Resource Allocation to Information Security in Smart Cities Based on Evolutionary Game

Jun Li
Kai Zou
Shang Xiang
Zhen Wan
Lining Xing

Smart city highly relies on cloud computing, Internet of Things and other new technology means, which bring hidden information risk diffusion to urban information security. How to reasonably allocate current urban resources, avoid these information security risks as much as possible, and obtain the highest benefits, have become a practical problem to the current healthy development of smart cities. Based on the discussion of related concepts and technical theories, the information security resource allocation influencing factors index system is constructed from the following aspects: resources, threat sources, vulnerabilities and security measures. With the further analysis of information security factors and their affecting mechanisms, the basic theoretical framework of information security resource allocation is established based on the evolutionary game. The information security resource allocation problem is divided into the internal resource allocation and external resource allocation. External resource allocation is subdivided into complementary external resource allocation, alternative external resource allocation and weakly related external resource allocation. Under this framework, the subject relationship in various situations is analyzed. This research work can conduct a reasonable allocation of resources related to information security.

Keywords: smart city; information security; resource allocation; evolutionary game
Tob Regul Sci.™ 2021;7(4-1): 805-815
DOI: doi.org/10.18001/TRS.7.4.1.35

The concept of smart cities, originating from the field of media, refers to using a variety of new technologies or innovative concepts to effectively connect and integrate various systems and services through reasonable resource allocation in cities, so as to optimize urban management and improve life quality of residents [1-3]. Smart cities fully apply all kinds of new technologies (such as Internet of things (IoT), cloud computing, virtual reality, etc.) into all walks of life in cities [4-6]. By establishing the interconnection in broadband ubiquitous networks, integrating application of intelligent technologies and sharing resources widely, smart cities obtain com-prehensive and thorough perception abilities to realize fine and dynamic management of cities and effective improvement of life of residents [7-10].

Smart cities have been valued by countries all over the world since they came into being, which provide more convenience for people's life while improving the intelligent level of cities [11-13]. However, smart cities are highly dependent on new technologies including cloud computing and IoT [14-16], which brings a hidden danger of spreading the information risk while applying technologies and poses multi-facetted impacts on information security in cities [17-20]. How to reasonably allocate the current resources in cities to avoid the information security risk as far as possible and obtain the maximum benefits has become a practical problem that smart cities have to be faced in their healthy development [21-25]. Firstly, the relevant concepts and theories of resource allocation to information security in smart cities were introduced. Based on this, an index

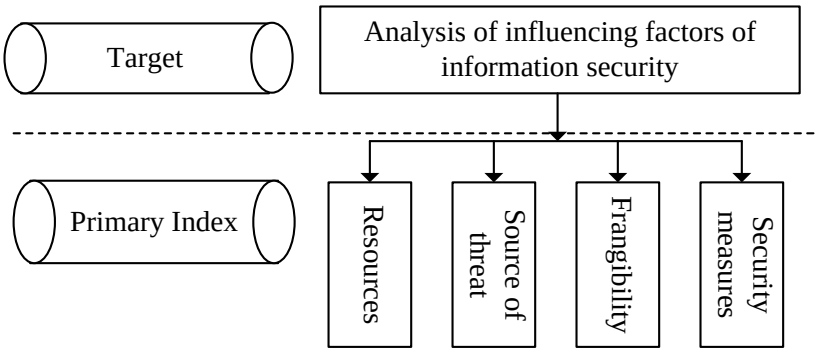
Jun Li School of Public Administration, Xiangtan University, Xiangtan 411105, P.R. China, Kai Zou School of Public Administration, Xiangtan University, Xiangtan 411105, P.R. China, Shang Xiang School of Public Administration, Xiangtan University, Xiangtan 411105, P.R. China, Zhen Wan* School of Public Administration, Xiangtan University, Xiangtan 411105, P.R. China, Lining Xing School of Software Engineering, Shenzhen Institute of Information Technology, Shenzhen 518172, P. R. China, School of Mathematics and Big Data, Foshan University, Foshan 528225, P.R. China, *Corresponding author: School of Public Administration, Xiangtan University, Xiangtan 411105, P.R. China*

system of factors influencing resource allocation to information security was established, mainly including four first-level indexes, nine second-level indexes and 31 third-level indexes [26]. These indexes all play an important role in the resource allocation to information security. Secondly, according to the actual situations, the resource allocation to information security was classified into internal resource allocation and external resource allocation in cities and the latter was sub-classified into complementary, alternative and weakly-correlated external resource allocation. Based on the evolutionary game theory, the basic theoretical framework of resource allocation to information security was established. In this framework, the relationships between subjects under various situations were analyzed.

INFLUENCING FACTORS INDEX SYSTEM

Comprehensive analysis on factors influencing resource allocation to information security and establishment of the corresponding index system are the bases for reducing the information security risk in smart cities in the context of big data. From the perspective of information security, the first-level indexes in the index system can be summarized into four aspects, namely resources, threat sources, vulnerability and safety measures by combining with the current situations of smart cities, as shown in Figure. 1.

Figure. 1
Factors influencing information security



Information Resources

There are many kinds of information resources, but it is evident that the higher the value of resources, the greater the risk may be faced in the actual situations. In accordance with relevant definitions of smart cities and information resources, the influencing factors of resources are sub-classified into three second-level indexes: management personnel, infrastructure and economic investment, that is, manpower, material resources and financial resources. By further analyzing the information security risk based on these indexes, the third-level indexes are obtained and the results are shown in Figure. 2. The number of management personnel for information security has an obvious impact on information security. By mastering network security skills, these personnel can provide a guarantee for information security in smart cities. Personnel quality is used as an index mainly because if management personnel do not abide by the rules and thus cause unauthorized access, it is easy to leave information out of control, thus affecting information security. In terms of core equipment, at present, most infrastruc- tures and key technologies for information security in China are still mastered by big companies in other countries, which brings a great security risk to a certain extent. There may be bugs and backdoors in some systems, so that the information is easily tampered or stolen. With the continuous development of the IoT, the IoT infrastructure is playing an increasingly important role in smart cities, supporting all kinds of application services in cities. When the IoT infrastructure is attacked, it easily leads to disclosure of personal privacy or leaking of business secrets, and even paralysis of the system. Equipment for wireless networks is also taken as an index mainly because WIFI, as an essential part of urban infrastructure, provides a lot of convenience for residents, but there is the risk of information leakage during data transmission. Application systems can directly affect the construction and development of smart cities, and their maturity reflects the level of information security in cities. Direct economic investment refers to the funds that cities directly invest in the construction of information security. Its proportion in the total output value and the amount of investment play a decisive role in the construction

and guarantee of information security to a great extent. Indirect economic investment mainly implies the additional construction funds for information security invested in other ways or for other purposes, which also provides a certain guarantee for the construction of information security.

Threat Sources

Threat is an objective factor that probably causes the potential risk for information security in smart cities. The influencing factors of a threat source are sub-classified into two second-level indexes, namely technological and management threats. By further analyzing the information security risk based on the indexes, the third-level indexes are obtained and the results are illustrated in Figure. 3. The physical environment is used as an index because the system operation may be interrupted by various external disasters, which results in the loss of some important data or files and increases the probability of the information security risk. As for software and hardware, its failure rate is mainly taken into consideration. Because the system of smart cities contains a large number of software and hardware, in the event of a fault, it may lead to service interruption or data damage and loss, resulting in the information security risk. In terms of data, data theft and tampering are mainly considered, which is the most prominent problem faced by smart cities at present. Collusion of service providers with lawbreakers for interest and intrusion of hackers will cause leakage of personal information and business secrets and some sensitive data are likely to be out of control, so that the confidentiality of data is difficult to be ensured. With regard to the management system, from the perspectives of preventing uncertain factors and unreasonable management systems, it is mainly risk-oriented and focuses on formulating reasonable regulations for medium- and high-risk systems to ensure the healthy development of information security in smart cities. Human threat is the security factor that is most difficult to control in the confirmation of threat sources. In many recent events, the integrity, confidentiality and availability of the information system are threatened all due to intentional or unintentional operation of insiders.

Figure. 2
Index system of factors influencing information security in smart cities based on resource value

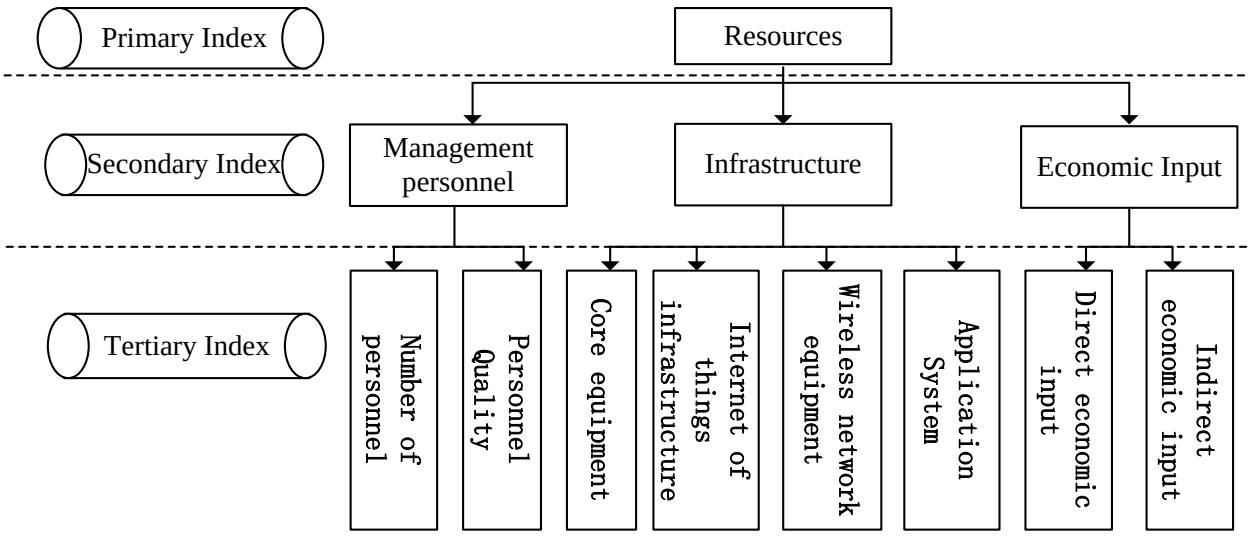
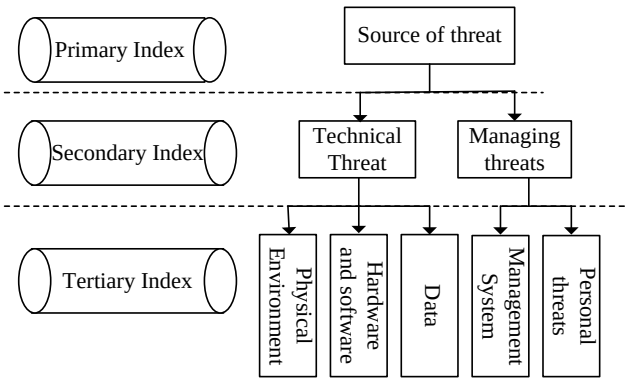


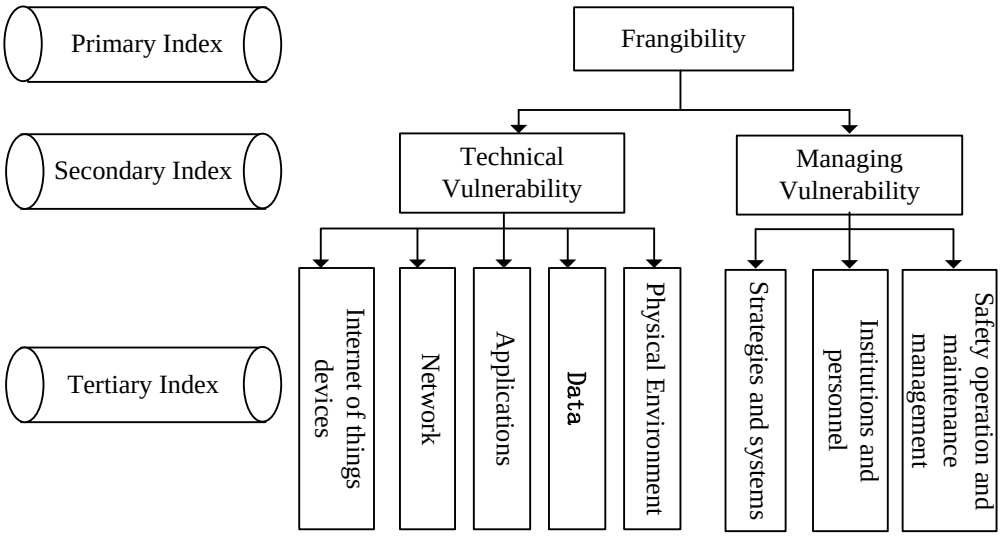
Figure. 3
Factors influencing information security in smart cities in the confirmation of the threat sources



Vulnerability

Vulnerability is considered mainly because in the context of big data, the defects of the information system in smart cities are threatened and taken advantages of, which renders the system possibly under risk of attack. The influencing factors of vulnerability are sub-classified into two second-level indexes: vulnerability in technology and management. The third-level indexes are obtained by analyzing the information security risk based on the above factors, and the results are demonstrated in Figure. 4. The IoT equipment is the basis of smart cities; however, a lot of important equipment has not been localized but relies on big companies in other countries to a large extent and is easily restricted. In the meanwhile, because the equipment is widely distributed in an open space, it is very vulnerable. As to the network, its system vulnerabilities, defects of network components, and incorrect configuration of the system are mainly taken into consideration. Preventing this potential threat can effectively guarantee the information security in smart cities. In terms of applications, there are numerous applications in smart cities, and many of them adopt open-source software, which brings a hidden danger for information security and renders them susceptible to malicious attack of lawbreakers. Data which are generated all the time in smart cities are very important for smart cities. However, various vulnerabilities easily appear in the process of data storage, transmission, access and encryption, which leads to data theft and tampering. As for the physical environment, the internal and external environment, supporting protection equipment and support equipment around are mainly considered. Strategy and system are considered mainly because it is the only way to standardize information security, formulate security strategies and management systems, and prevent and control the information security risk in the context of big data in smart cities. Organizations and personnel of security management can promote the effective development of information security, and ensure the stable operation of the information system. At the same time, to specific personnel, the protection responsibilities to prevent the information security risk can be assigned. With respect to security operation and maintenance management, with the continuous advancement of information security construction in smart cities, its importance is gradually valued. It is mainly aimed at the daily maintenance and management of information security. Once unstable factors are found, reasonable measures should be taken immediately.

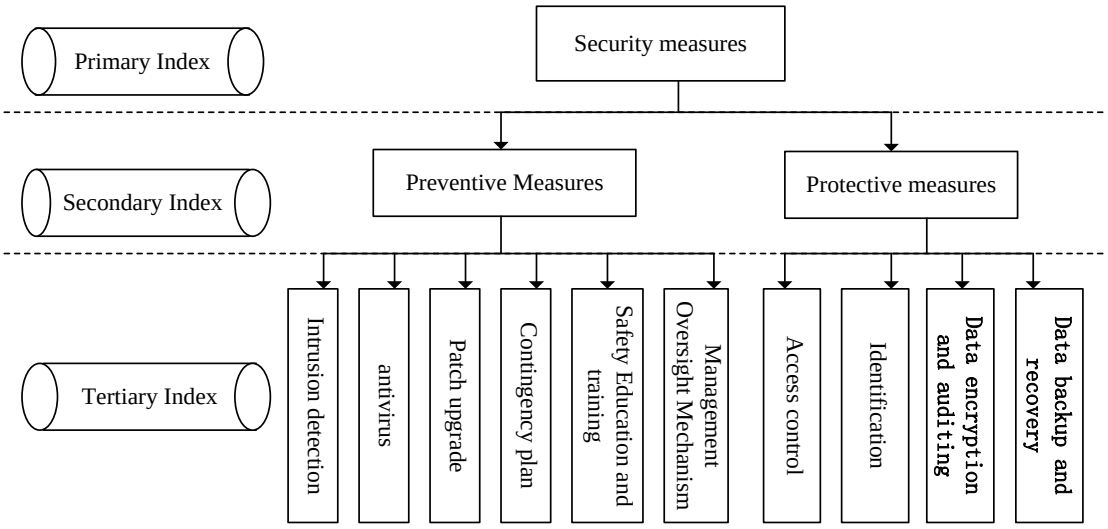
Figure. 4
Factors influencing information security in smart cities in the identification of vulnerability



Safety Measures

Safety measures are a barrier to protect information security in smart cities, which can effectively reduce risks of security accidents and vulnerabilities, and provide technical supports and management mechanisms for some resources. The influencing factors of safety measures are subclassified into two second-level indexes: preventive measures and protective measures, on which basis the information security risk is further analyzed to obtain the three-level indexes. The results are shown in Figure. 5. The intrusion prevention and detection, as an important part of information security, can effectively prevent network infrastructure from denial-of-service attack. Anti-virus software is taken as an index by mainly considering that network virus has become a high-risk field threatening information security, and a good way to prevent against network virus at present is to install anti-virus software with a strong anti-virus ability. However, since development of virus always precedes the anti-virus software, the coverage of the software is more important. Patch upgrading is selected as an index because it can effectively prevent occurrence of information security events in time when vulnerabilities of application software are emerging in an endless stream, resulting in diverse types of attack virus. Taking the emergency plan as an index is mainly because network information security events are often emergencies, which may cause huge losses. Therefore, formulating a reasonable emergency plan for information security can effectively reduce the information security risk. Safety education and training is mainly to enhance the ability of smart cities in identifying the information security risk through education of basic knowledge of public information security and cultivation of ability of professionals for information security. The management and supervision mechanism is selected mainly considering that the healthy and efficient operation of smart cities needs an orderly, standardized and unified management and supervision mechanism to assign safety responsibilities and avoid the system damage caused by unintentional or malicious behaviors of staffs. As for access control, it is used as an index because a lot of open interfaces of application programs in the system provide opportunities for illegal access, so the information security risk is controlled by setting the limit of authority of users to ensure that information is not illegally accessed. Identity authentication is also an effective prevention and control means for the information security risk. By identifying identities of accessors, the types of resources that they can access are prescribed, while the information beyond authority cannot be obtained by them. In the meanwhile, this also facilitates the accountability after information interception by visitors. Data encryption and audit is mainly to encrypt data in the context of big data, which can effectively prevent the information from being spied and ensure the integrity of data to a certain extent. Data backup and recovery is particularly important to ensure security of data. In case of system failure or data loss, the system can be restored to its original state immediately.

Figure. 5
Factors influencing information security in smart cities based on safety measures

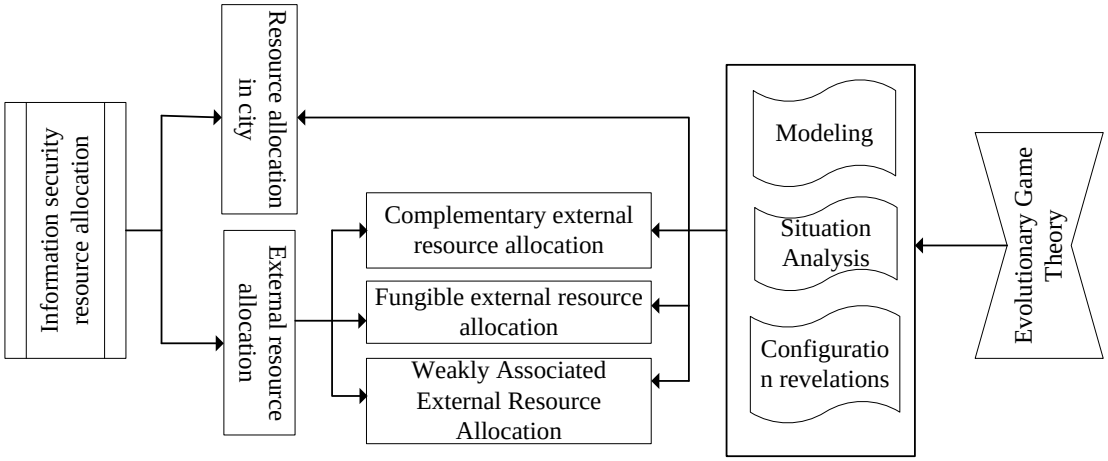


PROPOSED RESOURCE ALLOCATION METHOD

Basic Framework

With the constant development and progress in new technologies, such as artificial intelligence, big data, IoT, cloud computing and virtual reality, the development and construction of smart cities has been realized, but there are also great threats and challenges in information security. To effectively respond to these threats and challenges, by fully understanding the factors influencing resource allocation to information security, this study established a reasonable and effective theoretical framework of resource allocation to information security based on the current popular evolutionary game theory. The framework can play its due role in the protection of information security. By analyzing the index system of influencing factors in the above section, it can be seen that these common links including software and hardware, data, network, application, external environment and management are involved in all influencing factors in smart cities. In a city, how to plan the limited resources and avoid the restrictions of the above factors, so as to play the maximum efficiency of all resources and well protect the information security is one of the problems that need to be considered. For a city that has communication with the outside world, all internal resources therein are regarded as a whole, in which some external resources can complement, be replaced, and weakly correlated with internal resources. How to allocate the resources reasonably to improve the safeguard effects on information security is also an issue to be considered. In conclusion, the resource allocation to information security in a smart city is to analyze how to allocate internal and external resources of the city. According to the evolutionary game theory, the theoretical framework of resource allocation to information security was obtained, as displayed in Figure. 6.

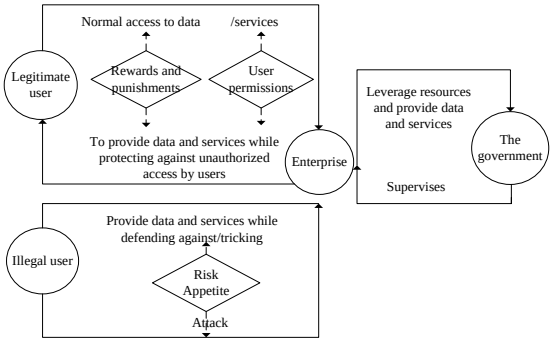
Figure. 6
Theoretical framework of resource allocation to information security



Internal Resource Allocation in Cities

In a city, subjects relating to information security are classified into enterprises, users and government, and users can be classified into legal and illegal ones. The relationship between subjects relating to information security is shown in Figure. 7. Enterprises, as undertakers of information security and providers of data and services, have certain relationships with the government and users. They provide a good enough guarantee of information security for the government and users to prevent illegal users from embezzling resources and provide normal data services for legal users (including the government). The government plays a certain role in supervising behaviors of enterprises through incentives and punishment measures; users decide their asset allocation by whether to buy products and services or not. Therefore, for enterprises, to realize their own interests, they have to consider both management and economy in combination and, choose and distribute various products and services relating to information security, so as to gain the best results with the least investment. As the users of information security, users can choose to legally obtain the data and services provided by enterprises, or illegally intrude into the information system to benefit themselves by stealing, spying or tampering data. The government is the supervisor and one of users of information security, which can not only obtain the data and services provided by enterprises, but also supervise enterprises through incentives and punishment measures.

Figure. 7
Relationship between subjects relating to information security in cities



Complementary External Resource Allocation

For the complementary external resources of a city, if the city is intruded by illegal users, the intrusion may not affect other cities. For example, the parts of a certain type of equipment are produced in Cities A and B. If illegal users only intrude into City A or City B, they cannot obtain the final assembly of the equipment. Only when the two cities are illegally intruded can illegal users obtain all the information of the equipment. This increases the difficulty in intrusion by illegal users, thus ensuring information security to a certain extent. However, in practice, enterprises relating to information security in the two cities may not be willing to cooperate with each other. Therefore, for the complementary external resources of the cities, resource allocation in the

non-cooperated and fully cooperated cases needs to be considered. In the meanwhile, the incentive agreements can be signed when enterprises cooperate, that is, if illegal attack to the enterprise in City A gets the enterprise in City B involved, the enterprise in City A needs to pay a certain compensation to the enterprise in City B. A relationship between subjects relating to information security of complementary external resources in cities is demonstrated in Figure. 8.

4.4 Alternative external resource allocation

For alternative external resources between cities, when illegal users intrude into City A, the incremental benefits of intruding into City B are much lower than its costs, indicating that the resources of the two cities are alternative. For alternative external resources, illegal users can obtain the required resources in any one of the cities, and then stop attacking immediately thereafter; on the contrary, if illegal users fail in attacking City A, they may continue to attack City B. For instance, City A (where certain equipment is produced) and City B (where the equipment is sold) are connected through the network, and City A can search information, such as inventory, sales volume and unit price in City B. If illegal users want to obtain the information, they can attack City A or City B. A relationship between subjects relating to information security of alternative external resources in cities is illustrated in Figure. 9.

Weakly Correlated External Resource Allocation

For weakly correlated external resources in cities, the benefit of information security is mainly achieved by sharing of information security. Cities can also reduce the input by information sharing. If cities A and B choose to share information, then they are able to learn information of illegal users, system vulnerability, and path upgrading of each other, thus informing relevant departments to make preparation in advance. If they do not choose information sharing, cities can only be engaged in construction of information security alone, which turns to internal resource allocation in cities. The relationship of subjects relating to information security of weakly correlated external resources in cities is shown in Figure. 10.

Figure. 8
Relationship between subjects relating to information security of complementary external resources in cities

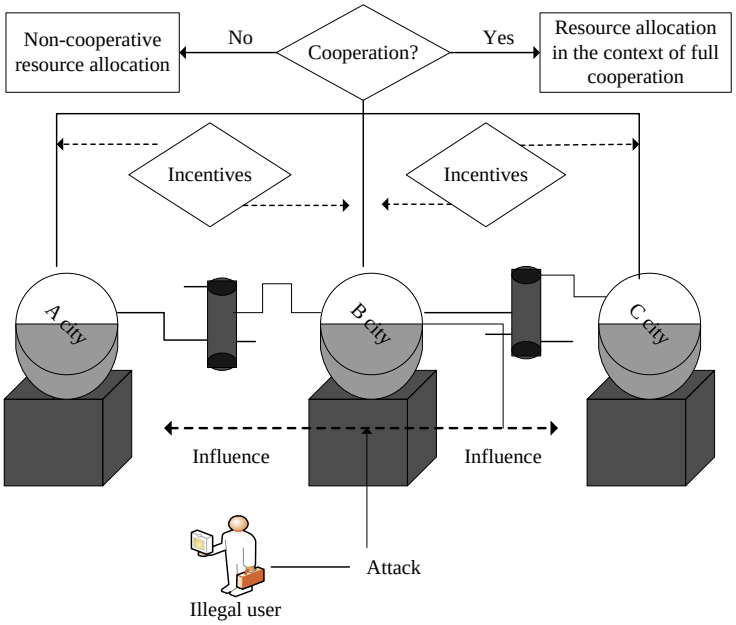


Figure. 9
Relationship between subjects relating to information security of alternative external resources in cities

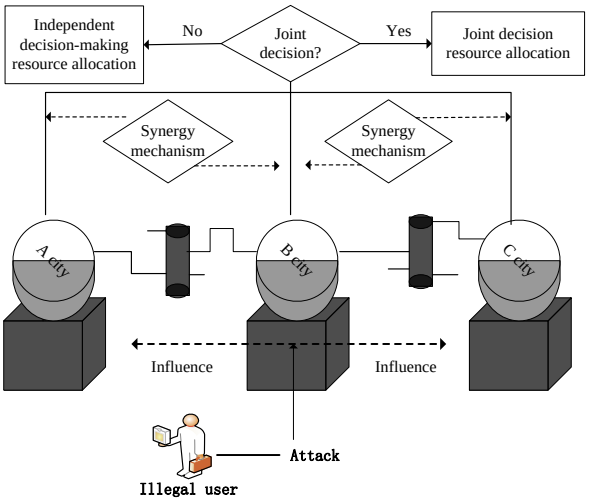
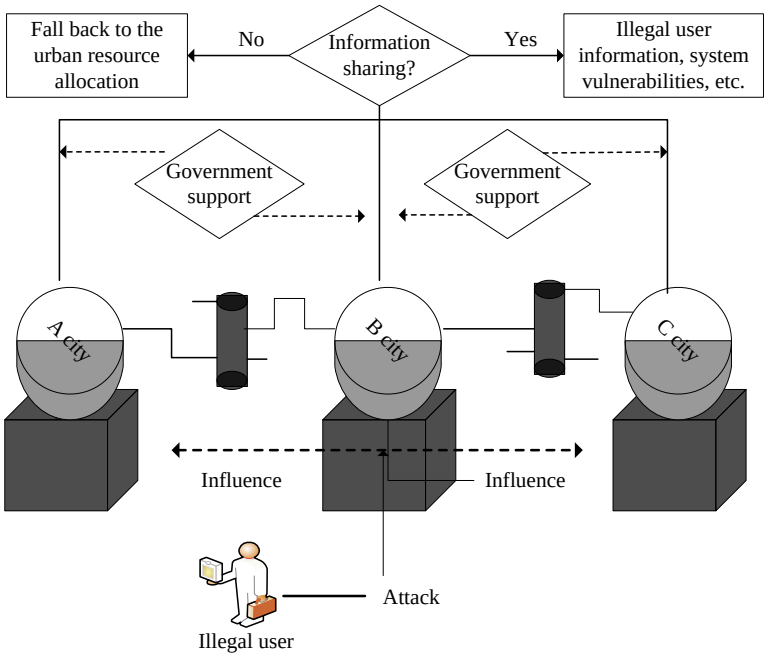


Figure. 10 Relationship between subjects relating to information security of weakly correlated external resources in cities



CONCLUSIONS

At present, the design of the majority of smart cities lacks overall consideration and faces large network security risks. Particularly, problems relating to information security have become an obstacle in the development of smart cities. How to reasonably allocate existing resources in cities and avoid these risks in information security as much as possible so as to gain the highest benefit has become a practical problem faced in the healthy development of smart cities. On the basis of discussing relevant concepts and technical theories, the research established the index system of factors influencing resource allocation to information security from aspects including resources, threat sources, vulnerability, and safety measures. The system includes four first-level indexes, nine second-level indexes, and 31 third-level indexes, which all play a significant role in resource allocation to information security. Furthermore, the factors and mechanisms that influence information security were analyzed and the basic theoretical framework of resource allocation to information security was built based on evolutionary game. The resource allocation to information se-

curity is divided into internal and external resource allocation in cities, and the latter can be sub-divided into complementary, alternative, and weakly correlated external resource allocation. Moreover, subject relationships under various circumstances were analyzed under the framework.

ACKNOWLEDGEMENTS

This research work is supported by the National Social Science Fund of China (No. 18BTQ055), the National Natural Science Foundation of China (61773120), the Youth Fund of Hunan Natural Science Foundation (2020JJ5149, 2020JJ5150) and the Innovation Team of Guangdong Provincial Department of Education (2018KCXTD031).

CONFLICTS OF INTEREST

The authors declare that they have no conflict of interest.

REFERENCES

1. Knapp K J, Marshall T E. Information security policy: An organizational-level process model [J]. Computers & Security, 2009, 28(7): 493-508.
2. Anjaria K, Mishra A. Relating Wiener's cybernetics aspects and a situation awareness model implementation for information security risk management [J]. Kybernetes, 2017, 47(1): 69-81.
3. Webb J, Ahmad A, Maynard S B, et al. A situation awareness model for information security risk management [J]. Computers & Security, 2014, 44: 1-15.
4. Ahmad A, Maynard S B, Park S. Information security strategies: towards an organizational multi-strategy perspective [J]. Journal of Intelligent Manufacturing, 2014, 25(2): 357-370.
5. Bojanc R. An economic modeling approach to information security risk management [J]. International Journal of Information Management, 2008, 28(5): 413-422.
6. Nazareth D L, Choi J. A system dynamics model for information security management [J]. Information & Management, 2015, 52(1): 123-134.
7. Houmb S H, Franqueira V N L, Engum E A. Quantifying security risk level from CVSS estimates of frequency and impact [J]. Journal of Systems & Software, 2010, 83(9): 1622-1634.
8. Feng N, Li M. An information systems security risk assessment model under uncertain environment [J]. Applied Soft Computing Journal, 2011, 11(7): 4332-4340.
9. Kong H K, Kim T S, Kim J. An analysis on effects of information security investments: a BSC perspective [J]. Journal of Intelligent Manufacturing, 2012, 23(4): 941-953.
10. Li S, Bi F, Chen W, et al. An Improved Information Security Risk Assessments Method for Cyber-Physical-Social Computing and Networking [J]. IEEE Access, 2018, 6(99): 10311-10319.
11. Basallo Y A, Senti V E, Sanchez N M. Artificial intelligence techniques for information security risk assessment [J]. IEEE Latin America Transactions, 2018, 16(3): 897-901.
12. Grunske L, Joyce D. Quantitative risk-based security prediction for component-based systems with explicitly modeled attack profiles [J]. Journal of Systems & Software, 2008, 81(8): 1327-1345.
13. Gusm OA , Silval CE, Silva MM, et al. Information security risk analysis model using fuzzy decision theory [J]. International Journal of Information Management, 2016, 36(1): 25-34.
14. Baskerville R. Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective [J]. Data Base for Advances in Information Systems, 2017, 49(1): 69-87.
15. Huang CD, Hu Q, Behara RS. An economic analysis of the optimal information security investment in the case of a risk-averse firm [J]. International Journal of Production Economics,2008, 114(2): 793-804.
16. Yong J L, Kauffman R J, Sougstad R. Profit-maximizing firm investments in customer information security [J]. Decision Support System, 2011, 51(4): 904-920.
17. Li J, Li M, Wu D, et al. An integrated risk measurement and optimization model for trustworthy software process management [J]. Information Sciences, 2012, 191(9): 47-60.
18. Benaroch M. Real Options Models for Proactive Uncertainty-Reducing Mitigations and Applications in Cybersecurity Investment Decision-Making [J]. Social Science Electronic Publishing, 2017, 4: 11-30.
19. Gao X, Zhong W, Mei S. Security investment and information sharing under an alternative security breach probability function [J]. Information System Frontiers, 2015, 17(2): 423-438.
20. Liu D, Ji Y, Mookerjee V. Knowledge sharing and investment decisions in information security[J]. Decision Support System, 2012, 52(1): 95-107.
21. Gao X, Zhong W, Mei S. A game-theoretic analysis of information sharing and security investment for complementary firms [J]. Journal of Operation Research Society, 2014, 65(11):1682-1691.
22. Gao X, Zhong W. A differential game approach to security investment and information sharing in a competitive environment [J]. IIE Trans, 2016, 48(6): 511-526.
23. Wu Y, Feng G Z, Wang N M, et al. Game of information security investment: Impact of attack types and network vulnerability [J]. Expert Systems with Applications, 2015, 42(15-16): 6132-6146.
24. Wang Q, Zhu J. Optimal information security investment analyses with the consideration of the benefits of investment and using evolutionary game theory [C]. Proceedings of the International Conference on Information Management, 2016: 957-961.
25. Qian X, Liu X, Pei J, et al. A game-theoretic analysis of information security investment for multiple firms in a network [J]. Journal of Operational Research So-

ciety, 2017, 68(10): 1-16.
26. Wang Gaihua, Zhang Tianlun, Dai Yingying, Lin Jinheng and Chen Lei. A Serial-Parallel Self-Attention Network Joint With Multi-Scale Dilated Convolution, IEEE Access, 9(5), 2021: 71909-7191. DOI: 10.1109/ACCESS.2021.3079243