UNIVERSITI PUTRA MALAYSIA

MULTICAST-UNICAST KEY MANAGEMENT AND DATA DELIVERY METHOD IN WIRELESS IPv6 NETWORKS

ABBAS MEHDIZADEH ZARE ANARI

MULTICAST-UNICAST KEY MANAGEMENT AND DATA DELIVERY METHOD IN WIRELESS IPv6 NETWORKS

By

ABBAS MEHDIZADEH ZARE ANARI

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

July 2012

DEDICATION

This thesis is dedicated to

MY BELOVED WIFE, HAMIDEH FOR HER ENDLESS CARE, COMFORT, AND LOVE IN MY LIFE

AND

MY RESPECTED PARENTS, MOHAMMAD & ZEINAB FOR THEIR GREAT SUPPORT AND CARE, MY LOVELY SISTERS, AND MY WONDERFUL BROTHERS

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

MULTICAST-UNICAST KEY MANAGEMENT AND DATA DELIVERY METHOD IN WIRELESS IPv6 NETWORKS

By

ABBAS MEHDIZADEH ZARE ANARI

July 2012

Chairman: **Assoc. Prof. Raja Syamsul Azmir Raja Abdullah, PhD**

Faculty: **Engineering**

Multicast is an efficient way of transmitting data simultaneously to a group of users. It has the advantage of reducing the required bandwidth of data delivery compared to unicast transmission. Nevertheless, existing multicast method suffers from several major drawbacks which can be viewed from two different viewpoints, namely, security and Quality of Service (QoS).

In regard to security, the main challenge is to provide security protection to data which are multicast to many users. This can be achieved by using a secure key management process, specifically by increasing the level of encryption/decryption of transmitted data. Whenever a new node is granted to join or leave a multicast group, a new key should be generated and distributed to every node in the network. Considering a highly dense environment where connection of users to the network is frequently changing due to join or leave operations, such approach may burden a network device with a huge amount of complex encryption and decryption process.

While a number of algorithms has been proposed to address this issue, most of the existing approaches have to increase their encryption and decryption cycles in order to maintain the security level of the key management, thereby again suffering from high computation cost.

Meanwhile, from the QoS perspective, multicast over Wireless Local Area Networks (WLANs) offers a trade-off between data transmission rate and coverage. The larger the coverage is, the lower the transmission rate would be. Unfortunately, the transmission rate of existing multicast is confined by the user with the lowest data rate in the group, also known as fixed base rate problem.

In this thesis, the aforementioned issues are addressed extensively in a new and efficient way. Instead of focusing on either security or QoS, this research highlights the possibility of addressing both criteria without having to sacrifice one for the sake of the other. By focusing mainly on Internet Protocol version 6 (IPv6) wireless networks, the use of both multicast and unicast transmissions for multicast service are considered. By integrating both multicast and unicast methods, it is envisaged that the proposed solution inherits their monumental advantages, and therefore is able to facilitate a lightweight key management process to multicast IPv6 as well as addressing the fixed base rate problem of multicast transmission. Moreover, this thesis places emphasises more on the IPv6 multicast transmission instead of the conventional Internet Protocol version 4 (IPv4).

The feasibility and performance of the proposed key management method is evaluated analytically and empirically (in an IPv6 test-bed environment), as well as is analyzed based on Markov Chain and Poisson Arrival Process. The results are

compared with existing key management methods in terms of communication, computation, and storage costs. The performance evaluation indicates the efficiency of the proposed scheme in reducing such costs, while at the same time maintaining both forward and backward securities. The overall improvements of communication, computation, and storage costs are more than 64%, 19%, and 29%, respectively.

For evaluation of the proposed data delivery method, the proposed method is implemented in indoor and outdoor environments and the results are compared to the conventional multicast method. The transmission of real-time video application is considered in the test-bed. The proposed method is able to improve the throughput and video quality experienced by end user, with low packet loss and transmission delay. The average improvements are 65%, 48.3%, 67.3%, 47.9%, and 66% for throughput, packet loss, packet delay, end-to-end delay, and jitter, respectively.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Doktor Falsafah

MULTISIAR-UNISIAR PENGURUSAN KUNCI DAN KAEDAH PENGHANTARAN DATA DALAM RANGKAIAN IPv6 WAYARLES

Oleh

ABBAS MEHDIZADEH ZARE ANARI

Julai 2012

Pengerusi: Profesor Madya Raja Syamsul Azmir Raja Abdullah, PhD

Fakulti: Kejuruteraan

Multisiar adalah satu cara yang berkesan bagi menghantar data secara serentak kepada sekumpulan pengguna. Ia mempunyai kelebihan dari segi mengurangkan jalur lebar yang diperlukan bagi penghantaran data berbanding dengan penggunaan penghantaran unisiar. Walau bagaimanapun, kaedah multisiar yang sedia ada mempunyai beberapa kelemahan nyata yang mana boleh dilihat dari perspektif-perspektif yang berbeza, yakni, keselamatan dan kualiti perkhidmatan (QoS).

Berkenaan keselamatan, cabaran utama adalah bagi membekalkan perlindungan keselamatan terhadap data multisiar kepada ramai pengguna. Ini dapat dicapai melalui penggunaan kunci proses pengurusan yang selamat, khususnya dengan meningkatkan tahap penyulitan/penyahsulitan bagi data yang telah dihantar. Bila mana satu nod yang baru diterima untuk menyertai atau meninggalkan sebuah kumpulan multisiar, sebuah kunci baru hendaklah diaktifkan dan dibahagikan kepada setiap nod di dalam rangkaian. Mengambil kira tentang kepadatan persekitaran yang tinggi di mana saluran para pengguna terhadap jaringan adalah berubah-ubah secara

kerap disebabkan oleh operasi-operasi keluar dan masuk, pendekatan sebegitu boleh membebankan sebuah alat jaringan dengan jumlah penyulitan yang besar serta kompleks di samping proses penyahsulitan. Walaupun sejumlah algoritma telah dicadangkan bagi menghadapi isu ini, kebanyakan pendekatan yang sedia ada perlu meningkatkan kitaran penyulitan dan penyahsulitan mereka bagi menyeimbangkan tahap keselamatan kunci pengurusan, dengan itu ia sekali lagi mengalami kos pengiraan yang tinggi.

Di samping itu, dari perspektif QoS, multisiar bagi Rangkaian Kawasan Setempat Wayarles (WLANs) menawarkan pertukaran di antara kadar penghantaran dan liputan. Semakin luas sesebuah liputan, semakin kecil kadar penghantaran tersebut. Malangnya,kadar penghantaran bagi multisiar yang sedia ada adalah dibatasi oleh pengguna yang mempunyai kadar data terendah di dalam kumpulan tersebut, juga dikenali sebagai masalah kadar asas tetap.

Di dalam tesis ini, isu-isu yang telah dinyatakan di atas telah disentuh serta dibincangkan secara mendalam melalui cara baru yang berkesan. Berbanding meletakkan fokus ke arah sama ada keselamatan atau QoS, penyelidikan ini menegaskan tentang kemungkinan menyentuh kedua-dua kriteria tanpa perlu mengabaikan salah satu untuk kebaikan yang lain. Dengan memfokuskan khususnya ke arah jaringan wayarles Protokol Internet versi 6 (IPv6), penggunaan kedua-dua penghantaran multisiar dan unisiar untuk perkhidmatan multisiar telah dipertimbangkan. Dengan mengintegrasikan kedua-dua teknik multisiar dan unisiar, ianya dijangka bahawa cadangan yang telah dikemukakan mewarisi kelebihan-kelebihan monumental mereka, dan oleh itu mampu memudahkan proses kunci

pengurusan yang ringan kepada multisiar IPv6 serta menyatakan masalah kadar tetap asas bagi penghantaran multisiar. Tambahan pula, tesis ini meletakkan fokus yang lebih bagi penghantaran multisiar IPv6 berbanding Protokol Internet versi 4 (IPv4) yang sedia ada.

Kemungkinan dan prestasi kunci pengurusan yang dicadangkan telah dinilai secara analitikal dan empirikal (dalam persekitaran ujian IPv6) dan juga berdasarkan Rantai Markov dan Proses Ketibaan Poisson. Dapatan keputusan telah dibandingkan dengan kaedah pengurusan utama dari segi komunikasi, pengiraan dan juga kos penyimpanan. Penilaian prestasi menunjukkan kecekapan skim yang dicadangkan dalam segi pengurangan kos dan juga turut membantu dalam mengekalkan keselamatan ke depan dan ke belakang. Peningkatan keseluruhan komunikasi, pengiraan, dan kos penyimpanan masing-masing adalah lebih daripada 64%, 19%, dan 29%.

Untuk penilaian kaedah penghantaran data yang dicadangkan, kaedah ini telah diaplikasikan dalam persekitaran dalaman dan luaran dan hasil dapatan dibandingkan dengan kaedah multisiar lazim. Penghantaran aplikasi video masa nyata turut diambil kira dalam ujian ini. Kaedah yang dicadangkan bukan sahaja berupaya untuk meningkat kualiti video dan truput yang dialami oleh pengguna tetapi juga berupaya untuk mengurangkan kehilangan paket data dan juga mengatasi kelewatan penghantaran. Peningkatan purata adalah 65%, 48.3%, 67.3%, 47.9%, dan 66% masing-masing untuk truput, kehilangan paket, kelewatan paket, kelewatan hujung-ke-hujung, dan ketar.

ACKNOWLEDGEMENT

Praise be upon Allah, the Almighty who is Just, Kind, and Compassionate. He has given me the guidance and confidence to complete this research which would has never been finalized without His blessings and will.

There are many people that I would like to appreciate and thank them for their contribution to complete this research, and for their knowledge sharing and wonderful friendships which have provided me a fascinating experience in last few years at the Universiti Putra Malaysia. If I miss some of them here, they have my sincere apologies.

First and foremost, I would like to express my heartiest thanks to my supervisor, Assoc. Prof. Dr. Raja Syamsul Azmir Raja Abdullah for his valuable guidance, unfailing advice, and constant support that made this work possible.

I wish to extend my deepest gratitude to Professor Borhanuddin Mohd Ali for his support, efforts in professional reviewing, and constructive feedbacks in writing my thesis.

My special thanks to Dr. Fazirulhisyam Hashim who helped me with inspirational encouragements, continuous and constructive feedbacks, and thoughtful insights throughout this research that have extremely improved the quality of this research. I truly appreciate his kindness bestowed on me.

I also wish to thank my respected co-supervisors, Professor Mohamed Othman and Professor Sabira Khatun for their great helps and guidance during the period of my study.

I would like to reserve the most extensive acknowledgment for my beloved wife, my respected parents, and my family members who endured this long process with me always offering care, unlimited support, and patience. Thanks to them who loved me and made me stronger to overcome the moments of depression and uncertain situations.

Finally, I wish to thank many fellow colleagues and friends, in particular, Dr. Amin Malek Mohammadi, Mojtaba Mohammad Pour, Farhad Mesrinejad, Seyyed Masoud Seyyed Shohadaei, Ayyoub Akbari, Mohammad Mehdi Gilanian Sadeghi, Hadi Sargolzaey, Nidhal Odeh, Mohammad Reza Ranjbari, and of course many others for their help and wonderful friendships.

APPROVAL

I certify that a Thesis Examination Committee has met on 12 July 2012 to conduct the final examination of ABBAS MEHDIZADEH ZARE ANARI on his Doctor of Philosophy thesis entitled "Multicast-Unicast Key Management and Data Delivery Method in Wireless IPv6 Networks" in accordance with the Universities and University Colleges ACT 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Doctor of Philosophy.

Members of the Thesis Examination Committee were as follows:

Ahmad Fauzi Abas, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Salasiah bt. Hitam, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Internal Examiner)

Zuriati Ahmad Zukarnain, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Lawrence Wong, PhD
Professor
Faculty of Engineering
National University of Singapore
(External Examiner)

SEOW HENG FONG, PhD
Professor and Deputy Dean
School Of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Doctor of Philosophy. The members of the Supervisory Committee were as follows:

Raja Sysmsul Azmir Raja Abdullah, PhD
Associate Professor
Faculty of Engineering
Universiti Putra Malaysia
(Chairman)

Borhanuddin Mohd. Ali, PhD
Professor
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Fazirulhisyam Hashim, PhD
Lecturer
Faculty of Engineering
Universiti Putra Malaysia
(Member)

Mohamed Othman, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Sabira Khatun, PhD
Professor
Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
(Member)

BUJANG BIN KIM HUAT, PhD
Professor and Dean
School Of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or at any other institutions.

ABBAS MEHDIZADEH ZARE ANARI

Date: 12 July 2012

TABLE OF CONTENTS