Environmental/Economic Dispatch Using a Improved Differential Evolution

Libiao Zhang, Xiangli Xu, Sujing Wang, Chunguang Zhou, Caitang Sun
College of Computer Science and Technology, Jilin University, Changchun 130012, P. R. China
e-mail:lbzhang@jlu.edu.cn

Abstract—**This paper presents a new multiobjective evolutionary algorithm for Environmental/Economic power Dispatch (EED) problem based on Differential Evolution (DE). The proposed algorithm is different from the classical DE in the process of mutation. The mutation is carried out with three vectors; one is the local best, other is the global best and third one is selected as randomly. The improved mutation operation is more explicit directional than classic ED, and it push the trial vector quickly towards the global optima. It effectively guarantees the convergence of the algorithm and the diversity solutions. On this basis, a new multiobjective evolutionary algorithm is proposed to handle the EED. The performance of algorithm has been examined over the standard IEEE 30 bus six generator test system, and other multi-objective evolutionary algorithm are compared. Testing and comparing results showed the effectiveness of the algorithm.**

Keywords-environmental/economic dispatch; multiobjective evolutionary; differential evolution

I. Introduction

The EED problems of electrical power systems is study that the minimization of cost of power generation and the minimization of emission of harmful gases under meet a certain total power demand of system. It is great significance to the national economy, and has become a research hot topic in recent years [1, 2, 3]. The EED problems is a multiobjective Optimization problem having conflicting objectives, as the minimization of emission is contrary to the maintenance of cost economy. At present, there has been much research techniques to handle the EED problem have been reported. Generally speaking, there are three approaches to solve EED problem. The first approach is that the problem has been reduced to a single objective problem by treating the emission as a constraint with a permissible limit [4]. This formulation, however, has a severe difficulty in getting the tradeoff relations between cost and emission. The second approach is that the emission and the fuel cost are treat as the optimization objective. However, the EED problem was converted to a single objective problem either by linear combination of both objectives or by considering one objective at a time for optimization. A linear programming technique has been proposed in a reference [5] which considers one objective at a time. References [6, 7] linearly combined different objectives through the weighted sum method to convert the multiobjective EED problem in single-objective optimization problem. This type of approach requires a strong prior knowledge. These methods generate the non-dominated solution by varying the weights, thus requiring multiple runs to generate the desired Pareto set of solutions. Moreover, these methods are not efficient in solving problems having non-convex Pareto optimal fronts. The third approach handles both fuel cost and emission simultaneously as competing objectives, and recent studies have also concentrated on these. The following are some representative multiobjective evolutionary algorithms, Vector Evaluation Genetic Algorithm (VEGA) [8], Niched Pareto Genetic Algorithm (NPGA) [9], Strength Pareto Evolutionary Algorithm (SPEA) [10], based on non-dominated sorting genetic algorithm NSGA[11] SPEA2[12], NSGA2[13] and so on. Also be used to solve the EED problem multiobjective evolutionary algorithms that based on Particle Swarm Optimization (PSO) [2, 3] and based on DE[14].

DE is proposed a new evolutionary algorithm by Storn and Price in 1997[15]. It is population-based, direct search algorithm, adopting real number coding, simple and effective and has been successfully applied in various fields [16, 17]. It is easy to understand and realized and has a strong spatial search capability compared to other evolutionary algorithms. As a new evolutionary algorithm, DE algorithm firstly generates initial population at random in the search space. And DE algorithm creates new individuals by adding the vector difference between two randomly chosen individuals to a third individual in the population. If the new individual has a better value of the fitness function then it will replace old individual. The mutation of the classical DE is improved in this paper. It effectively guarantees the convergence of the algorithm and the diversity solutions. On this basis, a new multiobjective evolutionary algorithm is proposed to handle the EED.

II. Environmental/Economic Dispatch Problem

The EED problem is to minimize two competing objective functions, fuel cost and emission, while satisfying several equality and inequality constraints. Generally the problem is formulated as follows.

A. *Fuel Cost Objective*

The objective of fuel cost is the minimization of total generation cost, while satisfying several constraints. The total fuel cost can be expressed as the following second-order polynomial

$$C = \sum_{i=1}^{n} \left(a_i + b_i \times P_{Gi} + c_i \times P_{Gi}^2 \right)$$

Where C is the total fuel cost, a_i , b_i and c_i are the cost coefficients of the $i-th$ generator, and P_{Gi} is the real power

Corresponding author: Caitang Sun, Email address: sunct@jlu.edu.cn

978-1-4244-6349-7/10/$26.00 ©2010 IEEE

attacks on distributed certification services: passive attacks and active attacks. In passive attacks, adversaries simply drop and refuse to forward other nodes' requests of assigning or renewing certificates. In contrast, adversaries may return a fake reply (namely, an invalid partial certificate) to the requesting node to implement active attacks.

Both passive and active attacks destroy the availability of the certification services without threatening the system wide shared secret. In this paper, we consider another type of attack that threats the shared secret. A malicious node can also target other nodes. It may occasionally compromise and control one or a few well-behaving nodes through software bugs or system backdoors and get the sharing piece key of controlled nodes. Once no less than threshold nodes are compromised, the malicious node can rebuild the shared secret the broken sharing piece keys in hand. It means that the trust and security of the network has been cracked. It is the same that more than threshold nodes are compromised by different malicious node.

Intuitively, the larger the size of threshold T and the shorter the updating period P of the sharing secret, the more secure is the network. However, security is dynamic and relative in reality. In a given time interval, the more attacks the network received, the less secure the network is. In order to describe the relations of proper size of T, updating period P and attacks, we investigate the characters of attack process that the sharing secret scheme received firstly.

B. Attack process character

Many researchers focus on the attack processes, aiming at finding the characters of attack processes and modeling it in quantitative terms.

Kaaniche [10, 11] presented some empirical analysis and some preliminary statistical modeling of attack processes based on the data collected from the honeypot platforms deployed on the Internet. In the work, the probability distribution corresponding to the time between the occurrence of two consecutive attacks at a given platform can be characterized by a mixture distribution combining a Pareto distribution and an exponential distribution. The probability density function $pdf(t)$ can be defined as follows.

$$pdf(t) = p_a \frac{k}{(t+1)^{k+1}} + (1-p_a)\lambda e^{-\lambda t}. \qquad (1)$$

Where, k is the index parameter of the Pareto distribution, λ is the rate associated to the exponential distribution and P_a is a probability.

Another model was proposed by Jonsson and Olovsson [12]. They performed a practical intrusion test on a distributed computer system which consisted of a set of 24 SUN ELC diskless workstations connected to one file-server. All the attackers were supposed to be legal users of the system with normal user privileges and with physical access to all workstations except the file server. The intrusion process can be split into learning phase, standard attack and innovative attack phases. Most of the collected data can be related to the standard attack phase. For this phase, there is statistical evidence that the intrusion process could be described by an exponential distribution.

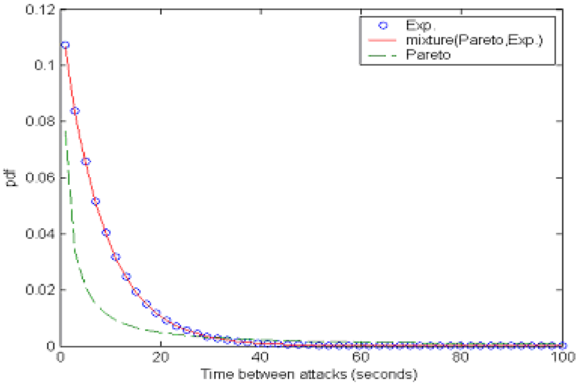

Fig. 1. Comparisons of different attacks pdf

The two different models were deduced from different experiment environments, one is Internet which is an opening network system, and the other is a specified system which can be seen as a closed network system. Both of them show that the intrusion process has the typical exponential distribution. Even in the mixture distribution model, we find that the weight Pa of Pareto distribution in mixture distribution varies from 0.0019 to 0.0115 in all the platforms of honeypot. It means that exponential distribution dominants the mixture distribution. In Fig.1, the probability density function (pdf) of the mixture distribution, Pareto distribution and an exponential distribution are compared according to (1). It seems that the mixture distribution is closer to exponential distribution than Pareto distribution.

C. Attack model

In this paper, we only consider the inside attacks by malicious nodes in MANET. These nodes are already in the system and have normal privileges of network resources. The network can be seen as a closed system similar to Jonsson [12]. So, we adopt the exponential distribution to approximate the time distribution between the occurrences of two consecutive attacks, and then attack process can be approximated by Poisson process.

In order to describe the attack process that sharing secret scheme received, we introduce the concept of Attack Stream firstly, and this is defined as follows.

Definition1 *(Attack Stream) Attack Stream is a counting process* $\{N(t), t \geq 0\}$*, which is time dependent.* $N(t)$ *denotes the number the system received in the interval [0, t), it is a nonnegative integer and a time continuous stochastic process and N(0)=0 i.e. no attack happened to the system.*

Let $N(t) - N(t_0) = N(t_0, t), 0 \leq t_0 \leq t$ denotes the attack numbers that system received in interval $[t_0, t)$. The system receiving m attacks in interval $[t_0, t)$, i.e. $\{N(t_0, t) = m\}$is an event, its probability is:

$$P_m(t_0, t) = P\{N(t_0, t) = m\}, m = 0, 1, 2, \cdots. \quad (2)$$

From the analysis above, attack stream $\{N(t), t \geq 0\}$ can be approximated by Poisson process with rate λ. The probability of m attacks arising during $[t_0, t)$ is as following equation:

$$P_m(t_0, t) = \frac{[\lambda(t - t_0)]^m}{m!} e^{-\lambda(t-t_0)}, t > t_0, m = 0, 1, 2, \cdots.$$

Particularly, considering the time interval $[0, t)$, we can obtain:

$$P_m(0, t) = \frac{[\lambda t]^m}{m!} e^{-\lambda t}, t > t_0, m = 0, 1, 2, \cdots. \quad (3)$$

For simplicity, we denote $P_m(0, t)$ with $P_m(t)$. The expectation of the Attack Stream $\{N(t), t \geq 0\}$ can be deduced from (3) on the assumption that:

$$E[N(t)] = \lambda t \quad (4)$$

Considering unit time $t = 1$, then $\lambda = E(N(1))$.

Definition2 *(Attack Intensity) Rate of Attack Stream* $\{N(t), t \geq 0\}$ *is called Attack Intensity.*

We can see that Attack Intensity is the expectation of the attack number that the system received in the unit interval. So the attack process is approximated by Poisson process with rate λ in MANET.

III. Dynamic Evaluation Model

Due to the protection and detection of the network, not all attacks can take effect and compromise nodes. We assume that each node may be compromised with probability p at each attack. Now we consider the probability distribution of the successful attack process.

Theorem1 *If the Attack Stream* $\{N(t), t \geq 0\}$ *is a Poisson process with rate* λ*, i.e. Attack Intensity, the successful probability that attackers crack a node is p at each attack, unsuccessful probability is 1-p. Let Y(t) denotes the number of nodes that attackers cracks successfully in interval [0,t), which is a Poisson process with rate* λ*, i.e. the probability that k nodes are cracked in the interval [0, t) is*

$$P_k(t) = P\{Y(t) = k\} = \frac{(\lambda pt)^k}{k!} e^{-\lambda pt}, k = 0, 1, 2, \cdots. \quad (5)$$

The result can be easily obtained according to Poisson process [9].

From (5), it is easy to obtain $P_k(0) = 0, k > 0$ which means that no node has been cracked at time $t = 0$ and the system is secure at that time for there is no attack to the system at present.So the Initializing Security Value is 1.

The model built according to (5) is called Security Dynamic Evaluation Model which gives the probability that k nodes are cracked at any given time. Obviously, the Attack Intension, the physical protection of the nodes and the cracked nodes' number play an important role in the security evaluation model. The model with different k, p and λ is shown in Fig.2. Fig.2 (a) shows that increasing the sharing threshold can enhance the security of system: lower cracked probability and longer security time. However, we can see that smaller p and λ only prolong the security time and the maximum probability still remain unvarying from Fig.2(b) and Fig.2 (c).

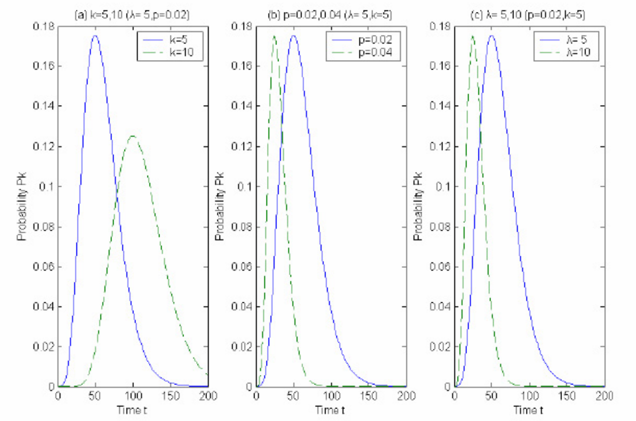

Fig. 2. Model with different *k*, *p* and λ

It's important to obtain the peak time through Theorem 1. The following theorem will show approaches to decide the threshold T and updating period P for a secure system.

Theorem2 *The probability that k nodes in the network have been cracked reaches maximum at time t at the given* λ *and p, where*

$$t = \frac{k}{\lambda p}. \quad (6)$$

Given threshold $k = T$, the updating period P of sharing secret should be less than $T/\lambda p$.

Proof: Differentiating from (5), we can obtain the peak time as follows:

$$P_k'(t) = \lambda p \frac{(\lambda pt)^{k-1}}{k!} e^{-\lambda pt}(k - \lambda pt), k = 0, 1, 2, \cdots. \quad (7)$$

Let $P_k'(t) = 0$, it is easy to obtain the unique extremum of (5) at time $t = k/\lambda p$, which is $\frac{k^k}{k!}e^{-k}$ as the maximum. ■

Equation(6) provides a convincing criterion to decide the risk time of the system under given condition. It is also clear that the occurrence time of the maximum probability decreases as λ and p increase linearly, but inverse ratio of k. It can be worked out from (6) that $t = 10$ when $p = 0.02, \lambda = 5$ and k=5, which shows that the probability that five nodes have been cracked reaches maximum at time $t = 10$ in a given interval [0, 24).

Theorem 2 provides the time of maximum cracked probability. We can obtain $k = \lambda pt$ from (6), so the threshold T of the system should be greater than k to resist the attack at that time.

Theorem3 *The threshold T of the system should be greater than* $k = \lambda pt$ *at the given attack stream and p, where:*

$$T = [\lambda pt] + 1. \quad (8)$$

[.] denotes integer function that round towards plus infinity. This can be deduced from (6) easily.

The administrator can predict the trend of the system security and the most dangerous time through theorem 2 and adjust the threshold value T according to theorem 3, which can help administer the network dynamically and securely.

IV. Evaluation of Distributed CA Schemes

In this section, we will discuss the influence of threshold value T on the security performance of the distributed CA scheme using the dynamic security evaluation model.

An attacker who wants to crack the network must crack no less than T nodes to recover the share secret of system. The probability of cracking no less than T nodes in time interval $[0, t)$ is:

$$P\{Y(t) \geq T\} = \sum_{k \geq T}^{n} \frac{(\lambda pt)^k}{k!} e^{-\lambda pt}. \tag{9}$$

Now, the probability of system security is

$$P_{sec} = 1 - P\{Y(t) \geq T\} = 1 - \sum_{k \geq T}^{n} \frac{(\lambda pt)^k}{k!} e^{-\lambda pt}. \tag{10}$$

The difference between the partial and full distributed CA schemes is the proportion of nodes holding the pieces of sharing secret. Every node in the full distributed scheme has the secret share of the CA secret key while only a part of creditable nodes in partial distributed scheme hold the secret share.

In the following, we discuss the security of the two schemes with the same threshold through an example. There are 40 nodes in the network and the parameters are selected as $\lambda = 5$, T=5 and p=0.04. There are 10 creditable nodes holding key pieces in the partial distributed scheme while each node in the full distributed scheme keeps a secret share. In the Fig.3(a), it is easy to see that the security of partial distributed scheme (n=10) is superior to the full distributed scheme (n=40) except the short time at the beginning. This result is coincident with the theoretical analysis in previous work.

Particularly if we select nodes with better physical protection as creditable nodes in the partial distributed scheme, the crack probability p of the nodes may be decreased more, which is shown in Fig.3(b). The partial distributed scheme (n=10, p=0.02) gains much more security than the full distributed scheme (n=40, p=0.04). In practical, since the nodes in the MANET are likely with different configuration, it is apt to select some robust nodes to share the TTP responsibility.

V. Conclusion

This paper presents a dynamic security evaluation model to the distributed threshold cryptography schemes in MANET. Using the stochastic process approach, Attack Stream and Attack Intensity are introduced to model the attacks that the network system received. The main assumption with reference of some previous work is that attack process can be approximated by Poisson process. Based on the attack model, a dynamic evaluation model is built to show the change trend of the security of the network under different conditions, and how to choose proper values of threshold and updating period of sharing secret. Finally, we evaluated and compare the security of two existing distributed CA schemes and verify the theoretical analysis of previous papers. As the distributed CA is an example of the secret share applications, the dynamic evaluation model here can be extended to measuring and evaluating other distributed TTP schemes in MANET. This evaluation model can help administrator master the dynamic security of the network and take measure in time. It may be useful in security design and construction for practical networks.

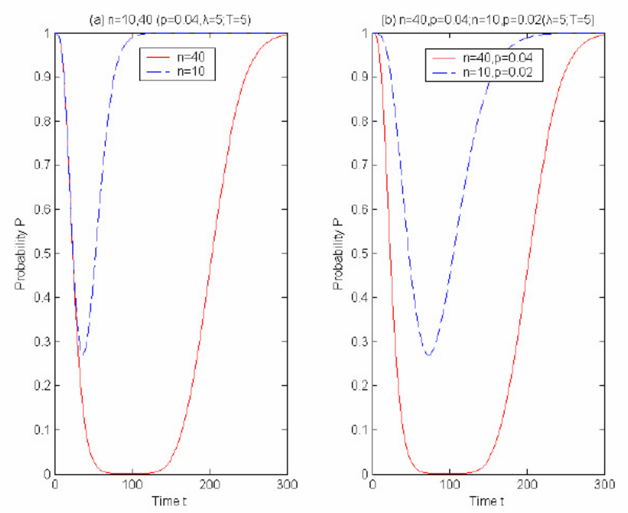

Fig. 3. Security of full and partial distributed CA schemes

Acknowledgment

This paper is supported by National High Technology and Development Program of China(863 Program)No.2009AA01Z423 and the Foundation of Key Laboratory of Communication and Information System(Beijing Jiaotong University).

References

[1] Shamir A.. How to share a secret. Communications of the ACM,1979, 24(11): 612-613.

[2] L. Zhou and Z.J. Haas. Securing Ad Hoc Networks. IEEE Network, vol. 13, no. 6, 1999, pp. 24-30.

[3] J. Kong et al.. Providing Robust and Ubiquitous Security Support for Mobile ad hoc Networks. Proc. 9th Int'l Conf. Network Protocols (ICNP 01), IEEE CS Press, Los Alamitos, Calif, 2001, pp. 251-260.

[4] H.Luo and Jiejun Kong, Petros Zerfos. URSA: Ubiquitous and robust access control for mobile ad hoc networks. IEEE/ACM Transactions on Networking, 2004. 12(6): 1049-1063.

[5] Kuang X, Lu X. Secure group communications for mobile ad hoc networks. Journal of Computer Research and Development, 2004, 41(4):704-710.

[6] Kaya T,Lin G,Noubir G,Yilmaz A. Secure Multicast Groups on Ad Hoc Networks. In:Proc. of the 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03),2003.

[7] Y. Dong, H. W. Go. Providing Distributed Certificate Authority Service in Mobile Ad Hoc Networks. Proc. of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005.

[8] Ning Hongzhou. Ad Hoc Network Security Measurement and Evaluation. IEEE, Proc .of ICEMI 2005, 2005.

Technical Report, 103, Lausanne: Swiss Federal Institute of Technology, 2001.

[13] Deb K, Pratap A, Agarwal S, Meyarivan T. A fast and elitist multiobjective genetic algorithm: NSGA2 Ⅱ. IEEE Transactions on Evolutionary Computation, 2002, 6 (2): 182-197.

[14] Perez-Guerrero, R.E. Cedeno-Maldonado, J.R., Differential evolution based economic environmental power dispatch. in: Power Symposium, 2005. Proceedings of the 37th Annual North American, pp. 191- 197, 23-25 Oct. 2005.

[15] Storn R, Price K. Differential evolution-a simple and efficient heuristic for global optimization over continuous spaces. Journal of Global Optimization, 1997, 11(4):341–359.

[16] Mayer D G, Kinghorn B P, Archer A A. Differential evolution - an easy and efficient evolutionary algorithm for model optimization. Agricultural Systems, 2005, 83(3): 315-328.

[17] Mendes Rui, Mohais Arvind, DynDE: A Differential Evolution for dynamic optimization problems Mendes. In: IEEE. Proceedings of the 2005 IEEE Congress on Evolutionary Computation (CEC'2005). New York: IEEE Service Center, 2005. 2808-2815.

[18] D. B. Das and C. Patvardhan, New multi-objective stochastic search technique for economic load dispatch," IEE Proc. Gen., Trans. Distrib., vol. 145, no. 6, 1998, pp. 747–752.

[19] M. A. Abido, A novel multiobjective evolutionary algorithm for environmental/economic power dispatch, Electr. Power Syst. Res., vol.65, 2003,pp. 71–91.

[20] M. A. Abido, A niched Pareto genetic algorithm for environmental/economic power dispatch, Electr. Power Syst. Res., vol. 25, no. 2, 2003,pp.97–105.

[21] T. F. Robert, A. H. King, C. S. Harry, Rughooputh, and K. Deb, Evolutionary multi-objective environmental/economic dispatch: Stochasticversus deterministic approaches, KanGAL, Rep. 2004019, 2004, pp.1–15.

TABLE III. BEST FUEL COST

	LP	MOSST	NSGA	NPGA	SPEA	NSGA-II	This Paper
P_{G1}	0.1500	0.1125	0.1567	0.1080	0.1062	0.1059	0.1083
P_{G2}	0.3000	0.3020	0.2870	0.3284	0.2897	0.2177	0.3265
P_{G3}	0.5500	0.5311	0.4671	0.5386	0.5289	0.5216	0.5299
P_{G4}	1.0500	1.0208	1.0467	1.0067	1.0025	1.0146	1.0123
P_{G5}	0.4600	0.5311	0.5037	0.4949	0.5402	0.5159	0.5013
P_{G6}	0.3500	0.3625	0.3729	0.2574	0.3664	0.3583	0.2580
Best cost	606.314	605.889	600.572	600.259	600.15	600.155	600.157
Emission	0.22330	0.22220	0.22282	0.22116	0.2215	0.22188	0.22176

TABLE IV. BEST EMISSION

	LP	MOSST	NSGA	NPGA	SPEA	NSGA-II	This Paper
P_{G1}	0.4000	0.4095	0.4394	0.4002	0.4116	0.4074	0.4094,
P_{G2}	0.4500	0.4626	0.4511	0.4474	0.4532	0.4577	0.4487
P_{G3}	0.5500	0.5426	0.5105	0.5166	0.5329	0.5389	0.5277
P_{G4}	0.4000	0.3884	0.3871	0.3688	0.3882	0.3837	0.3634
P_{G5}	0.5500	0.5427	0.5553	0.5751	0.5383	0.5352	0.5550
P_{G6}	0.5000	0.5142	0.4905	0.5259	0.5148	0.5110	0.5213
Best Emission	0.19424	0.19418	0.19436	0.19433	0.1943	0.19420	0.19419
Cost	639.600	644.112	639.231	639.182	638.51	638.269	638.285