Expert Systems With Applications 64 (2016) 11–23

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Optimizing security and quality of service in a Real-time database system using Multi-objective genetic algorithm

Xuancai Zhao, Qiuzhen Lin*, Jianyong Chen, Xiaomin Wang, Jianping Yu, Zhong Ming

College of Computer Science and Software Engineering, *Shenzhen University*, *Shenzhen*, *P.R. China*, *518060*

ARTICLE INFO

Article history:
Received 3 June 2015
Revised 16 July 2016
Accepted 17 July 2016
Available online 18 July 2016

Keywords:
Multi-objective optimization
Genetic algorithm
Network security
QoS

ABSTRACT

Both network security and quality of service (QoS) consume computational resource of IT system and thus may evidently affect the application services. In the case of limited computational resource, it is important to model the mutual influence between network security and QoS, which can be concurrently optimized in order to provide a better performance under the available computational resource. In this paper, an evaluation model is accordingly presented to describe the mutual influence of network security and QoS, and then a multi-objective genetic algorithm NSGA-II is revised to optimize the multi-objective model. Using the intrinsic information from the target problem, a new crossover approach is designed to further enhance the optimization performance. Simulation results validate that our algorithm can find a set of Pareto-optimal security policies under different network workloads, which can be provided to the potential users as the differentiated security preferences. These obtained Pareto-optimal security policies not only meet the security requirement of the user, but also provide the optimal QoS under the available computational resource.

1. Introduction

Database systems are widely used in today's computer system, which are adopted for storing and accessing data in various application services (Andres, Jose, Ernesto, & Alfredo, 2013; Hababeh, Khalil, & Khreishah, 2015; Tang, Li, Jiang, & Chen, 2014). With the expansion of database application fields, the new applications not only need to maintain a large amount of shared data, but also keep the data fresh for the transaction, such as data communications, e-commerce, and real-time simulation. For traditional database system, it is designed to process the permanent, stable data, and maintain the integrity and consistency of data. Its performance targets mainly focus on the high throughput and the low cost of system. Whereas, a real-time database is designed to use the real-time processing, such that it can handle the workloads whose state is constantly changing (Laura, Jorge, & Viviana, 2005).

With the widespread use of database systems, they are exposed to more and more internal and external threats (Al-Sayid & Aldlaeen, 2013; Poolsappasit, Dewri, & Ray, 2012), as the data stored in databases always involve much sensitive information, such as personal privacy, bank information and commercial secrets. More and more real-time services in database are required, which will highly impact the quality of service (QoS). Real-time database system has become the basis of enterprise information data platform, which is used to process the real-time transaction data for the e-commerce system of the enterprise, to simulate and monitor the system performance for simulation system of the laboratory or to storage historical data for data sharing platform and so on (Laura et al., 2006). Since the mutual influence between network security and QoS, there is a growing interest to figure out their actual relationship on database systems. For example, with the increasing use of the real-time network application services that contain sensitive information, it is required to provide the adequate security service for maintaining the users' security and high QoS to satisfy the real-time requirements.

In most cases, security and QoS are investigated independently. On the improvement of QoS, over the past decades, a lot of research studies on the QoS of real-time database have been conducted (Amirijoo, Hansson, & Son, 2006; Kang, Oh, & Son, 2007a; Kang, Son, & Stankovic, 2004; Woochul, Son, & Stankovic, 2012). Traditional security mechanisms such as access control mechanisms (Bertino & Sandhu, 2005; Parmar, 2014) and policy enforcement mechanisms (Jabbour & Menasee, 2008; Jabbour & Menasee, 2009) are not sufficiently secure for database system, as the anomaly detection mechanisms are required to protect database system against the potential threats such as SQL injection and impersonation attacks (Kamra & Bertino, 2009; Srivastava, 2014). Thus, intrusion detection and prevention systems (IDPSs)

* Corresponding author.
E-mail addresses: zhaoxcszu@gmail.com (X. Zhao), qiuzhlin@szu.edu.cn (Q. Lin), jychen@szu.edu.cn (J. Chen), wangxm@szu.edu.cn (X. Wang), yujp@szu.edu.cn (J. Yu), mingz@szu.edu.cn (Z. Ming).

http://dx.doi.org/10.1016/j.eswa.2016.07.023
0957-4174/

Table 1
The contributions of the references regarding the improvement of security and QoS.

References	Contributions	Category
Amirijoo et al., 2006; Kang et al., 2004	Feedback control has been applied to real-time database to maintain data freshness for the timeliness of transactions in dynamic workloads.	the improvement of QoS
Woochul et al., 2012	By controlling both I/O and CPU resources, the proposed approach supports both the timeliness of transactions and the high data freshness in real-time database.	
Bertino & Sandhu, 2005; Jabbour & Menasee, 2008; Jabbour & Menasee, 2009; Parmar, 2014	Their researches illustrate that the traditional security mechanisms such as access control mechanisms and policy enforcement mechanisms are not sufficiently secure for database system.	the improvement of security
Kamra & Bertino, 2009; Srivastava, 2014	The anomaly detection mechanisms are used to protect database system against the potential threats such as SQL injection and impersonation attacks.	
Darwish et al., 2013; Rao et al., 2014; Saad et al., 2012	IDPSs have been extended to protect database system from malicious intrusions.	
Taneja et al., 2011	It illustrates that network security services in some application cases will consume resources and reduce the resource allocated to QoS.	the relationship between network security and QoS
Chen et al., 2009	The research shows the impact of security on QoS in communication network.	
Nieto & Lopez, 2014	A context-based parametric relationship model (CPRM) is provide to measure the security and QoS tradeoff in configurable environments.	
Alomari & Menasce, 2012	A single-objective optimization model based on the database platform is designed to optimize network security and QoS.	

have been used to complement the traditional security model in database system. IDPSs have been recently extended to protect database system from malicious intrusions (Darwish, Guirguis, & Ghozlan, 2013; Rao, Singh, Amin, & Sahu, 2014; Saad, Mahdi, & Zbakh, 2012).

However, the database system needs the security service and QoS simultaneously. Both network security and QoS consume computational resource and thus may affect the performance of application services. When high QoS is required, less available resources are provided to network security service. On the other hand, network security services are demanded to reach high level in some application cases, which will consume more resources and may greatly reduce the resource allocated to QoS (Taneja, Raman, & Gupta, 2011). Therefore, some researchers start to study the relationship between security and QoS in recent years (Chen, Hu, Zeng, & Zhang, 2009; Kashif, Madjid, Shi, & Sohail, 2013; Mostafa, Pal, & Hurley, 2014; Nieto & Lopez, 2014). A single-objective optimization model is designed in (Alomari & Menasce, 2012) based on the database platform, which uses intrusion detection system to guarantee the system security. A linear weighted method is used to convert the security and QoS as the global utility, and then a traditional climbing algorithm is performed to find out the combination of IDPSs configuration with maximum global utility. However, this linear relationship between security and QoS is not studied in detail and the users cannot simply select the IDPSs configuration according to either security or QoS. The main contributions of the above mentioned algorithms are clearly listed in Table 1.

Depending on the nature of the applications, their security requirements for the same user may be different. For example, trading online always needs high security requirements while watching video in internet only requires low security configuration. Moreover, different security requirements even for one application may be demanded by different users. For example, when users access a database, high security strength is asked for the user with root privilege while low security strength is provided for the user with visitor privilege. Due to the need of differentiated security, database system has to provide a set of optimal security solutions, which can satisfy the request of different security strength and maintain high QoS. Without any further information, these optimal solutions integrating the requirements of security and QoS are termed Pareto-optimal solutions (Bayon, Grau, Ruiz, & Suarez, 2012; Wang, Li, Yen, & Song, 2014), which indicate that no any other solution is better than them in both QoS and security. By this way, the database system has to find the representatives of Pareto-optimal solutions, which can be served as the available solutions for various requirements. Such that, users can select one Pareto-optimal solution to configure security mechanisms based on their preferences. However, even with the optimal settings of security and QoS in database system, real-time monitoring the required security and QoS parameters is a tremendous pressure for the system administrator who has lots of other work to monitor the performance parameters and run the optimal approach manually in a dynamic environment (Alomari & Menasce, 2012). To solve the aforementioned problem, autonomic system is a promising technique, as it is capable of self-management by self-configuring, self-optimizing, self-protecting and self-healing with feedback loops (Menasce & Kephart, 2007). Inspired by the autonomic computer system (Bennani & Menasce, 2005) designed by queuing networks models (Kleinrock, 1975; Menasce, 2004), it is also able to provide an automatic configuration for both security and QoS in database system.

Therefore, in this paper, an autonomic model for real-time database system is designed, which is aimed at optimizing QoS and security by dynamically changing the security configurations according to the requests from users. It is noted that, although the key indicators of QoS includes delay (the response time), jitter and packet loss rate, this paper mainly considers the relationship of the response time and network security in order to simplify the multi-objective model. The main reason to select the response time as the quantitative evaluation of QoS is mainly based on the facts that, relatively high response time is generally required in some application systems with real-time databases, such as maintenance management and expert systems. Moreover, the extra delays can also be easily captured by the uses and greatly affect the user experience when they use some resource-constrained terminals, such as networking terminals and handheld devices. After that, a classical multi-objective genetic algorithm (NSGA-II) is revised to get the Pareto-optimal sets of our model, as NSGA-II has demonstrated the effectiveness in solving many practical engineering problems (Martins, Carrano, Wanner, Takahashi, & Mateus, 2011; Metaxiotis & Liagkouras, 2012; Rubio-Largo, Vega-Rodriguez, Gomez-Pulido, & Sanchez-Peerez, 2012; Sengupta, Das, Nasir, Vasilakos, & Pedryc, 2012; Shaygan, Alimohammadi, Mansourian, & Govara, 2014). These Pareto-optimal solutions obtained by autonomic controller with NSGA-II can guarantee the security and the delay of the service within an acceptable range. Users can select one of