Step3. From (10) calculate every ant's adaptness value, and then by (11) calculate every ant's pheromone thickness.

Step4. Randomly select *P* ants from ant colony, find out the optimal ant's position X_{best} based on the pheromone thickness of every ant's position. Set it up as individual target X_{obj}.

Step5. The non-optimal ants in the ant colony moving to target ant's position by (12) make the overall search.

Step6. The optimal ant make overall search according to its neighborhood.

Step7. Update every ant's pheromone thickness.

Step8. Confirm if satisfies its iteration termination condition, if so, then iteration terminates and outputs the optimal parameter (C, σ, ε); otherwise, return step4.

Step9. Apply the optimal parameter (C, σ, ε) and training sample to build up SVM prediction model.

V. THE ANALYSIS OF THE EXPERIMENTAL RESULTS

A. Experimental platform and data set introduce.

KDDCUP99 is formed from the IDS data set of MIT LL in 1998, which only contains network traffic data

- All data set: the training data set (kddcup.data.gz) ,the test data set. (kddcup.testdata.unlabeled.gz)
- 10 percect data set: the training data set (kddcup.data．10 percent．Gz) , the test data set. (kddcup.newtestdata.unlabeled 10 .percent .gz)
- Corrected.Gz is a test data set contain attacking mark, researchers can compare and analyze the results of their own algorithm test by using this data set.

This paper takes the 10 percent data set to analysis object. In the 10 percent data set offered by KDDCUP99 (including training data set and test data set), it contains 4 kinds of network attack types, which has obvious features in the MIT LL intrusion detection data: the training data set contains 23 kinds of aggressive behavior; test data set contains 38 kinds of aggressive behavior, the type of data sample and distribution is shown in TABLE Ⅰ.

TABLE I. KDDCUP99 DATA DISTRIBUTION

Type	**10% Rrain Set**		**10% Test Set**	
	Data	***Rate(%)***	***Data***	***Rate(%)***
Nomal	97 278	19.69	60 593	19.48
Probe	4 107	0.83	4166	1.34
DOS	391 458	79.24	229 853	73.90
U2R	52	0.01	228	0.07
R2L	1 126	0.23	16 189	5.20

B. The comparative analysis of the algorithm

Relate to neural network and traditional SVM algorithm, the ACO-SVM algorithm which improves the data sample of network intrusion detection shows a higher accuracy. the Contrasted results that several algorithms apply in training and test in the previous section selected shown in the TABLE Ⅱ.

TABLE II. THE EXPERIMENT'S RESULT

Type	***BP***	***N-SVM***	***ACO-SVM***
Categorised precision（%）	87.3	90.5	99.2
Training time（S）	13.4	12.4	5.6
Testing time（S）	0.93	0.86	0.79
Result tested	ordinary	good	better

The improved ACO-SVM makes separating hyperplane ant colony quickly find the right radial basis kernel function, makes the algorithm substantially higher than the pervious 2 kinds of methods for anomaly detection rate. while the training sample distribution law tends to test sample, the anomaly detection rate reached 99.2%

VI. CONCLUSION

This paper proposes a intrusion detection method based on improved ant colony algorithm which the SVM, the simulation results show that the method is quick convergent, less iteration, and can improve the accuracy of intrusion detection system to a certain extent. The above analysis shows that the ant colony algorithm is rapid, simple and precious in test, relative to the neural network algorithm and the traditional support vector machine algorithm in BP network study.

REFERENCES

[1] WANG Ze-long, YAN, Feng—xia and HE Feng, "A new SVM multi-class c1assification method based on error-correcting code[C] ", Suzhou : 2008 InternationalConference On Computational Intelligence and Security, 2008.

[2] Gjorgji Madzarov, Dejan Gjorgjevikj and Ivan Chorbev, "A multi-class SVM classifier utilizing binary decision tree[J] . Informatica , 2009(33) : 233—241.

[3] Song Guangjun, Zhang Jialin and Sun Zhenlong, "The research of dynamic change learning rate strategy in bp neural network and application in network intrusion detection[C]", 3rd International Conference on Innovative Computing Information and Control, Dalian,Liaoning:IEEE Press,2008:513-513.

[4] Wang Huiran and Ma Ruifang, "Optimization of neural networks for network intrusion detection[C]" , First International Workshop on Education Technology and Computer Science. Wuhan,Hubei, China:IEEE Press, 2009:418-420.

[5] Dorigo M.Optimization, "learning and natural algorithms[D]" , Italy:Ph.D.Thesis,Department of Electronics,Politecnico di Milano,1992.

[6] Dorigo M, Maniezzo V and Colomi A, "The ant system:optimization by a colony of cooperating agents[J]", IEEE Transactions on Systems, Man, and Cybernetics:Part B,1996,26(1):29-41.

[7] LIU Yi-guang, YOU Zhi-sheng and CAO Li-ping, "A novel and quick SVM—based multi-class classifier[J]", Pattern Recognition, 2006, 39(11) : 2258—2264.

[8] S C Lee and D V Heinbuch, "Training a neural－network based intru-siondetector to recognize novel attacks［J］", IEEE trans, on sys-tems, man, and cybernetics, 2001.294－299.

[9] K M C Tan, K S Killourhy and R A Maxion, "Undermining an anomaly based intrusion detection system using common exploits［J］", Raid, 2002. 16－18.