IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Security & Concurrency control in Real-Time Database Systems: A Survey

Ebrahim Abduljalil[1], Dr. S.B. Thorat[2]

Ph.D candidate, School of Computational Science, SRTM University, Nanded, Maharashtra, India[1]

Director, Institute of Technology and Mgmt, Nanded, Maharashtra, India[2]

Abstract: Real-time Database Systems (RTDBS) ought to fulfill timing constraints related to transactions. Usually, a timing constraint is stated as a deadline, which is characterized as a necessity to be utilized by schedulers. Currently, security becomes another significant challenge in several real-time systems. In many systems, sensitive information is expressed by numerous users with various levels of security clearance. More complicated database systems are now being employed in applications that need to support timeliness while coping with sensitive information. Key issues of real-time developers have been addressed in this paper. Furthermore, an extensive survey of real-time systems research has been presented. The survey classification of the proposed mechanisms has been proposed based on the security and concurrency control in RTDBS.

Keywords: Real-Time, security, concurrency control, transaction.

1. INTRODUCTION

RTDBS is considered a database system that has the same features of traditional database system such as concurrency control and data independence, but at the same time enforces real-time constraints that applications may have [1].

There is a different between the Traditional database systems and a RTDBS in many features. RTDBSs have different correctness conditions, applications assumptions, and performance goal. RTDBS can be evaluated by the rate of transactions that didn't meet their deadlines, the average delay of late transactions and the cost of missing the deadlines of transactions.

In addition to maintaining data consistency, timing constraints associated must satisfy with transactions in Database systems for real-time applications. Beside real-time requirements, security is required in a lot of applications. In this paper, we address the key issues to be considered in real-time developers. Furthermore, we present an extensive survey of current real-time systems research. We classify the proposed mechanisms based on the security and concurrency control in RTDBS.

2. REAL-TIME DATABASE SYSTEMS

We can get from conventional database systems the requirements of correctness expanded by RTDBS. In real-time systems Transactions must meet the constraints of their timing, to be correct it. It's expressed as deadlines, [2]. Another important requirement in many real-time applications is security. With different levels of security clearance, the system keeps sensitive information to be shared by multiple users. Since more of such systems are used, one cannot neglect the need for integrating them [2].

3. SECURITY IN RTDBS

Recently, security has become a significant key issue in real-time applications. Thus, more research work has proposed in security issue under real-time database, as following:

K-D Kang and S. Son [3] proposed a novel adaptive method for security support. In this method a RTES primarily uses a short cryptographic key to maximize the QoS. When the length of key increases, the level of security risk will be increased. So, a possibility of cryptanalysis of magnitude harder can be made by demanding the attacker to found out the larger key space, while meeting all deadlines by degrading the QoS in a controlled manner. By an offline polynomial time algorithm, they derive the suitable QoS levels for several key lengths to minimize the overhead. When the risk level appears online, a longer key can be used and adapted to the corresponding QoS level (derived offline) by a real-time task in O(1) time.

Kyoung-Don Kang et al. [4] presented a novel real-time database architecture for secure transaction processing with certain miss ratio guarantees. In a simulation study, they showed that their approach can significantly improve the miss ratio compared to several baselines, while supporting the mandatory access control mechanism based on Bell-LaPadula model and the notion of non-interference to prevent the illegal direct/indirect information transfer between different security classes. According to the performance evaluation results, their approach was able to support the specified average/ transient miss ratio.

Binto George and Jayant Haritsa [5] proposed and assessed a novel dual method to secure transaction concurrency control which permits the real-time database system to use different concurrency control mechanisms at the same time for guaranteeing security. It also helps to improve real-time performance. Unlike other studies, which used a tradeoff approach between security and timeliness, they considered security as an all-or-nothing"

issue, that is, as a correctness criterion. Their experiments showed that, under normal loads, the overall miss percent of the secure system is worse than that of the direct system, whereas under heavy loads, it is the other way around.

In their work, Ahmed h. Omari et al, [6] a new cryptographic algorithm is improved to develop the time for encryption and decryption of data of end-to-end delay and provide higher level of security. The work that is in their paper tries to establish a new encryption/decryption method. This method enhances a minimum delay time that makes it suitable for RTA. Moreover, it offers high level of security by choosing a key length of 1024-bitlong. Another interesting property of the algorithm is the skill of using a new different key for every packet. Through a trusted agency, the distribution of the encryption keys is usually carried out. Their results start in a significant delay before the real time application.

Kyoung-Don Kang and Sang H. Son [7] proposed a novel approach for systematic security and timeliness tradeoffs based on the concept of the strength of defense. Their approach is not only meet real-time constraints but also provides desirable security and system properties in RTESs. In the simulation study, their approach significantly improves the success ratio under overload.

Multilevel secure database systems have a set of supplies. They are away from those of conventional database systems. A number of conceptual models exist which specify the access rules for transactions in secure database systems. Another significant model is the Bell-LaPadula model [2].

Chanjung Park and Seog Park [8] proposed a new concurrency control protocol for multilevel security (MLS) /RT DBMSs. Their protocol satisfies MLS properties and ensures no priority inversion. They classified transactions by their operations and discussed the conflicting natures in MLS/RT DBMSs.

Sang H. Son et al. [2] offered the idea of requirement specification which allows the system designer to identify important properties of the database at an appropriate level. They presented policies to allow the union of security and real-time requirements in database systems. The definition of partial security is a key part of this union.

Rasikan David et al. Sang H. Son [9] presented a scheme to permit partial violations of security for developed timeliness. The capacity of the resultant covert channel is derived. Moreover, a feedback control scheme is offered that does not permit the capacity to surpass a definite upper bound.

Kyoung-Don Kang and Sang H. Son [7] claimed that multilevel security requirements are due to the conflicting goals of each requirement. Trade-offs need to be made between security and timeliness. They defined capacity, a measure of the degree to which security is being satisfied by a system.

Sang H. Son et al. [10] proposed a security manager featuring adaptability and multilevel security services. They demonstrated that the concept of adaptable multilevel security can be applied in a soft real-time environment to achieve performance gains. Test results show that a 100% adaptable system can make deadline completions twice at the rate of a similar system without adjustable security.

Son et al. [11] defined mutual information as a measure of the degree to which security is being fulfilled by a system. After that a secure two-phase locking protocol is described. Then a scheme is presented to permit partial violations of security for developed timeliness. A feedback control scheme is proposed that does not allow the mutual information to exceed a specified upper bound and analytical expressions for the mutual information of the resultant covert channel are derived. Results showing the efficacy of the scheme are obtained through simulation experiments which are also discussed.

4. CONCURRECY CONTROL IN RTDBS

In RTDBS, timeliness is the main performance measure. Scheduling of transactions is driven by priority order. Given these challenges, many researches has recently contributed in designing CC methods for RTDBSs and in evaluating their performance. Most of these methods are based on one of the two basic concurrency control mechanisms: optimistic or locking concurrency control.

4.1 Optimistic CC

Quazi N. Ahmed and Susan V. Vrbsky [12] showed the covert channel property of secure RTDBs and they proposed a new secure optimistic concurrency algorithm based on this property. Results clearly show that their algorithm performs fairly well in terms of security and timeliness compared to the non-secure algorithm. They also showed that achieving security does not necessarily mean much sacrifice in real-time performance. It possible to made a system totally covert channel free, but can still have a low percentage of deadline miss for an arrival rate as high as 20.

Maysam Hedayati et al. [13] presented concurrency control algorithm for secure real-time databases, which the Secure OPT algorithm employ use the properties of an optimistic concurrency protocol. Results showed that the algorithm achieves fairly well in terms of security and timeliness match up to a non-secure algorithm. They proved that more security does not essentially mean more sacrifice in real-time performance.

Shiby Thomas et al. [14] presented new database system architecture in which real- time transactions use optimistic CC and at the same time standard transactions use locking. They proved that their architecture maintains data integrity and through a simulation study, they showed that it provides significantly improved performance for the standard transactions without diminishing the real-time transaction performance. They also showed, more generally, that the proposed architecture correctly supports the coexistence of any group of concurrency control algorithms that adhere to a standard interface.

Byeong-Soo Jeong et al. [15] presented based on an optimistic approach a secure real-time CC scheme. Their protocol solves the conflict between real-time constraints and security requirements by maintaining multiple data

versions, and it ensures serializability by suitably marking conflicting transactions and letting their continuously proceed with the correct data versions. They compared it with PSMVL the existing method based on a locking approach, to assess the characteristics of its performance.
Their experiments show that an optimistic approach gives performance better than the performance that is given by the locking approach when there is high data contention. That is because the forward validation of an optimistic method has an ability to minimize the unnecessary restarts to a higher degree than the locking method has.
Jiandong Huang and John A. Stankovic [16] proposed an optimistic scheme, in connection with CPU scheduling, for real-time transaction concurrency control. Using a pseudo locking method, they developed two protocols for implementation of the optimistic concurrency control scheme, which have the properties of deadlock freedom and predictable blocking time. The two protocols can be applied to main memory resident and disk resident database systems, respectively. In addition, they proposed a set of algorithms for conflict resolution accompanied with the optimistic scheme. They also developed a CPU scheduling scheme to accommodate starvation problem commonly found in optimistic concurrency control schemes. The proposed protocols and algorithms have been implemented on a real-time database testbed. The experimental results indicate that integrated with real-time oriented CPU scheduling, OCC outperforms 2PL with respect to total weighted value, and OCC provides higher transaction deadline guarantee ratio than 2PL as long as transaction deadlines are not extremely tight. Due to its limited blocking time, OCC performs better than 2PL particularly for long transactions when data contention exists. Binto George And Jayant R. Haritsa [17] identified which of the previously real-time CC protocols are able to provide covert channel security. Then, they profiled the RT performance of these secure CC protocols representative set using a complete simulation model. Their experiments exhibited that the OPT-WAIT, provides the most excellent performance. Also, they proposed and evaluated a novel "dual-CC" approach that allows the RTDB to use different CC mechanisms at the same time for ensuring security and for improving RT performance. Then, they proposed an adaptive admission-control policy , GUARD, which designed to give fairness to the killed transactions distribution across levels of security. They showed that GUARD provides nearby perfect fairness for RT applications that can tolerate covert channel bandwidths of up to one bit per second.

4.2 Locking CC

A secure two phase locking protocol presented by Sang H. Son et al. [18] and discussed a supporting of trading off security for timeliness by an adaptive method, depending on the system's existing state. The performance of the adaptive secure two-phase locking protocol showed improved timeliness. They presented an approach to scheduling transactions to improve timeliness in a secure real-time database. The performance results substantiate their claim that an adaptive security policy that sacrifices the security properties to some extent can improve the deadline miss performance.
Chanjung Park and Seog Park [8] presented a new locking protocol in order to eliminate covert channels and priority inversion. They gave some examples and showed that this protocol ensures one-copy serializability.
Chanjung Park et al. [19] proposed a new multiversion concurrency control protocol that ensures that both real-time requirements and security are met. They proposed a new method, called the freezing method. FR serializability is a new serializability for multiversion CC which is more general than traditional serializability, defined by them to show that the concurrency of their protocol provides is higher degree than existing multiversion protocols concurrency. Their new protocols' significant performance improvement showed in their simulation's results. They also presented a simulation model and an evaluation of the relative performance of the protocol compared with other protocols. The simulation study showed that even though the proposed protocol has additional features such as satisfying security and real-time requirements, it provides reasonable performance compared with four other protocols.
A new lock-based CC protocol proposed by sungyoLlng et al. [20], Secure Dynamic Copy Protocol, ensuring both conflicting requirements. Their protocol aims for reducing the storage overhead of maintaining secondary copies and minimizing the processing overhead of update history. In their protocol they lay out to keep a secondary copy when it is needed to resolve the conflicting in secure RTDB. They also examined the performance characteristics of their protocol through simulation under different workloads. The results show that proposed protocol consumed less storage and decreased the deadline missing transactions.

5. CONCLUSION

RTDBS is one of the interesting issues nowadays which have been developed greatly in the relatively short time of its existence. Next-generation of RTDBS investigator is based on continues progress of this evolution that makes research study on this field continue to pursue state-of-the-art applications and apply both existing techniques to them; as well as to develop a new one when needed. This study provides an extensive survey of real-time systems research. We classify the existing proposed mechanisms based on the security and concurrency control in RTDBS.

REFERENCES

[1] A. Buchmann. Real Time Database Systems. Idea Group, 2002.
[2] Sang H. Son, Craig Chaney and Norris P. Thomlinson, "Partial Security Policies to Support Timeliness in Secure Real-time Databases", in Security and Privacy, 1998, IEEE Symposium, 10.1109/SECPRI.1998. 674830 ,pp: 136 – 147.
[3] Kyoung-Don Kang, Sang H. Son, "Towards Security and QoS Optimization in Real-time Embedded Systems", in The work-in-progress (WIP) session of the RTSS 2005, ACM SIGBED Review, Vol. 3 Issue 1, January 2006 , pp. 29-34.
[4] Kyoung-Don Kang, Sang H. Son and John A. Stankovic, " STAR: Secure Real-Time Transaction Processing with Timeliness Guarantees" in Proceedings of the 23rd IEEE REAL-TIME SYSTEMS SYMPOSIUM (RTSS'02), -8725/02 $17.00, 2002.

DOI 10.17148/IJARCCE.2016.5268

[5] Binto George and Jayant Haritsa, "Secure Transaction Processing in Firm Real-Time Database Systems" in the 1997 ACM SIGMOD international conference on Management of data, SIGMOD '97, 1997, Pages 462-473

[6] Ahmed H. Omari, Basil M. Al-Kasasbeh, Rafa E. Al-Qutaish And Mohammad I. Muhairat, "A New Cryptographic Algorithm for the Real Time Applications", in Proceedings of The 7th WSEAS International Conference On Information Security And Privacy, 2008, pp. 33-38.

[7] Kyoung-Don Kang and Sang H. Son, "Systematic Security and Timeliness Tradeoffs in Real-Time Embedded Systems", in 12th IEEE International Conference of Embedded and Real-Time Computing Systems and Applications, 2006, 10.1109/RTCSA.2006.59, pp. 183 – 189.

[8] Chanjung Park and Seog Park, " A Multiversion Locking Protocol for Real-Time Databases with Multilevel Security", in IEEE, Real-Time Computing Systems and Applications, 1996, Proceedings., Third International Workshop , 0-8186-7626-4, pp. 136 – 143.

[9] RasikanDavid, Sang H. Son and Ravi Mukkamala, "Supporting Security Requirements In Multilevel Real-Time Databases", in Security and Privacy, 1995, IEEE, 10.1109/SECPRI.1995.398933, pp. 199 - 210.

[10] Sang H. Son, Robert Zimmerman and J orgen Hansson, "An Adaptable Security Manager for Real-Time Transactions", in IEEE Real-Time Systems, Euromicro RTS 2000. 12th Euromicro Conference , 2000, 10.1109/EMRTS.2000.853993, 1068-3070, pp. 63 – 70.

[11] Sang H. Son,Senior, Ravi Mukkamala and Rasikan David," Integrating Security and Real-Time Requirements Using Covert Channel Capacity", in IEEE Transactions on Knowledge and Data Engineering, Vol. 12, No. 6, 2000, 865 – 879.

[12] Quazi N. Ahmed and Susan V. Vrbsky, "Maintaining Security in Firm Real-Time Database Systems" ,in Computer Security Application IEEE Conference, 1998, Proceedings. 14th Annual,10.1109/ CSAC.1998.738584 , 1998 , pp. 83 – 90.

[13] Maysam Hedayati, Seyed Hossein Kamali, Reza Shakerian and Mohsen Rahmani "Evaluation of Performance Concurrency Control Algorithm for Secure Firm Real-Time Database Systems via Simulation Model", in 2010 InternationalConference on Networking and InformationTechnology, 2010, IEEE.

[14] ShibyThomas,S.SeshadriandJayant R.Haritsa, "Integrating Standard Transactionsin Firm Real-Time DatabaseSystems", in the Journal :Information Systems - Special issue on real-time database systems , Vol. 21, 1996, pp. 3 - 28

[15] Byeong-Soo Jeong, Daeho Kim, and Sungyoung Lee, "Optimistic Secure Real-Time Concurrency Control Using Multiple Data Version", in LCTES '00 Proceedings of the ACM SIGPLAN Workshop on Languages, Compilers, and Tools for Embedded Systems,2001 ,ISBN:3-540-41781-8, pp. 33 – 47.

[16] Jiandong Huang and John A. Stankovic, "Concurrency Control in Real-Time Database Systems:Optimistic Scheme vs. Two Phase Locking", in a Technical Report : Concurrency Control in Real-Time Database System:Optimistic Scheme vs. Two-Phase Locking, University of Massachusetts Amherst, USA , 1990.

[17] Binto George And Jayant R. Haritsa, "Secure Concurrency Control in Firm Real-Time Database Systems", in Journal : Distributed and Parallel Databases - Security of data and transaction processing, Vol. 8, 2000, pp 41 – 83.

[18] Sang H. Son, Rasikan David, Bhavani Thuraisingham, " Improving Timeliness in Real-Time Secure Database Systems", in ACM SIGMOD Record, Vol. 25 Issue 1, March 1996, PP. 29-33 .

[19] Chanjung Park, Seog Parkand Sang H. Son, "Multiversion Locking Protocol with Freezing for Secure Real-Time Database Systems", in IEEE Transactions on Knowledge and Data Engineering, Vol. 14, No. 5, 2002, pp. 1141-1154.

[20] Sungyoung Lee, Byeong-Soo Jeong and Hyon-Woo Seung, " A Secure Dynamic Copy Protocol in Real-Time Secure Database Systems", in LCTES '99 Proceedings of the ACM SIGPLAN 1999 workshop on Languages, compilers, and tools for embedded systems, 1999, pp. 73-79.