IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 3, June-July, 2013
ISSN: 2320 - 8791
www.ijreat.org

ISAMSA:Scheduling Security for Multimedia Applications in Heterogeneous Networks

K. Karnavel[1], R. Renita[2], U. Sathya Rekha[3]
[1]Assistant Professor, Department of Computer Science & Engineering, AIHT, Chennai
[2,3]PG student, Department of Computer Science & Engineering, AIHT, Chennai

ABSTRACT
When scheduling security is very important issue in the design of multimedia applications since these applications are most widely used in industry and academic organizations. Security requirements are not taken into consideration in existing scheduling schemes when making allocation and control decisions for real time multimedia service in heterogeneous networks. In this paper, we propose an improved security – aware multimedia scheduling algorithm (ISAMSA) in the framework of heterogeneous networks. At earliest, we build a general media distortion model according to the experimental parameters in each network, as well as each application's peculiarity. After that, we utilize a scalable graph-based authentication method which achieves a good trade-off between flexibility and efficiency. Furthermore, a improved security – aware multimedia scheduling algorithm is proposed by taking into account applications' timing and security requirements in addition to precedence constraints. The proposed algorithm first gives high priority to deal with schedulability when the real-time system is overloaded. When workload of the system is less, ISAMSA strives to improve the security levels while achieving high schedulability for real-time Multimedia application. ISAMSA shows excellent scheduling quality under a wide range of workload characteristics.

Keywords
Security-critical Scheduling, Heterogeneous networks, Multimedia applications, QoS Algorithms, Multimedia data scheduling, Real-time, Security-aware, Wireless networks.

1. INTRODUCTION
Current years have witnessed the increasing efforts towards standardization of architectures for the convergence of heterogeneous access networks, and the integration of heterogeneous networks has become a part of the 4G network design [9]. Supporting multimedia applications over heterogeneous networks have been one of the major research fields in the networking and multimedia communities. For example, the IMS (IP Multimedia Subsystems) platform [1] has defined an overlay architecture for providing multimedia services on top of heterogeneous wireless networks. Inevitably, there are huge and different kinds of application multimedia data streaming from different users which may influence each other and thus, it is essential to enforce a distributed scheduling policy designed for suitable application metrics and efficient network utilization. Indeed, the problem of scheduling over heterogeneous networks is, compared to traditional networks, further complicated by the heterogeneity in both the application contents and the network conditions. Nowadays, security is of critical importance for multiple real time applications in heterogeneous networks. Since heterogeneous networks are built to execute a broad spectrum of unverified user-implemented applications from a vast number of different users, both applications and users can be sources of security threats to networks. For example, the vulnerabilities of applications can be exploited by hackers to compromise the heterogeneous networks, and malicious users can access the heterogeneous networks to launch denial of service attacks. Even a legitimate user may tamper with shared multimedia data or excessively consume computing cycles to disrupt services available to other networks' users [2]. On the other hand, however, existing heterogeneous computing systems have not employed a security mechanism to counter the threats. Thus, it is mandatory to deploy security services to protect security-critical applications running on heterogeneous networks. Since snooping is the main attack in heterogeneous computing environments, we considered authentication service to guard against the common threat to the heterogeneous networks. Scheduling plays a key role in obtaining a high performance in heterogeneous networks. Unfortunately, conventional real-time scheduling algorithms, which are developed to mainly guarantee timing constraints while possibly ignoring security requirements, are not adequate for security-critical multimedia applications in heterogeneous networks. In this study, we propose a security-critical real-time heuristic strategy on heterogeneous networks, which integrates security requirements into real-time scheduling for multimedia applications running on heterogeneous networks. To illustrate the effectiveness, the proposed Improved security – aware multimedia scheduling algorithm (ISAMSA) is applied to heuristically find resource allocations that maximize the quality of security and the probability of meeting deadlines for all the multimedia applications running on heterogeneous networks. ISAMSA is one of the first Improved security – aware multimedia scheduling algorithm strategies for real-time multimedia applications running in heterogeneous

networks. The fundamental contributions of this paper include the following aspects:

- The design and evaluation of improved security – aware multimedia scheduling algorithm running on heterogeneous networks.
- An analysis of distortion model for various multimedia applications running on heterogeneous networks.
- A scalable graph-based authentication method is proposed to achieve a good trade-off between flexibility and efficacy.
- A security overhead model for quantitatively measuring overheads introduced by security Services.

2. SYSTEM MODEL

Multimedia applications accessing many users in simultaneously via a server, i.e., real-time video streaming and audio conversation. Allow a user to access the network one of the available applications. The server decides the constant allocated rate to the user that has chosen application. We imagine that server preserve scalably adapt the transmission process to the channel conditions for the user. In the direction of this end, for each application the server can choose the accurate transmission parameters, from a predefined set of accessible parameters. We imagine encoded video layers and audio transcoders available at the server. Every one video layer is characterized by the constant encoding rate and each transcoder is characterized by its encoding rate.

In wide-ranging, all the video and audio should be compressed conveniently for transmission and storage.

2.1. Heterogeneous networks

In this paragraph, we suggest the distortion model based on multimedia multimedia data loss in heterogeneous networks. Similar to the D_{comp}, the distortion caused by multimedia data loss can be modeled by a linear model related to the multimedia data loss rate P_{loss}:

$$D_{loss} = KP_{loss},$$

The multimedia data loss rate P_{loss} reflects the combined rate of random losses and late arrivals of multimedia datas. In a bandwidth-limited network, this combined loss rate can be further modeled based on the M/M/1 queuing model [7]. In this case, the delay distribution of multimedia datas over a single link is exponential [8]. Note that, since the end-to end delay of multimedia data delivery in wireless network is dominated by the queuing delay at the bottleneck link, the empirical delay distribution for realistic traffic patterns can still be modeled by an exponential formulation:

$$\Pr\{\text{Delay} > T\} = e^{-\omega T},$$

where Pr{.} denotes the distribution probability, T reflects the delay constraint, and ω is the arriving rate which is determined by the average delay:

$$\omega = 1/E\{\text{Delay}\},$$

where E{.} represents the expectation value of non-negative random variable. Generally, ω should be determined empirically from end-to-end delay statistics over the networks. In order to present a general solution for online operation, we construct a model to approximate the average multimedia data delay.

3. MULTIMEDIA DATA SCHEDULING MODEL

We representation in our study an enhanced scheduler model compared with that given in [16]. It is assumed that each node has a single transmitter and a single receiver. Due to economical reasons, the single transmitter and single receiver on a mobile node are usually combined in a single "transceiver" which alternates between a transmitter and a receiver [15]. It should be noted that the scheduler is implemented for a wireless link, thereby; routing is out of the scope of our study. The multimedia data scheduler illustrated in Fig. 1 is located between transmitters and receivers. Fig. 1 depicts the scheduler model. When a new multimedia data arrives, it is put in the schedule queue first to wait for scheduling and assigned the lowest security level. The real-time controller in the scheduler gets a new multimedia data from the schedule queue based on the earliest deadline first (EDF) policy and determines whether or not a new multimedia data can be accepted. To be noted that the real-time controller considers both the new multimedia data and multimedia datas waiting in the accepted queue to maximize the schedulability. If the new multimedia data cannot be accommodated, it will be dropped into the rejected queue. Otherwise, it will be transferred into the accepted queue. After a new multimedia data is allocated to the accepted queue, the real-time controller notifies security level controller to work. The security level controller strives to increase the security level of multimedia datas in the accepted queue, which efficiently utilizes the system resource to enhance the security of multimedia datas in wireless networks.

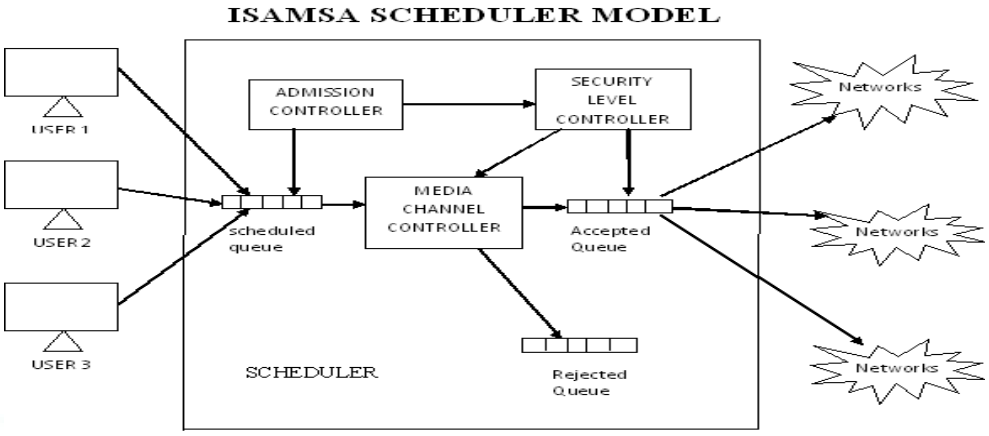

Figure: 1

4. ISAMSA ALGORITHM

The ISAMSA algorithm presented in this paper is used to adaptively make tradeoffs to the system workload. When the system is under heavy workload, ISAMSA regards the schedulability as a main goal. In contrast, when the system is in light workload, ISAMSA strives to maximize the security levels of accepted multimedia datas to efficiently utilize the system resource [18].

TABLE 1

Main notation used throughout this paper

NOTATION	DEFINITION
M_i	The i^{th} media in multimedia set M_i
a_i	The arrive time of M_i
C_i	The cut-off rate of M_i
F_i	The finish time of P_i
B_i	B_i=1 if M_i is allocated, else B_i=0
S_i	The security level of M_i
T_i	The transmission time of M_i
So_i	The security of overhead of M_i
Pt_i	The processing time of M_i
St_i	The start time of M_i
O_i	The transmission order of M_i
W_i	W_i=1 if M_i is waiting in the accepted queue, else W_i=0

ISAMSA is a heuristic algorithm. When a new multimedia data arrives, the minimal security level admission test is performed. That is, the multimedia data is given the

minimal security level and is inserted into the accepted queue of a node by the earliest deadline first (EDF) policy. If this test can guarantee the timing constraints of the new multimedia data and multimedia datas whose execution orders are later than that of the new multimedia data in the accepted queue, it is denoted that the multimedia data can be accepted. Otherwise, ISAMSA degrades the security level of multimedia datas waiting in the accepted queue using the Round Robin policy until the new multimedia data can be accepted. If all the security levels of multimedia datas being degraded to minimal still miss the deadline of the new multimedia data or violate the timing constraints of multimedia datas whose execution orders are later than that of the new multimedia data, it is rejected, or it is allocated to the accepted queue. If a new multimedia data can be inserted into the accepted queue without degrading the security levels of multimedia datas waiting in the accepted queue. In our ISAMSA algorithm, the adaptivity is sufficiently considered. If a new multimedia data cannot be allocated with the minimal security level, the security levels of some multimedia datas in accepted queue will be degraded to improve the schedulability, but SPSS just rejects the new multimedia data. In this algorithm, the inputs include multimedia data count, bandwidth, multimedia data size, arrival rate, deadline, and security level; the output is scheduling decision.

4.1. Algorithm 1: Pseudocode of ISAMSA

1: For each new multimedia data M_i do
2: $S_i \leftarrow S_k$; find ←false;
3: while $S_i <= S_k$ do
4: Calculate the start time st_i;
5: if properly 1 can be satisfied then
6: find← TRUE;
7: Raise S_i's security level, S_i++:
8: else
9: break;
10: endif
11: endwhile
12: Put all multimedia datas in the accepted queue to set S;
13: while find==FALSE && S≠0 do
14: For each multimedia data M_k in accepted queue do
15: if $S_k \neq S1$ then
16: Degrade one security level, S_k - -;
17: Calculate the start time St_i;
18: if properly 1 can be satisfied then
19: find ←TRUE;
20: else
21: break;
22: endif
23: else
24: remove M_k from S;
25: endif
26: end for
27: endwhile
28: if find==TRUE then
29: Insert M_i to the accepted queue;
30: else
31: Reject multimedia data M_i;
32: endif
33: endfor

ISAMSA is a heuristic algorithm. When a new Multimedia data arrives, the minimal security level admission test is performed. That is, the Multimedia data is given the minimal security level and is inserted into the accepted queue of a node by the earliest deadline first (EDF) policy. If this test can guarantee the timing constraints of the new Multimedia data and Multimedia data whose execution orders are later than that of the new Multimedia data in the accepted queue, it is denoted that the Multimedia data can be accepted. Otherwise, ISAMSA degrades the security level of Multimedia datas waiting in the accepted queue using the Round Robin policy until the new Multimedia data can be accepted. If all the security levels of Multimedia data being degraded to minimal still miss the deadline of the new Multimedia data or violate the timing constraints of Multimedia datas whose execution orders are later than that of the new Multimedia data, it is rejected, or it is allocated to the accepted queue. If a new Multimedia data can be inserted into the accepted queue without degrading the security levels of Multimedia datas waiting in the accepted queue, ISAMSA raises the security level as high.

In our ISAMSA algorithm, the adaptivity is sufficiently considered. If a new Multimedia data cannot be allocated with the minimal security level, the security levels of some Multimedia datas in accepted queue will be degraded to improve the schedulability, but SPSS just rejects the new Multimedia data. In this algorithm, the inputs include Multimedia data count, bandwidth, Multimedia data size, arrival rate, deadline, and security level; the output is scheduling decision. The pseudocode of ISAMSA is described in Algorithm 1.

5. CONCLUSIONS AND FUTURE WORK

We present in this paper an improved security-aware Multimedia scheduling algorithm or ISAMSA for real-time multimedia data in wireless networks. ISAMSA is able to adaptively adjust security levels according to the system workload to guarantee that, when the system is in heavy workload, schedulability becomes the main objective. In contrast, when the system is lightly loaded, ISAMSA can yield higher security levels while maintaining higher guarantee ratio.

In future work, we will extend our algorithm to deal

with multimedia data's with dependent relations. In addition, more users' requirements will be considered while scheduling besides security in real-time wireless networks.

6. REFERENCES

[1]. A. Cuevas, J.I. Moreno, P. Vidales, H. Einsiedler, The IMS platform: a solution for next generation network operators to be more than bit pipes, IEEE Communications magazine 44 (2006) 75–81.

[2]. A. Luo, C. Lin, K. Wang, L. Lei, C. Liu, Quality of protection analysis and performance modeling in IP multimedia subsystem, Computer Communications 32 (11) (2009) 1336– 1345.

[3]. K. Patrick, C. Raju, H. Cao, G. Zhu, S. Porta, Efficient hybrid security mechanisms for heterogeneous sensor networks Traynor, IEEE Transactions on Mobile Computing 6 (6) (2007) 663–677.

[4]. L. Anna, Authentication without identification, IEEE Security & Privacy Magazine 5 (3) (2007) 69–71.

[5]. L. Zhou, B. Geller, A. Wei, B. Zheng, Cross-layer rate allocation for multimedia applications in pervasive computing environment, in: Proceedings of IEEE GLOBECOM 08, New Orleans, USA, December 2008, pp. 1–5.

[6]. L. Zhou, B. Zheng, A. Wei, B. Geller, J. Cui, A robust resolution-enhancement scheme for video transmission over mobile ad-hoc networks, IEEE Transactions on Broadcasting 54 (2) (2008) 312–321.

[7]. L. Zhou, B. Zheng, A. Wei, B. Geller, J. Cui, A scalable information security technique: joint authentication-coding mechanism for multimedia over heterogeneous wireless networks, Wireless Personal Communications 51 (1) (2009) 5–16.

[8]. L. Zhou, B. Zheng, A. Wei, B. Geller, J. Cui, Joint QoS control for video streaming over wireless multihop networks: a cross-layer approach, International Journal of Electronics and Communications 63 (8) (2009) 638–647.

[9]. Liang Zhou, Athanasios V. Vasilakos, Naixue Xiong, Yan Zhang, Shiguo Lian, Scheduling security-critical multimedia applications in heterogeneous networks, Journal of Computer Communication 34 (2011) 429–435.

[10]. N. Nasser, A. Hasswa, H. Hassanein, Handoffs in fourth generation heterogeneous networks Nasser, IEEE Communications Magazine 44 (10) (2006) 96–103.

[11]. N. Xiong, A.V. Vasilakos, L.T. Yang, L. Song, P. Yi, R. Kannan, Y. Li, Comparative analysis of quality of service and memory usage for adaptive failure detectors in healthcare systems, IEEE Journal on Selected Areas in Communications 27 (4) (2009) 495–509.

[12]. P. Vidales, J. Baliosion, J. Serrat, G. Mapp, F. Stejano, A. Hopper, Autonomic system for mobility support in 4G networks, IEEE Journal on Selected Areas in Communications 23 (2005) 2288–2304.

[13]. S. Lian, Multimedia encryption and watermarking in wireless environment, in:Book Handbook of Research on Wireless Security, Idea Group Reference, An imprint of Idea Group Inc., 2008.

[14]. S. Lian, Z. Liu, Y. Dong, Scalable Authentication Method and System, FR2008052376.

[15]. S. Al-Harthi, R. Rao, A Switch model for improving throughput and power fairness in Bluetooth piconets, in: Proc. The 22nd IEEE Conf.Global Telecommunications (GLOBECOM 2003), Dec. 2003, pp. 1279-1283.

[16]. T. Xie, X. Qin, Security-aware resource allocation for real-time parallel jobs on homogeneous and heterogeneous clusters, IEEE Transactions on Parallel and Distributed Systems 19 (5) (2008) 682–697.

[17]. X. Jin, G. Min, Performance analysis of priority scheduling mechanisms under heterogeneous network traffic, Journal of Computer and System Sciences 73 (8) (2007) 1207–1220.

[18]. X. Qin, M. Alghamdi, M. Nijim, Z. Zong, K. Bellam, X. Ruan, A. Manzanares, Improving security of real-time wireless networks through multimedia data scheduling, IEEE Trans. Wireless Commun. 7 (9) (2008)3273-3279.

[19]. Y. Wu, R.H. Deng, Scalable authentication of MPEG-4 streams, IEEE Transactions on Multimedia 8 (1) (2006) 152–161.

[20]. Z. Li, Q. Sun, Y. Lian, Joint source-channel-authentication resource allocation and unequal

authenticity protection for multimedia over wireless networks, IEEE Transactions on Multimedia 9 (4) (2007) 837–850.

[21]. Z. Zhang, Q. Sun, W.-C. Wong, Rate-distortion-authentication optimized streaming of authenticated video, IEEE Transactions on Circuits and Systems for Video Technology 17 (5) (2007) 544–557.

[22]. <http://en.wikipedia.org/wiki/Digital_Signature_Algorithm>.