Applied Mathematics and Nonlinear Sciences

<https://www.sciendo.com>

A prediction model of urban counterterrorism based on stochastic strategy

Xiangwei Qi^{1,2,4}, Haifang Li², Bingcai Chen^{2,3}, Gulila Altenbek^{1,4,5,†}

¹ College of Information Science and Engineering, Xinjiang University, Urumqi 830046, Xinjiang, China

² College of Computer Science and Technology, Xinjiang Normal University, Urumqi 830054, Xinjiang, China

³ College of Computer Science and Technology, Dalian University of Technology, Dalian 116024, Liaoning, China

⁴ The Base of Kazakh and Kirghiz Language of National Language Resource Monitoring and Research Center on Minority Languages, Urumqi 830046, Xinjiang, China

⁵ Xinjiang Laboratory of Multi-language Information Technology, Urumqi 830046, Xinjiang, China

Submission Info

Communicated by Juan Luis García Guirao

Received November 27th 2020

Accepted February 26th 2021

Available online May 25th 2021

Abstract

With ever increasing complexity and intelligence of the modern cities, protecting key public facilities and important targets from any damage is a major challenge for the security sector. In all types of anti-terrorism prediction models, the prediction of attack behaviour is indispensable. Therefore, the attack behaviour model plays an important role in the anti-terrorism security system. This paper builds the attacker's behaviour model, and carries out the prediction about the possible attack behaviour by the attacker model based on random strategy. According to the attack strategies, analysis and construction of the attack tree and attack graph are carried out based on the state-based stochastic model. The paper describes the security system in detail taking use of the state-based stochastic model method, so as to clarify the state distribution and the transfer relationship between the states of various security resources after threatened by attacks. At the same time, this paper applies the state-based stochastic model to establish the attacker model through the impact of attack on the security system.

Keywords: urban counter-terrorism prediction; stochastic strategy; defensive strategy; attacker model

1 Introduction

With ever increasing complexity and intelligence of the modern cities, protecting key public facilities and important targets from any damage is a major challenge for the security sector. The terrorist attacks have caused

[†]Corresponding author.

Email address: gla@xju.edu.cn

enormous losses on China and even the world. According to the Global Terrorism Index published by the Institute for Economic and Peace (IEP), the annual economic losses caused by global terrorism are equivalent to the annual gross domestic product of many developing countries. In order to prevent attacks by terrorist organisations, it's necessary for the security sector to reasonably deploy the limited security resources. However, there are still many obvious defects existing in the manual management scheme. At the same time, the terrorist organisation will secretly observe the protection measures planned by security sector before carrying out an attack. Therefore, it is an urgent problem for the security sector to optimise the allocation of limited security resources.

In all kinds of anti-terrorism prediction models, the prediction of attack behaviour is indispensable. Therefore, the attack behaviour model plays an important role in the anti-terrorism security system. The attack behaviours are the intentional destructive behaviours launched by attackers, so that there is a cooperation and correlation between the events caused by the attack strategy in the security system. The attacks we observed may be random, but they tend to correlate with each other in a covert way. At the same time, the current attacks have strong concealment, and the new attack strategies are constantly emerging. Sometimes it is difficult for us to understand the characteristics of attackers in time. Therefore, it is an important subject in the security field of counter-terrorism to build a stochastic attack model to predict [1, 2].

During the process of establishing the stochastic model, in addition to accurately describing the stability of the security system, quickly solving and analysing problems is another important factor. However, some classical stochastic methods still have great limitations in these aspects, so that this paper not only establishes the stochastic model for urban anti-terrorism, but also simplifies and abstracts the model to facilitate the later application of the model. The reason why the security sector has many loopholes is because of the vulnerability of the security system, so the criminals aim at the fragile point of the security resource allocation and carry out the attack smoothly. The implementation of attacks may require multiple steps or cooperative attacks, so it is an important part to analyse the vulnerability of security resource allocation in the security evaluation. The urban anti-terrorism security model can be divided into the three sub-models, such as defender model, attacker model and security system vulnerability model, and they have three main connections. The first is the relationship between security system vulnerability and attacker, which is about a game between system vulnerability and attacker; Second, the relationship between defensive strategy and attacker, which is about the combination of randomness of defensive strategy and criminal attack strategy; and third, the relationship between defensive strategy and security system vulnerability, which is about the impact of defensive strategy and stochastic management scheme on the vulnerability of security system. Based on the establishment of the sub-models, there is a need to synthetically analyse the sub-models and obtain the comprehensive urban anti-terrorism security system model so as to evaluate the performance of the security resources in the real scene [3, 4]. Although the contents and emphases of above sub-models are different, their model objects are defensive policy behaviour models and attacker policy models related to security. Therefore, it can be classified into the same security model. The classical random method can be used in the system description, and simplify and abstract the model at the same time.

2 Classification of Random Strategy Models

In order to establish a suitable attack behaviour prediction model, it is crucial to meet two requirements. First of all, the model should be properly abstract, which depends on the category and purpose of the attack model. For an assigned target, determining the appropriate abstraction of the model depends on many factors, such as the behaviour characteristics of the defender. Second, the model shall include the key points of the behaviours of the defenders and the attackers, such as the relevant state of the model may be changed due to the attack behaviour, as well as the relevant state of the defender who may affect the attack behaviour. At present, there are more and more new attack methods and means, with randomness and diversity. Therefore, it's required to consider the following three characteristics of the attack behaviour description [5]. First, attack is a kind of

the intentional act, and security events show the randomness, but there may be hidden cooperative relationships. Second, attackers have strong learning ability and the skill to make decisions. At the same time, the knowledge and experience of attackers are also important factors for the attacks. Third, the attack is an interactive behaviour between attackers and defenders, and the attacker should find the vulnerabilities of the security system.

2.1 Model of Attacker

The attacker is the main body of the attack behaviour, and the model of attacker directly affects the performance of the security system. When the attackers launch the factitious attacks, they have to consider many factors, such as the attackers' experience, knowledge, attack intention and so on. We expect to get the security performance index of the security system in the attack and security damage, which can reflect the overall security performance in a certain period of time. To describe the behaviours of attacker should be based on statistical law and probability analysis. In addition, before and during the attack, the attacker may face a variety of decisions; usually select a plan with high success rate of attack and greatest damage to security [6, 7]. Therefore, the decision model of the attacker is also an important aspect of attack modelling.

2.2 Attack Behavioural Model

In the multi-stage attack model, the duration of some security events in each stage can be assumed to be an exponential distribution, and it is easy to adopt the state-based stochastic modelling method, and the security index can be obtained. Exponential distribution is the simplest and most effective assumption. For the attackers, the process of attack behaviour and its quantitative statistical law are analysed, and the behaviour of attackers is divided into three stages: learning stage, basic attack stage and innovation stage. At the learning stage, attackers collect and learn relevant knowledge to prepare for attacks. As attackers improve their skills, the time they spend in the learning phase will gradually decrease. In the basic attack stage, the attacker looks for security vulnerabilities and tries various feasible attacks means to carry out the attack. When the basic attack is tried, the attacker will enter a more complex stage of innovation. They will look for new attack methods and security vulnerabilities, and the success rate of attacks will continue to improve. Attackers with different experiences have different usage times in the three attack stages [8, 9]. The basic attack stage is the main body of the attacker's behaviour, and the duration of the attack event is assumed to be exponentially distributed, which makes it easy to refer to the classical trusted physical analysis technology, especially based on Markov process.

This paper divides the attack behaviour into several state stages from the influence of attack, and makes the behaviour of the defender and its interaction with the attacker abstractive. The attack potential is the potential ability of the attacker to successfully carry out a specific security penetration or attack. The attack potential is related to the initial authority, knowledge and experience of the attacker. Selecting appropriate state transfer rate for specific environment and evaluation target can obtain necessary safety index of course, abstract acquisition of model parameters is an important issue. Decision model is also an important branch of attack model. The decision of the attacker has an important influence in the attack model. The attacker tries to explore the vulnerabilities of the security system so as to maximise the impact. As mentioned above, the Markov decision process is introduced into the model to quantify and analyse the attacker's intrusion path. At the same time, the defender implements the security strategy to ensure that the key target can be protected, and the game relationship between the attacker and the defender is formed [10].

3 Attack strategy

This paper carries out the modelling analysis of the attack strategy from the aspect of detecting attack behaviour in the attack tree and attack graph and the state-based stochastic model.

3.1 Attack Tree and Attack Graph

Attack tree and attack graph are the most commonly used methods to describe attacks at present. Attack tree and attack graph models mainly focus on the problem of security damage to the target, and describe the set of events that can lead to the destruction of the security system. Therefore, it is possible to simulate all the attacks that a security system may suffer. Using attack tree and attack graph model to analyse the security of the system, it is mainly divided into three stages: generating attack tree and attack graph for specific security system and attack type, giving a specific value to each node in the graph, so as to calculate out the qualitative or quantitative security index. In the attack tree and attack graph model, we use a tree or graph structure to describe the attack on the security system. The root nodes show the attack targets, the leaf nodes show the different methods used to reach the targets, and the non-leaf nodes represent the sub-target of the attack, including two types of "and" and "or", respectively, representing the logical relationship between the sub-targets to be satisfied to achieve the attack target [11, 12]. For example, if the attackers would like to achieve the "and" node, they have to meet all corresponding sub-targets, while they only need to meet a sub-target to achieve "or" node. The nodes of the attack tree and the attack graph can be given all kinds of parameter values according to their needs, such as the Boolean value, the success rate, the cost and the possibility of the attack. Through the derivation and calculation of node values, the performance index of security system can be obtained. For "or" node, the calculation rule is to take the maximum value of all child nodes. On the contrary, it shall take the minimum value for "and" node. For example, give the success rate of node attack in the middle of attack tree, the probability of each sub-node and root node being attacked can be deduced according to the above calculation rules.

An attack tree model is shown in Figure 1, where each non-leaf node is a sub-target of the attack, and the node is assigned according to the probability and difficulty of the target success. Finally the probability of attack success can be estimated by the recurrence method from the bottom to top.

Fig. 1 Simulation of an Attack Tree Model.

3.2 State-based Stochastic Model

The state-based stochastic model method can describe the security system in detail and clarify the state distribution and the transfer relationship between the states of various security resources after threatened by attacks. By using the state-based stochastic model, we can build the attack model from the influence of the attack on the security system, which not only ignores some unknown behaviour details, but also does not affect the calculation of security evaluation. In addition, unknown attacks can be described and prevented from attack impact. In fact, unknown attacks have become the biggest threat to the current security field. At present, some people have tried to use the state-based stochastic model method to analyse the security of the network system, and to establish the running state set of the system and its transfer relationship under the condition of attack. It is usually assumed that the state residence time is exponentially distributed, so that the corresponding state-based stochastic model has the property of Markov [13, 14]. Based on the state model of Markov process, the Markov income model can be obtained as long as the different income values assigned to each state and other security indexes of the security system can be obtained. Markov chain and Markov income model have been widely used in the evaluation of system reliability.

However, the attacker has purposiveness actions in real scenes, and there may be a specific interrelationships

between security events, so that the assumption of exponential distribution is not necessarily reasonable at some time. In this case, we can do two things. One is to select the parameters reasonably, in order to approximate the exponential distribution. For example, to reasonably divide the attack into multiple phases, the time at each stage are assumed to have exponential distribution. The other thing is to select appropriate stochastic variables to characterise the attack behaviour. For example, broaden the residence time in some states to a PH distribution or general distribution; using a semi-Markov process model to build model for security system, and figure out the steady state probability, and calculate the related safety index. Using a semi-Markov process to describe a random model, that is, the residence time of the state is distributed randomly, and the state transfer point is memoryless [15, 16]. Model parameters include the average stay time of the state, showing $h=(h_g, h_{tr}, h_A, h_F)$ and the transfer rate matrix between states, showing P_{ij} . Among the formulae, $i, j \in \{G, TR, A, F\}$. First, solve the embedded chain, the steady-state probability distribution of discrete time of Markov chains is showed that $v=(v_G, v_{TR}, v_A, v_F)$. As a result, the steady-state probability of the semi-Markov process model can be expressed as:

$$\pi_i = \frac{v_i h_i}{\sum_j v_j h_j}, i, j \in \{G, TR, A, F\}$$

And the, the steady-state availability of the security system can be calculated as $As1-F$. From the orifice, "G" means the normal state in a complete attack, "TR" is the attack state, "F" is the attack success and "A" is the alarm information.

In the attack behaviour of real scene, the attack events are often not independent, and there may be interdependence or cooperative relationship between them. Therefore, it may encounter state space explosion issue to take use of three state-based stochastic model method to analyse large-scale security problems. To solve the state space explosion issue, two methods are always used [17]. One is to reduce the scale of the model by using the state explosion avoidance technology so as to avoid the emergence of the state space coal explosion problem, including the model level and the state level and so on. The second method is to put forward feasible processing techniques for inevitable state explosion to reduce the demand of state space in calculation by using special data structure, including higher level stochastic model method.

4 Evaluation of Attack Prediction Based on Stochastic Model

Based on the above prediction model of attacker behaviour, this paper analyses the possible attacks from different angles and directions, and compares the efficiency of the algorithm and the size of the total return value. We simulate not only the data such as the population density, time, distance and the probability value of resource coverage of the regional target "i", but also the attack situation of the regional target "I" and the previous attack. In different regions, we give the return value for the defender to successfully defend each area "I" and the penalty return value for failing to defend each area "I". Meanwhile, we assume that these return values is changeable every year, since with the increase in construction and development of the cities every year, the benefits are different for the attackers to attack each target "i". This also leads that the attack have the impact on the profits that the defenders get for defending each area "i". In terms of the analysis of the algorithm, this paper analyses the advantages of the algorithm through the three aspects namely the accuracy, the efficiency and the income. According to the experimental results, it can be inferred that the algorithm has some advantages for predicting the attacker model in terms of the efficiency of the algorithm or the income of the model.

Acknowledgements

This work was supported by Natural Science Foundation of Xinjiang Province (No.2018D01A28), Scientific Research Program of the Higher Education Institution of XinJiang (XJEDU2017M021), National Natural

Science Foundation of China (No.U1903215, 61363062), China Postdoctoral Science Foundation and Xinjiang Postdoctoral Science Foundation, Xinjiang University Research Foundation(No.BS180250).

References

- [1] Liu Xia, Han Ziqiang, Jin Shigen. "New Features and Development Trends of International Terrorism," *China Soft Science: Strategy and Decision*, No.11, pp. 5, Nov. 2015.
- [2] Wang Zhen, Yuan Yong, An Bo, Li Mingchu, Wang Feiyue, "A Review of Security Game Theory Research," *Journal of command and control*, vol.1, No.2, pp. 122-129, Jun 2015.
- [3] Chen Zihan, Cheng Guang, "A moving target defense technique based on Stackelberg-Markov nonreciprocal tripartite game model," *Chinese Journal of Computers*, vol.42, No.61, pp. 3, May 2019.
- [4] Dong Rui, "Dynamic complexity of Stackelberg model under different rational expectations," *System Engineering-Theory & Practice*, vol.37, No.7, pp.1761, Jul. 2017.
- [5] Wang Yuedi, Su Xing, Jia Yibin, Guo Limin, Ding Zhiming, "Journal of University of Science and Technology of China," *Computer Science*, vol.48, No.6, pp.465, June 2018.
- [6] Wang Shuai, Jiang Huawei, "Research on Application of Genetic-Ant Colony Algorithm in Path Planning of Emergency Materials," *Computer Applications and Software*, vol.35, No.9, September 2018.
- [7] Yue Feng, He Jianmin, Sun Yan, Liu Xiangdong, "Research on ant colony algorithm for emergency resource scheduling with stochastic path time," *Decision participation*, vol.15, No.32, August 2011.
- [8] Yang Jijun, Yu Lian, "Game Model and Optimization of Emergency Resource Scheduling for Multi-disaster Point Demand," *Chinese Journal of Management Science*, vol.24, No.8, pp.478-481, August 2016.
- [9] Wu Deng, Junjie Xu, Huimin Zhao. "An Improved Ant Colony Optimization Algorithm Based on Hybrid Strategies for Scheduling Problem," *IEEEAccess*, vol.7, February 2019
- [10] Wang Zhen, Yuan Yong, An Bo, et al. Review of Security Game Theory Research [J]. *Journal of Command and Control*, 2015, 1(2): 121-149.
- [11] Branislav Bosansky, Ji Cermak: Sequence-Form Algorithm for Computing Stackelberg Equilibria in Extensive-Form Games.
- [12] Paruchuri P, Pearce J P. Playing games for security: an efficient exact algorithm for solving bayesian stackelberg games[C]//*Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems(AAMAS'08)*. Estoril Portugal, 2008: 895-902.
- [13] Jain M, Korzhuk D. A double oracle algorithm for zero-sum security games on graphs[C]//*Proceedings of the 10th International Joint Conference on Autonomous Agents and Multiagent Systems(AAMAS'11)*. Taipei, Taiwan, 2011:327-334.
- [14] Jain M, Conitzer V. Security scheduling for real-world networks[C]//*Proceedings of the 2013 International Conference on Autonomous Agents and Multi-Agent Systems (AA-MAS'13)*. Bologna, Italy, 2013: 215-222.
- [15] Tambe M. Security and game theory: algorithms, deployed systems, lessons learned[M]. Cambridge University Press, 2012.
- [16] Tsai J, Rathi S, Kiekintveld C, et al. IRIS - A tool for strategic security allocation in transportation networks[J]. *Journal of Guangzhou Panyu Polytechnic*, 2015.
- [17] Shieh E, An B, Yang R, et al. PROTECT: a deployed game theoretic system to protect the ports of the United States[C]. *International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*. 2012: 13-20.