (R)	**2.4**	**2.4**
Frequency Bias (B)	**0.425**	**0.425**
a12	**-1**	**-1**

REFERENCES

[1] T. Alpcan and T. Başar*, Network Security: A Decision and Game TheoreticApproach*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[2] NIST, Glossary of Key Information Security Terms, Feb. 2011, IR 7298 Revision 1.

[3] Y. W. Law, T. Alpcan, M. Palaniswami, and S. Dey, "Security games and risk minimization for automatic generation control in smart grid," in *Proc. 3rd Conf. Decision and Game Theory for Security (GameSec2012)*, 2012, vol. 7638, pp. 281–295, ser. LNCS, Springer Heidelberg, Germany.

[4] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for voltage control in smart grid," in *Proc. IEEE 50th Annual Allerton Conf. Communication, Control, and Computing*, 2012.

[5] Y. Shoham and K. Leyton-Brown*, Multiagent Systems: Algorithmic,Game-Theoretic, and Logical Foundations*. Cambridge, U.K.: Cambridge Univ. Press, 2009.

[6] S. Sridhar, M. Govindarasu, and C.-C. Liu, "Risk analysis of coordinated cyber attacks on power grid," in *Control and Optimization Methods for Electric Smart Grids*. NewYork,NY,USA:Springer, 2012, vol. 3, pp. 275–294.

[7] Y.W. Law, T.Alpcan and M. P. swami "Security Games for Risk Minimization in Automatic Generation Control" *IEEE Trans.Power syst.,* vol. 30, no. 1, pp. 223-232, Jan. 2015

[8] J.Machowski, J.W. Bialek, and J. R. Bumby*, Power System Dynamics: Stability and Control*, 2nd ed. New York, NY, USA: Wiley, 2008.

[9] C. Luo, H. Far, H. Banakar, P.-K. Keung, and B.-T. Ooi, "Estimation of wind penetration as limited by frequency deviation," *IEEE Trans. Energy Convers.*, vol. 22, no. 3, pp. 783–791, Sep. 2007.

[10] S. K. Mullen, "Plug-in hybrid electric vehicles as a source of distributed frequency regulation," Ph.D. dissertation, Univ. Minnesota, Minneapolis, MN, USA, 2009.

[11] A. M. Fink, "Equilibrium in a stochastic -person game," *Hiroshima Math. J.*, vol. 28, no. 1, pp. 89–93, 1964.

[12] L. Shapley, "Stochastic games," *Proc. Nat. Acad. Sci. USA. (PNAS)*, vol. 39, pp. 1095–1100, 1953.

[13] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for voltage control in smart grid," in *Proc. IEEE 50th Annual Allerton Conf. Communication, Control, and Computing*, 2012.