Introduction

Jianhua Ma, Makoto Takizawa and Timothy K. Shih

New networking and computing paradigms are emerging due to fast progress in high processor performance and memory density, wide availabilities of wired and wireless broadband communications, and the active research results on distributed processing, agent technology, mobile computing, web technology, real time system, etc. Novel networking mechanisms, approaches, infrastructure, architecture, middleware and services are needed to support a variety of novel networking and computing. The special issue addresses advanced networking protocols and security techniques to provide powerful, flexible, reliable and trustful networking systems and applications.

This special issue on Advanced Networking Protocols and Security is organised from the papers of the International Conference on Advanced Information Networking and Applications (AINA2004), which was sponsored by IEEE Computer Society and held in the Fukuoka Institute of Technology (FIT), Fukuoka, Japan, from March 29 to March 31, 2004. The conference received 402 submissions and every paper was reviewed by three reviewers based both on quality and significance. We accepted 101 papers as long papers and 122 papers as regular ones for AINA-2004. All the authors of long papers were encouraged to submit their revised manuscripts to this special issue and 22 submissions in total were received. All the submissions were carefully reviewed again and finally 11 papers were selected, based on their quality and suitability to the special issue as well as the journal. The papers 1–5 in this issue cover novel protocols in group communications, QoS guarantee, adhoc networking and P2P systems, and the remaining 6 papers present various techniques for secure communications.

The first paper in this special issue, entitled ‘An autonomic group communication protocol for distributed applications’ is presented by T. Enokido and M. Takizawa. Their work focuses on a group protocol which supports applications with group communication services when QoS supported by networks or required by applications is changed. Their autonomic group protocol is realised by cooperation of multiple autonomous agents, each of which autonomously takes a class of each protocol function so as to support only and all QoS required. A group is composed of views for scalability. Each view is a subset of the agents when the agents autonomously take protocol classes consistent with each other. They clarify what combination of classes can be autonomously taken by agents in a view and how to autonomously change retransmission classes.

In ‘Quality of service (QoS) in internet cache coherence’ by J. Sustersic and A. Hurson, the authors present a very effective general purpose cache coherence protocol based on the QoS approach for providing strong consistency for those data items that require it, while permitting weaker consistency for less critical data. A statistical analysis of the read/write behaviour of typical internet data is used to suggest a low overhead, inexpensive QoS solution to cache coherency issues on the internet. An experimental framework is given and many simulation results are shown to study and verify the potential of the proposed scheme as a viable solution to cache coherence for general internet applications.

The third paper is entitled ‘Performance evaluation of a scalable media access control protocol for single hop WDM networks’ and is written by L. Barolli et al. The authors propose a novel media access protocol for single hop wavelength division multiplexing (WDM) networks with a passive star topology. In the conventional protocols, when the control packets collided with each other or the packets did not get a data channel from the channel reservation mechanism, these packets had to be retransmitted. The proposed protocol can allocate data channels without retransmitting control packets except the collided ones. By using the proposed protocol, it is possible to reduce the transmission delay time and to get high throughput because the number of retransmitted control packets is reduced.

In the fourth paper entitled ‘An overlay network for replica placement within a P2P VoD network’, K. Wan and C. Loeser show a hybrid peer to peer architecture and related algorithms for point to point streaming in autonomous systems as it might occur in large companies, a campus or even in large hotels. Their major aim is to create a replica situation so that intersubnet RSVP streams are reduced to a minimum. To realise this, they introduce a layered overlay networking architecture for interconnecting subnetworks, each of which contains a so called local active rendezvous server (LARS) acting as both a directory server and a controller of movie content availability in its subnetwork.

The fifth paper, by K. Takata and J. Ma, is entitled ‘A decentralised P2P revision management system using a proactive mechanism’. In this paper, the authors present a P2P system of group revision assistance management (GRAM) based on a proactive mechanism. It performs the revision collision prevention management and software source code synchronisations in a pure decentralised overlay network of peers connected via the internet or a LAN/WAN.

Copyright © 2005 Inderscience Enterprises Ltd.

This system offers four special features in comparison with other version management systems: higher system reliability and robustness, effective revision collision prevention using proactive agents, context aware environment for team software revision, and a unified XML format for configuration and history files as well as messages exchanged between the agents.

The sixth paper entitled 'A scalable group rekeying scheme using secret mask patterns' is coauthored by Y. Asem and A. Kara. The authors propose a new group rekeying method for changing the multicast group key: matrix-mask-based group rekeying (MMGR). The main objective of their rekeying method is to solve the rekeying problem that arises when some group members leave the group. In MMGR, the group controller constructs the rekeying message using a numerical matrix and the group members apply secret bit masks on the matrix to get the group key. It does not need computationally expensive encryption of the group key before transmission and hence eliminates the need to decrypt it after receiving the rekeying message. The computational cost of the rekeying server is low, and the computational cost of the group members is low and constant, regardless of the rekeying message size.

In the seventh paper entitled 'Secure distribution and access of XML documents', J. Zhang et al. present a novel scheme for securing XML documents and their distribution over the internet. The proposed scheme has some distinct features. It requires only one private key for each user. Therefore, when a user leaves or joins the system, keys of all the other existing users in the system remain unchanged. The encryption key is computed only once and the encryption and decryption of a session key require only two or three exponential computations. This makes the proposed scheme more attractive and hence particularly suitable for the dynamic distribution of documents over the internet.

The eighth paper entitled 'A security system implementation using software agents' is coauthored by E. Shakshuki, Z. Luo and J. Gong. The authors present a multiagent system architecture to provide a secure environment for protecting hosts and users at two levels. At the first level, the user is authenticated and authorised. At the second level, the messages are encrypted, decrypted, signed and verified. The system architecture is comprised of three tiers. At the front end of the system, interface agents interact with the users to fulfil their interests. At the middle tier of the system, service guard agents act as the system safeguard by authenticating and authorising users so that they can access the system and use the service resources appropriately. At the back end of the system, service provider agents offer different security services to different users.

In the ninth paper which is entitled 'A dynamic mechanism for determining relationships in a partially ordered user hierarchy', C. Chang et al. address a protection system in which some mechanism is needed for determining the relationship between any two users so as to be used to help the decision making requests to change access attributes. In this paper, they propose a mechanism in the partially ordered user hierarchy, instead of the tree hierarchy discussed till now, by assigning each user an interpolating polynomial constructed from the user's own id number and his father's id number. In this way, any two users' relationship can be quickly determined by evaluating their associated polynomials. Moreover, whenever a new user is added into or deleted from the user hierarchy, none or only some relevant polynomials need to be updated; this is different from preciously proposed schemes, where the information from all over needs to be reconstructed.

The tenth paper 'Use of cryptographic technologies for privacy protection of watermarks in internet retails of digital contents' is presented by C. Wang et al. They propose a scheme of secure watermarking protocol using cryptographic technologies for use in real life internet retails market of digital contents, in which trust between customers and digital contents providers may not be assumed. A commutative encryption algorithm is used in the proposed scheme to doubly lock the information by the secret keys of both a contents provider and its customer, separately. The privacy of the watermark pattern is maintained, while the digital rights of the contents provider are protected. This is achieved by allowing the customer to choose a secret pattern of watermark combination unknown to the contents provider. Consequently, the quality of the watermarked digital contents can be guaranteed. They also show that the protocol is secure against any possible attacks from the customer and the contents provider.

The last paper by G. Yee et al. is entitled 'Context aware privacy and security agents for distance education'. Although distance education applications have been widely deployed, not many of them provide privacy and security for their users. Most of them only provide access control by requesting a user id and password. The authors first convey the importance of privacy and security for distance education and then show how they can be provided. They further present an extension of the previous work to the use of context aware agents that can provide privacy and security for distance education applications in an intelligent manner, based on the user's interaction context. Such context aware agents are based on an agent framework adapted from IEEE P1484.1/D9: the Learning Technology Systems Architecture (LTSA).

Taking this opportunity, we would like to thank all the authors for submitting papers to the special issue, and the referees for giving valuable comments, which are very important for authors to further revise their papers and keep them in good quality. Our special thanks go to AINA2004 Program Chair, Professor Leonard Barolli at Fukuoka Institute of Technology (FIT), for his invaluable help in handling the paper reviewing, and members in Takizawa Lab for their assistance in managing all the submissions.

Finally, we would like to thank the Editors in Chief of the *International Journal of High Performance Computing and Networking* (IJHPCN), Dr. Laurence T. Yang and Dr. Yi Pan for giving us the opportunity to publish this special issue.