International Journal of Wireless Communications, Networking and Mobile Computing
2016; 3(3): 29-35
http://www.aascit.org/journal/wcnmc
ISSN: 2381-1137 (Print); ISSN: 2381-1145 (Online)

American Association for Science and Technology

Keywords
Information Security,
Information System,
Wireless Networks

Received: March 5, 2016
Accepted: July 20, 2016
Published: August 18, 2016

Data Placement Strategy for Hadoop Clusters

Mohammed I. Alghamdi

College of Comp. Science and Information Technology, Albaha University, Albaha, Kingdom of Saudi Arabia

Email address
mialmushilah@bu.edu.sa

Citation
Mohammed I. Alghamdi. Data Placement Strategy for Hadoop Clusters. *International Journal of Wireless Communications, Networking and Mobile Computing.* Vol. 3, No. 3, 2016, pp. 29-35.

Abstract
Wireless technology has become very widely used; and an array of security measures, such as authentication, confidentiality strategies, and 802.11 wireless communication protocol based security schemas have been proposed and applied to real-time wireless networks. However, most of the measures only consider security issues in static mode, in which security levels are all configured when wireless network systems are built. In real-time applications such as a stock quoting and trading system, users may need flexible quality of security that can be, e.g. measured in security levels. For example, the data of a current stock's price may require higher security than the data of the same stock ten years earlier. Thus flexible security mechanisms for real time applications transmitting packets through wireless networks would be highly desirable. In this paper, we propose a novel security-aware packet scheduling strategy for a real time wireless link where the wireless networks can dynamically set security levels according to different user requests.

1. Introduction

In recent years, wireless technology has become very widely used; and an array of security measures, such as authentication, confidentiality strategies, and 802.11 wireless communication protocol based security schemas have been proposed and applied to real-time wireless networks. However, most of the measures only consider security issues in static mode, in which security levels are all configured when wireless network systems are built. In real-time applications such as a stock quoting and trading system, users may need flexible quality of security that can be, e.g. measured in security levels. For example, the data of a current stock's price may require higher security than the data of the same stock ten years earlier. Thus flexible security mechanisms for real time applications transmitting packets through wireless networks would be highly desirable. In this paper, we propose a novel security-aware packet scheduling strategy for a real time wireless link where the wireless networks can dynamically set security levels according to different user requests.

Supporting efficient and reliable data transmission, especially in real time, over wireless networks could be extremely challenging because wireless networks may face more complicated environments compared with conventional wired networks. To make matters worse, wireless networks are more vulnerable to various attacks. Boosting security of wireless networks, therefore, has become a most important issue in wireless communications. The packet scheduling algorithm proposed in this paper addresses some of the security issues of real-time wireless networks.

2. Related Work

Since security concern plays a vital role in the design and development of wireless mobile commercial applications, international wireless organizations, wireless equipment providers and academic researchers all made efforts in utilizing the existing security mechanisms and developing innovative security policies of wireless networks. IEEE improved the security character of 802.11 by designing 802.1X and 802.11i for WLAN [2]. The 802.1X, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802.1X. Cisco provides the solutions for wireless applications by using strong encryption technology and providing unified WLAN [3]. Papers addressing the security problems also provide valuable solutions for wireless business applications [10] [11] [12] [13]. However, most of the efforts were made at the levels of protocols or systems. In addition, most existing approaches were focused on non-real time wireless applications.

Packet scheduling plays an important role in achieving high performance in real-time wireless networks. A real time scheduler needs to guarantee both security and real-time constraints of packets even in the presence of hardware and software faults [15] [16]. In general, real time scheduling algorithms can be classified into static [17] [18] and dynamic [19] [20] strategies.

Our research provides an effective dynamic security mechanism at the packet level for real time wireless links. There are some existing packet-scheduling algorithms designed to improve the performance of wireless networks. Chang and Yu presented packet scheduling algorithms to guarantee the quality of service in wireless applications of ATM and video traffic [4] [14]. The fairness issue in packet scheduling has also been addressed in many research papers [5] [6] [7] [8] [9]. To the best of our knowledge, less attention has been paid towards the security issue in the context of packet scheduling for wireless networks. In this paper, we will integrate the proposed packet-scheduling algorithm with dynamic security adjustment strategy. In doing so, we build a new secure packet scheduling scheme for real-time wireless networks.

3. Packet Scheduling for Security

3.1. The Architecture

The architecture of wireless networks is mainly composed of a *Security Level Controller* (SLC), an *Admission Controller* (AC), and an EDF scheduler as depicted in Figure 1. This architecture is designed for a link of two nodes in a wireless network. All packets are submitted independently to the wireless link with arrival rates abided by passion distribution. The function of the *Admission Controller* is to determine whether incoming packets can be accepted or not. The *Security Level Controller* aims at increasing security levels of real-time packets residing in the A*ccepted queue* that can be finished before their deadlines. The EDF scheduler makes use of the Earliest Deadline First policy to schedule admitted packets in which security levels are maximized by the *Security Level Controller*.

The following steps depict the procedure.

Security-aware packet scheduling strategy (hereinafter referred to as SPSS).

Step 1: initialize the scheduler; the security values of incoming packets; and the number of rejected packets is set to zero. Wait for any incoming packets.

Step 2: if a packet *i* arrives and it is the only packet available, process the packet immediately using its highest security level. The starting time (ST_i) and the completion time (CT_i) of the packet are calculated. The security value is increased by the security level of packet *i* which is considered as SL_{max}.

Step 3: All the packets arriving in the system during the time period [ST_i, CT_i] are stored into a *Waiting Queue* in the non-decreasing order of their deadlines. The starting time of the next packet ST_{i+1} is set to CT_i.

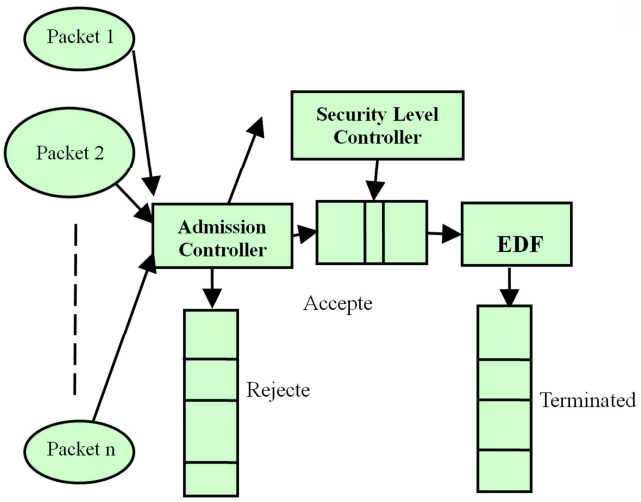


Fig. 1. *The Architecture of the Networked System.*

Step 4: the *Admission controller* main functionality is to decide whether a packet in the *Waiting Queue* can be accepted by considering the deadline of this packet. If the system can meet the packet's deadline while fulfilling the security requirement, the packet will be forwarded into the *Accepted Queue* for further processing. Otherwise, it will be rejected by being put into the *Rejected Queue* and the number of rejected packets is increased by one.

Step 5: the Security Level Controller raises the security levels of all the packets reside in the *Accepted Queue* as high as possible. The enhancements of the security levels for real-time packets residing in the *Accepted queue* are subject to the following two constraints: (a) Increasing of an accepted packet's security level should still guarantee the deadline of

the packet. (b) The increase of security levels must not lead to any rejection of currently accepted packet. We will discuss how the *Security Level Controller* increases the security level of the packets residing in the *Accepted Queue* in section 3.3.

Step 6: At this point, the security level SL_{i+1} of the next starting packet's can be maximized. Increase SV by SL_{i+1}. Its completion time CT_{i+1} is calculated. Therefore, we obtain a new time slot $[ST_{i+1}, CT_{i+1}]$ for the packet. Steps 3-6 are repeatedly executed until all the arriving packets are processed in one run.

3.2. The Packet Model

Our packet model assumes that all packets have soft deadline and all packets are independent of one another. We also assume that packets' arrival times follow the classical Poisson distribution.

Packet P_i is represented as a tuple (AT_i, PT_i, SL_i, D_i), where AT_i and PT_i denote the arrival time and the processing time of packet i. SL_i and D_i represent the security level and soft deadline of packet i. Besides, without loss of generality we assume that each packet is assigned a quality of security measured as a security level SL_i that in the range [1, 2, 3, …, 10], where 1 and 10 are the lowest and highest levels of security. For example, if packet i has a value of 1 as a security level, this means that the packet has the lowest security level.

To calculate the security overhead without loss of generality, we make use of formula (1) to model the security overhead envisioned as the extra execution time experienced by packet i.

$$SO_i = ET_i * (SL_i / R) \quad (1)$$

Where SO_i is the security overhead of packet i, SL_i is the security level provided to packet i, and R is set to 10. Thus, the total execution time of packet i can be expressed as:

$$WL_i = ET_i + SOi = ET_i * (1 + SL_i / R) \quad (2)$$

3.3. The SPSS Algorithm

The main goal of this study is to maximize the overall system performance, which reflects the Guarantee Ratio and security level.

Figure 2 below depicts the flow chart of the security-aware packet-scheduling algorithm (SPSS) for wireless links. The SPSS algorithm strives to assign a maximized security level to an Admitted packet resides in the *Accepted Queue* while making the best effort to guarantee its deadline. Recall that increasing the security level of the packet must not result in a potential rejection of any accepted packets. This criterion is important and reasonable because if a packet is admitted to the real-time wireless link, then the packet's timing constraint has to be guaranteed. In other words, the SPSS algorithm ensures that an admitted packet is not adversely affected by subsequently admitted packets.

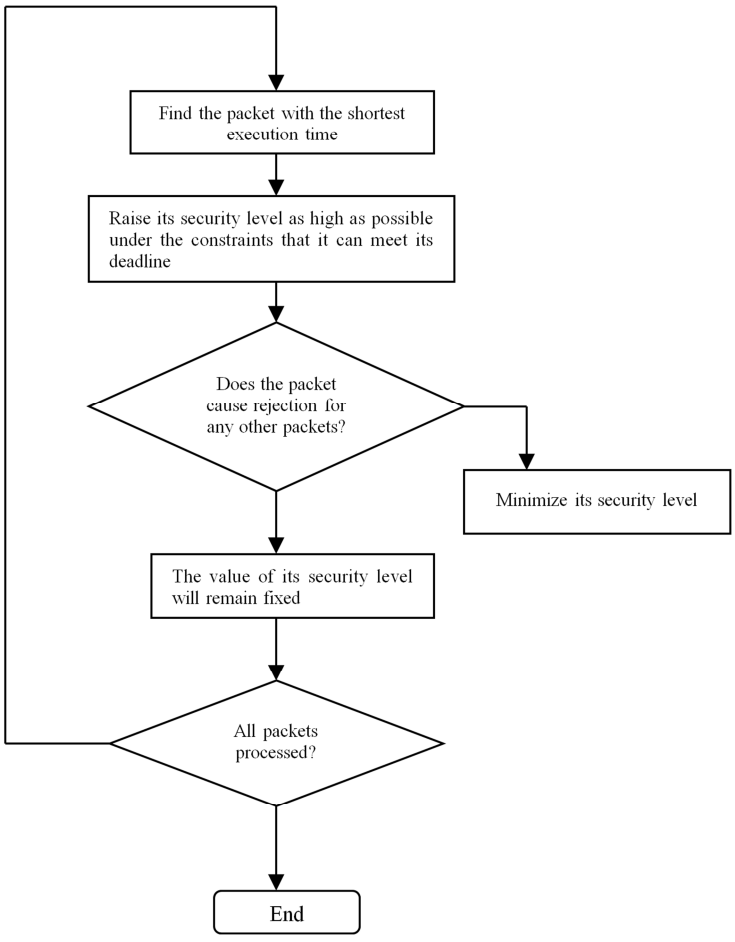


Fig. 2. *The SPSS packet-scheduling algorithm for wireless links.*

4. Simulation Results

4.1. Baseline Algorithms

Now we briefly outline the ideas of the following two baseline algorithms, which are used to compare with our proposed packet-scheduling algorithm.

MIN: The *Admission Controller* intentionally selects the lowest security level of each coming packet. Therefore, the guarantee ratio is improved at the cost of reducing overall security value of the system.

MAX: The *Admission Controller* chooses the highest security level for each accepted packet. As a result, the security values are increased while decreasing the guarantee ratio. On the other hand our proposed algorithm SPSS adaptively select the most appropriate security level of the accepted packet where both the guarantee ratio and the security level are increased which in turns increase the overall performance of the system significantly.

4.2. Performance Metrics

To evaluate the performance of our approach, we compare SPSS algorithm against two baseline algorithms, namely, MIN, and MAX.

The following three important performance metrics are used to effectively evaluate the proposed algorithm. The Overall Performance (*OP)* is measured as the product of security level (*SL*) and the guarantee ration (*GR*). The following expression is used to calculate *OP.*

$$OP = SL * GR \quad (3)$$

Where the *security level* is defined as the sum of security level values of all incoming packets issued to the network link. The *guarantee ratio* is defined as fraction of total arrived incoming packets that are found to be delivered before their deadline. Packet arrival rate λ, data sizes of packet, and deadlines are three workload parameters. We investigate performance impacts of these parameters on performance of a real-time wireless link in our simulation experiments.

4.3. Impact of Arrival Rate

This experiment is aimed at comparing the SPSS strategy with the two baseline schemes that make no use of SPSS scheme. The first baseline scheme is called MIN which always assigns the minimum security level to the incoming packets while the other baseline which is called MAX always assigns the maximum security level to the incoming packets issued to the networked system. With different settings to of data size, bandwidth, and deadline, we study the impacts of varying arrival rates on the system performance. To achieve this goal, we increased the arrival rate of the incoming packets from 0.2 to 0.9 No./Sec. while setting the data size to 0.5 KB, the bandwidth to 0.7mbps, and the deadline to 0.7 No./Sec.

Figure 3 plots the security level, guaranteed ratio, and the overall performance of the networked system with SPSS, Min, and Max schemes. Figure 3A reveals that the SPSS strategy can significantly increases the security level of the incoming packets. We can attribute this significant improvement to the fact that SPSS strategy increases the security level provided that it can meet the deadline requirement of the incoming packets.

Fig. 3B reveals that SPSS outperforms both MIN and MAX algorithms in terms of guaranteed ratio. This result can be explained by the fact that SPSS algorithm keeps increasing the security level of the incoming packets while making the best effort to guarantee their deadlines. Fig. 3C clearly shows that SPSS clearly outperform both MIN and MAX algorithms in terms of overall performance magnificently. Specifically, SPSS obtains an improvement in overall performance over MIN and MAX algorithm by an average of 9%.

This result is that when the incoming packets has loose deadline, it will have more time to be delivered before its deadline which causes the security level to be increased. Clearly, SPSS has higher security level than MIN and MAX strategies. This can be explained by the fact that the looser the deadline for the incoming packets, the more opportunities for SPSS to dynamically increase the security level for each incoming packets.

Figure 4B shows that SPSS outperforms MIN and MAX in terms of guarantee ratio. The rationale behind this result is that when the incoming packets has loose deadline, SPSS has more opportunities to deliver those packets before their deadlines thereby increasing the guarantee ratio.

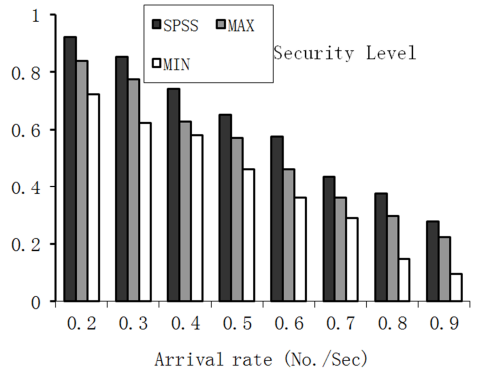


Fig. 3A. *Impact of arrival rate when data size = 0.5KB Bandwidth = 0.7MBPS, and deadline = 0.6 No./Sec.*

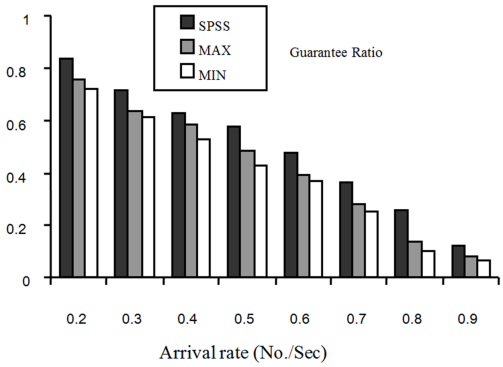


Fig. 3B. *Impact of arrival rate when data size =0.5KB, Bandwidth = 0.7MBPS, and deadline = 0.6No./Sec.*

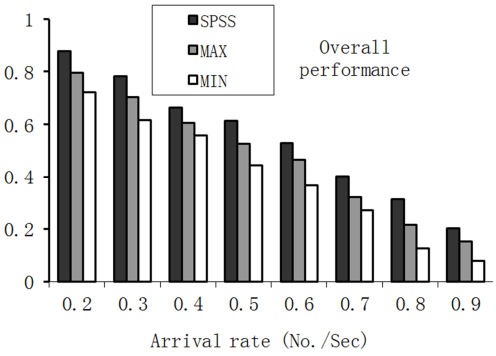


Fig. 3C. *Impact of arrival rate when data size =0.5KB, Bandwidth = 0.7MBPS, and deadline = 0.6No./Sec.*

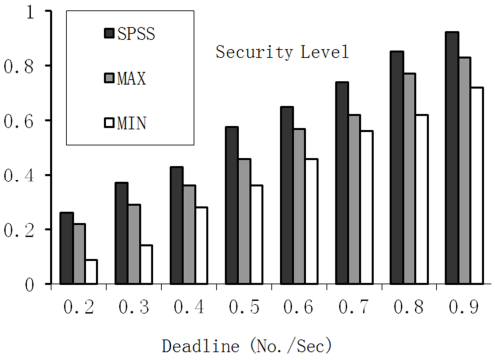


Fig. 4A. *Impact of deadline when data size =0.5KB, bandwidth=0.7MBPS, and arrival rate=0.5No./Sec.*

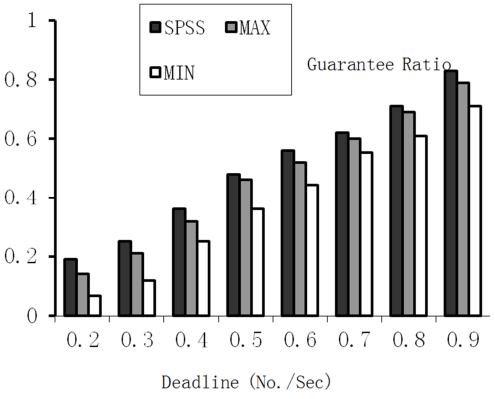


Fig. 4B. *Impact of deadline when data size =0.5KB, bandwidth=0.7MBPS, and arrival rate=0.5No./Sec.*

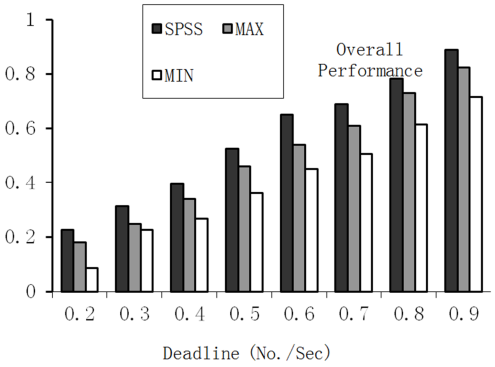


Fig. 4C. *Impact of deadline when data size =0.5KB, bandwidth =0.7MBPS, and arrival rate = 0.5No./Sec.*

4.4. Impact of Deadline

In this section, we varied the deadline from 0.2 to 0.9 No./Sec to examine the performance impact of deadline on the networked system.

This performance improvement can be attributed by the fact that SPSS adaptively enhance security levels of each incoming packets under the condition that all incoming packets can meet their deadlines.

Figure 4A shows that when the deadline increases from 0.2 to 0.9 No./Sec the security level performance metric increases. The main reason of Because the security level and the guaranteed ratio rapidly increase, the overall performance of SPSS also goes up (see figure 4C).

4.5. Impact of Data Size

In this group of experiment, we compared the performance of SPSS against MIN and MAX strategies when we varied the data size from 0.2 to 0.9KB.

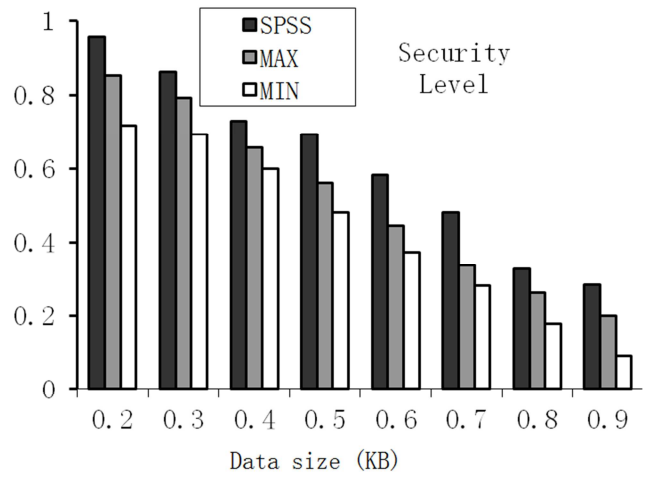
Figure 5A demonstrates that SPSS shows a significant improvement in security level over MIN and MAX strategies. Interestingly, it is also observed from figure 5A that the security level gradually drops as the value of data size increasing. This is because the increasing values of the data size results in an overload in the system which also turns in decreasing the values of the security level of the packets residing in the queue in order to finish most of the packets before their deadlines. Figure 5B shows that when the data size varied from 0.2 to 0.9KB the SPSS strategy delivers higher guarantee ratio that both MIN and MAX strategies. This result is consistent with the result in figure 3B which demonstrates that SPSS achieves good performance in guaranteed ratio. Further, we observe from figure 5C that when the data size goes up, the overall performance of SPSS decreases. This is because the security level of the incoming packets is lowered down due to the high load in the system which results in decreasing the overall performance of SPSS.

4.6. Impact of Bandwidth

In this experiment, we investigated the performance of SPSS, MIN, and MAX strategies when the network bandwidth varies from 0.2 to 0.9 MBPS.

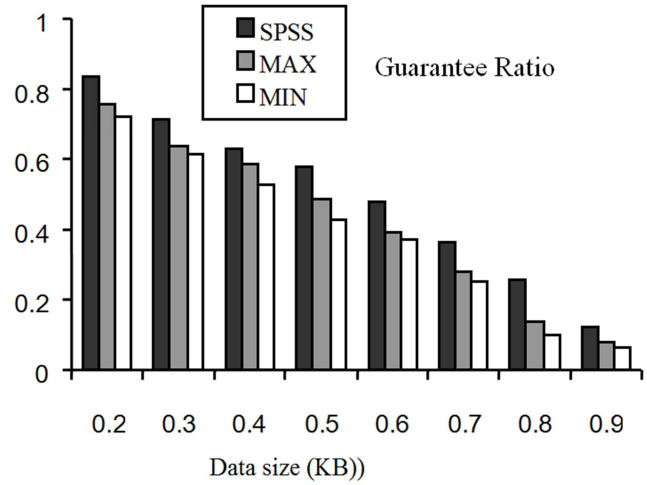
Fig. 6A shows that the security level increases as the network bandwidth is increased, because more packets can pass through the network before their deadline due to the short processing time of the packets over the network.

An important observation drawn from Fig. 6B is that as the network bandwidth increases, the guarantee ratios of the three strategies rise. The result can be explained by the fact that the high network bandwidth leads to short transfer times, which in turn result in short processing times of packets. Consequently, more packets can be passed through the network before their deadlines. Thanks to the increasing in the security level and the guarantee ratio, the overall performance of SPSS is substantially improved.



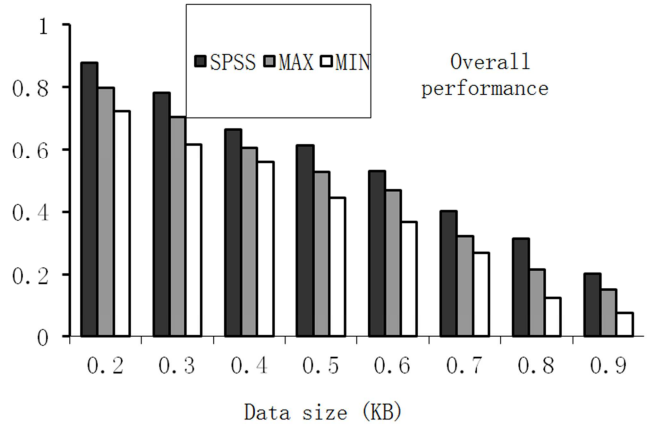
A. Data size vs. Security level

Fig. 5A. *Impact of data size when bandwidth =0.7MBPS, arrival rate =0.5No./Sec. and deadline= 0.6 No./Sec.*



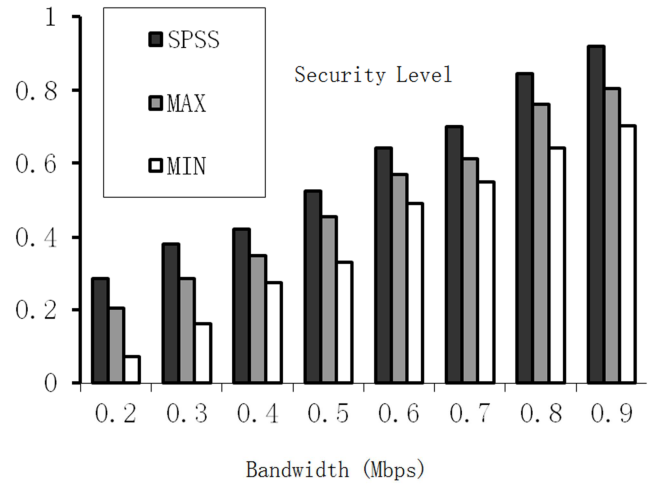
B. Data size vs. Guarantee ratio

Fig. 5B. *Impact of data size when bandwidth =0.7MBPS, arrival rate =0.5No./Sec. and deadline= 0.6 No./Sec.*



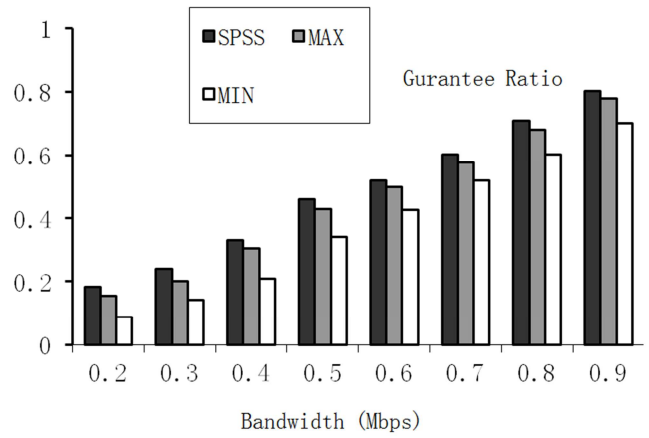
C. Data size vs. Overall performance

Fig. 5C. *Impact of data size when bandwidth =0.7MBPS, arrival rate =0.5No./Sec. and deadline= 0.6 No./Sec.*



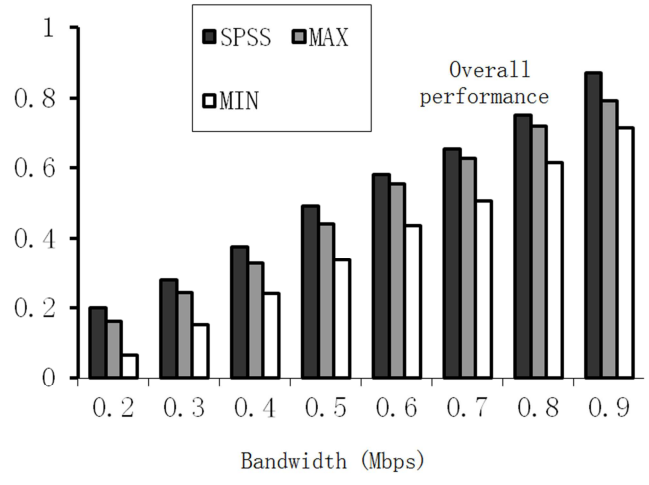
A. Bandwidth vs. Security level

Fig. 6A. *Impact of bandwidth when data size =0.6KB, arrival rate =0.6No/Sec., and deadline = 0.6 No./Sec.*



B. Bandwidth vs. Guarantee ratio

Fig. 6B. *Impact of bandwidth when data size =0.6KB, arrival rate =0.6No/Sec., and deadline = 0.6 No./Sec.*



C. Bandwidth vs. Overall performance

Fig. 6C. *Impact of bandwidth when data size =0.6KB, arrival rate =0.6No/Sec., and deadline = 0.6 No./Sec.*

5. Conclusion

In many real-time wireless network applications, not only high guarantee ratio for packets is required, but also high quality of security. To develop real-time wireless networks that provide both high security and high guarantee ratio, we proposed a novel dynamic security-aware packet-scheduling algorithm (or SPSS for short) which is capable of achieving high quality of security for real-time packets while making the best effort to guarantee real-time requirements of those packets. The SPSS algorithm is designed in a way that makes it possible to achieve a reasonably high guarantee ratio and to optimize security level. In particular, our SPSS algorithm leverages an intelligent *Security Level Controller* to adaptively assign security levels to incoming real-time packets transmitted via a wireless network link. The experimental results show that our approach delivers significant improvements in guarantee ratio, security level, as well as overall system performance under a wide range of workload patterns. Specifically, our approach can provide an overall performance improvement by up to 15%.

References

[1] Gavin Donoho, "Building a Web Service to Provide Real-Time Stock Quotes," MCAD. Net, February, 2004.

[2] Tom Karygiannis, Les Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices", chapter 2, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

[3] White Paper of Cisco, Building the Mobile Business with a Unified Wireless Network http://epsfiles.intermec.com/eps_files/eps_wp/

[4] C. Chang, J. Chang, K. Chen and M. You, "Guaranteed quality-of-service wireless access to ATM,"IEEE JSAC, 1997.

[5] S. Lu, V. Bharghavan and R. Srikant, "Fair Scheduling in wireless packet networks," IEEE Trans. Networking, August 1999.

[6] V. Bharghavan, "A new protocol for medium Access in wireless packet networks," online document, 1999.

[7] J. C. R. Bennett and H. Zhang, "WF2Q: Worst-case fair weighted fair queuing," IEEE INFOCOM'96, 1996.

[8] T. S. Ng, I. Stoica and H. Zhang, "Packet fair Queueing algorithms for wireless networks with location dependent errors," IEEE INFOCOM'98, March 1998.

[9] T. Nandagopal, T. Kim, X. Gao and V. Bharghavan, "Achieving MAC Layer Fairness in Wireless Packet Networks," ACM MOBICOM'00, Boston, MA, August 2000.

[10] Badamas M. A (2001). Mobile Computing Systems – Security Considerations, Information Management and Security 2001, 134-136.

[11] Gupta V and Gupta S (2001). Securing the Wireless Internet, IEEE communications Magazine, Dec 2001, 68-74.

[12] Owens M, Karygiannis S (2000). Wireless Network Security. NIST Special Publication 800 -48.

[13] Siau K., Lim E. P. & Shen Z. (2001). Mobile Commerce: Promises, Challenges and Research Agenda, Journal of Database Management, July – Sept 2001 Vol. 12, 4-19.

[14] Xiaomei Yu; Hoang, D. B.; Dagan Feng; "A QoS, control protocol for rate-adaptive video traffic", Networks, 2001. Proceedings. Ninth IEEE International Conference on 10-12 Oct. 2001 Page (s): 434–438.

[15] X. Qin, and H. Jiang, "Dynamic, Reliability-Driven Scheduling of Parallel Real-time Jobs In Heterogeneous Systems," Proc. Int'l Conf. On Parallel Processing, Valencia, Spain, pp. 113-122, 2001.

[16] X. Qin, H. Jiang, D. R. Swanson, "An Efficient Fault-tolerant Scheduling Algorithm for Real-time Tasks with Precedence Constraints in Heterogeneous Systems," Proc. Int'l Conf. on Parallel Processing, British Columbia, Canada, pp. 360-368, Aug. 2002.

[17] J. C. Palencia, and H. M. Gonzalez, "Schedulability, analysis for tasks with static and dynamic offsets," Proc. the 19th IEEE Real-Time Systems Symp., 1998, pp. 26-37.

[18] T. F. Abdelzaher and K. G. Shin, "Combined Task and Message Scheduling in Distributed Real-Time Systems," IEEE Trans. Parallel and Distributed Systems, Vol. 10, No. 11, Nov. 1999.

[19] M. A. Palis, "Online Real-Time Job Scheduling with Rate of Progress Guarantees," Proc. the 6th Int'l Symp. Parallel Architectures, Algorithms, and Networks, 2002, pp. 65-70.

[20] G. Manimaran and C. S. R Murthy, "An Efficient Dynamic Scheduling Algorithm for Multimachine Real-Time Systems," IEEE Trans. Parallel and Distributed Systems, Vol. 9, No. 3, 1998, pp. 312-319.