ITU-T Kaleidoscope Session 3

Protocols, QoS, Privacy and accessibility in NGN

Chair:

IKEDA Yoshikazu

Otani University, JP

S3.1: FUTURE CHALLENGES OF IRSIMPLE PROTOCOL: EFFICIENT FLOW CONTROL SCHEME AND LONG DISTANCE CAPABILITY

A M Shah, G Kitazumi and M Matsumoto
Waseda University, Japan

This paper examines the effectiveness of proposed flow control scheme for IrSimple protocol. It is carried out a complete examination for all possible cases where frame losses can occur due to transmission error. It shows that the proposed flow control scheme recovers from any possible frame losses without adding any complexity to the system as well as reduces the redundant data retransmissions. It was also examine the long distance capability of current IrDA links which is required to enhance IrSimple applications. Results are presented which reveal that IrDA links can support up to 3m distances by increasing the transmitted light intensity.

Key results are:

1. Infared Data Assocattion （IrDA）has specified “IrSimple Protocol”.
2. It is very useful for short distance data links; currently for 1 meter max, but up to 3 meters with the proposed improvements.
3. It is showed less costly and better performance for NGN Home Network etc.

S3.2: ANALYSIS AND OPTIMIZATION OF RESOURCE CONTROL SCHEMES IN NEXT GENERATION NETWORKS

*M S Hemami†, M Pirhadi‡, A I Tabrizipoor**

†Amirkabir University of Technology, Iran, ‡ Islamic Azad University, Science and Research Branch, Iran, * Iran Telecom Research Center

In this paper two resource control schemes are investigated, i.e. single-phase and two-phase, and their effect on different network parameters.

This investigation showed that the two-phase scheme has a higher call setup delay than single-phase. However, two-phase has better resource availability for best effort traffic, although it has a higher blocking probability for normal-load traffic.

According to the results It is found out that a dynamic approach for resource control scheme selection will have a better network performance than a static one.

It is also suggested a modification for RACF structure and consequently, a little revision in DIAMETER protocol implementation.

Key results are:

1. Improvements for “Resource and Admission Control Protocol” of NGN QoS is proposed.
2. Single-phase call flow process for the resource reservation& commitment is good for QoS applications; but Two-phase call flow shows better performance for “Best Effort”.
3. It is proposed Dynamic Selection Policy for the call flow schemes for the wide variety of application service requirements of NGN.

S3.3: A SELF-ENCRYPTION BASED PRIVATE STORAGE SYSTEM OVER P2P DISTRIBUTED FILE SHARING INFRASTRUCTURE

H Endo, Y Kawahara, and T Asami
The University of Tokyo, JP

This paper presents a private storage system using self-encryption scheme over P2P distributed file sharing infrastructure with the authentication and the secure path that IMS provides.

This system has several advantages as follows:

1. As unique encryption keys are automatically generated from each data and deleted after using them only by the internal processing of the terminal, users do not need to worry about key management.

2. In distributed storage method, the amount of the communication can be reduced, in addition the safety against information leakage at the loss of the terminal and from the network storage is also high.

(continued)

3. As distributed storage system stores distributed data based on P2P overlay network and shares this infrastructure with other users, the intruder cannot get all the distributed data only by hacking a single server.

4. As this system allows users to share common uploaded data already stored by other users, the physical upload process is reduced using a duplicate file existence.

In this paper, mobile terminals are authenticated by IP Multimedia Services Identity Module (ISIM) because they are managed in IMS framework . On the other hand, the servers are authenticated by Public Key Infrastructure (PKI). Certification Authority (CA) is required. In addition, the algorithms in self-encryption scheme and protocols for communication are required.

Key results are:

1. P2P distributed file sharing scheme is showed very useful for private storage system.
2. Self-Encryption protocol is proposed using IMS platform.
3. It is particularly efficient and reliable for “Mobile Handsets Distributed Storage” applications.
4. It is also proposed applicable ideas for the protocol improvements to protect information security in the era of NGN.

S3.4: POSITIONAL GESTURE FOR ADVANCED SMART TERMINALS: SIMPLE GESTURE TEXT INPUT FOR SYLLABIC SCRIPTS LIKE MYANMAR, KHMER AND BANGLA

Y K Thu, O Phavy and Y URANO
Waseda Uninversity, JP

The Positional Gesture text input for syllabic languages is proposed as it is very simple and easy to understand.

With our prototypes, even first time users can type Myanmar and Khmer text with appropriate typing speed. We use very few gesture commands for text input (basically 4 gesture commands such as left, right, up and down), and thus, it is a possible typing method not only for children but also for senior people.

Positional Gesture text input concept is applicable for many other input methods such as hand gesture, eye gaze and brain input etc.

(continued)

And it is extendable for other similar syllabic languages such as Nepali (language of Nepal), Lao (language of Laos) and Hindi (one of the languages of India) ,etc.

It have already been developed Bangla language prototype, and are planning to make user study and follow up analysis in the near future.

It is believed that Instant Messaging (IM) and Messaging Services (SMS, MMS, etc.) are important NGN Services.

For advanced smart terminals, this will provide as a possible text input methods for the syllabic languages in the NGN and Ubiquitous environments.

Key results are:

1. For syllabic script languages, e.g. Myanmar, “Positional Gesture” text input method is invented.
2. Very simple but very easy to understand to use because of the graphical interface using the position information and selection menu of symbols among each characters.
3. It is also useful for other languages with syllabic script; Khmer, Bangla are under developments with this idea.

Conclusions and Recommendations for Session 3 as a whole

- Protocols for Home Network access, optimization for QoS/BestEffort traffic flows, and Distributed Security Storage Mobile Systems are proposed and improved for the near NGN applications.
- Very simple and easy text input method is developed for south Asia languages.
- Steady progress and studies are taken place in the area of protocols, access and human interface for NGN and future networks.

Young Author Recognition awarded for:

- Mohammad Shah Alam (Waseda University)
- Hiroki Endo (University of Tokyo)
- Ye Kyaw Thu (Waseda University)