E^{2}T: END-TO-END TUNNELLING EXTENSION TO MOBILE IPV6

Deguang Le*, Xiaoming Fu*, Xiaoyuan Gu†, Dieter Hogrefe*
*Institute for Informatics, Universität Göttingen, Lotzestr. 16-18, Göttingen 37083, Germany
Email: {le,fu,hogrefe}@cs.uni-goettingen.de
†Institute of Operating Systems & Computer Networks, Technische Universität Braunschweig
Mühlenpfordtstr. 23, Braunschweig 38106, Germany
Email: xiaogu@ibr.cs.tu-bs.de

ABSTRACT

In the standard Mobile IPv6, bidirectional tunnelling through the home agent or route optimization show inefficiency in per-packet forwarding, especially when both communicating endpoints are mobile. To be scalable and compatible, mobile devices' packets should be forwarded efficiently with minimal changes to the network infrastructure. However, the current solutions do not provide any means for the end systems to perform optimized packet routing during the operation of the mobile devices. In this paper, we present an End-to-End Tunnelling Extension to Mobile IPv6 (E^{2}T) for routing packets, which reduces per-packet forwarding cost for the communications of mobile devices through a lower packet routing overhead. Besides, our approach requires little change to Mobile IPv6, but allows the more efficient forwarding behavior with a shorter end-to-end transmission latency between communicating endpoints. The simulation results show our approach is suitable for real-time multimedia applications.

I. INTRODUCTION

With the fast evolution of mobile communication and Internet technology, there is a strong need to provide connectivity for moving devices to communicate with other devices on the Internet. Internet mobility support has been a hot topic in the past decade, and studies that address this issue have arisen, coming up with a number of protocol proposals and schemes [1]. Among them, Mobile IPv6 (MIPv6) [2] as the most mature solution has been supported and adopted by mobile devices and network equipment vendors [3], and some of the network providers are even starting to deploy MIPv6 networks [4].

MIPv6 allows a Mobile Node (MN) to communicate with a Correspondent Node (CN) at any time and any place. Fundamentally, MIPv6 consists of functional blocks [2]: movement detection, Care of Address (CoA) configuration, (home or correspondent) registration, and packets routing. In [5], [6], [7], the former 3 aspects were addressed. However, to the best of our knowledge, there is little effort in improving the efficiency of routing for the MN's data packets. We believe efficient routing is necessary to fully exploit the potential of mobility enabled on the future Internet. At the network layer, the traditional routing mechanism is realized by employing tunnelling [8], the so called Bidirectional Tunnelling (BT) [2] in MIPv6. However, the BT forces all packets for a MN to be routed through its Home Agent (HA). Thus, packets to the MN are often routed along paths that are significantly longer than optimal ones [9]. Hence, the Route Optimization (RO) [2] was developed beside the traditional BT. The RO enables routing packets directly to the MN's CoA, which allows the shortest communication path to be used. It also eliminates congestion at the MN's home link and HA. However, in the RO, the MN needs to not only register its CoA to the HA, but also update binding to the CN, which suffers from greater control traffic. In addition, it relies on the Routing and Destination Option extension headers for packets routing, which is extra overhead.

Some improvements have been suggested to the standard RO mechanism. Vogt proposed proactive tests in [10], where the procedure of address tests in the standard RO can be done proactively. Perkins [11] presented a RO security enhancement mechanism between the MN and CN by pre-configuring data useful for pre-computing a Binding Management Key that can subsequently be used for authorizing Binding Updates. In [12], Bao et al. suggested that one of the HA's functions be act as security proxy for its mobile nodes. The authentication is based on the HA's certificate and the secret session keys are generated by strong cryptosystems. This proposal avoids many security obstacles in the Return Routability mechanism. Since these proposals have been focused on the security enhancements to the Return Routability and correspondent registration procedures based on the RO, the issue of signaling optimization for efficient packet routing is not tackled. This will however be covered in our work.

Besides, the prosperous development of mobile Internet together with the enormous growth of mobile users has resulted in a strong trend that there are more and more communicating endpoints, both of which are mobile on the Internet [13]. The scenario of communications between mobile users directly will be ubiquitous on the future mobile Internet. Therefore, in this paper, we investigate the performance of mobility routing mechanisms in more common mobile scenario, where communicating endpoints are mobile, and point out their strengths and weaknesses. In terms of the perspective of routing performance in mobile environments, we provide an alternative routing enhancement mechanism based on End-to-End Tunnelling Extension to MIPv6 (E^{2}T) for data packet routing. The approach has the advantages of optimal end-to-end traffic delay and reduced overhead. The simulation evaluation shows our approach has better routing performance against the current routing mechanisms, especially for real-time multimedia applications.

The remaining part of paper is organized as follows: In Section 2, we describe the routing mechanisms as specified in MIPv6 and formulize the problems of the standard routing mechanisms. Then, the goals for enhancement are discussed. Section 3 presents our approach, including the E^{2}T protocol architecture, adaptive tunnel setup, data packets routing and security considerations. Evaluation of the proposed E^{2}T mechanism is given in Section 4.Finally we draw our conclusions in Section 5.

II. Standard MIPv6 Routing Mechanisms and Their Problems

In this Section, starting with a presentation of the standard MIPv6 routing mechanisms, we reveal their problems. Then, we discuss the objectives for routing enhancement.

A. *Mobile Packet Routing Mechanisms in MIPv6*

In order that the communicating endpoints (i.e. the MN and CN) can trace and route packets to each other continuously even while moving, MIPv6 specifies two routing mechanisms for packet transmission between the MN and CN: the BT and RO. Figure 1 illustrates the mobile routing mechanisms in MIPv6.

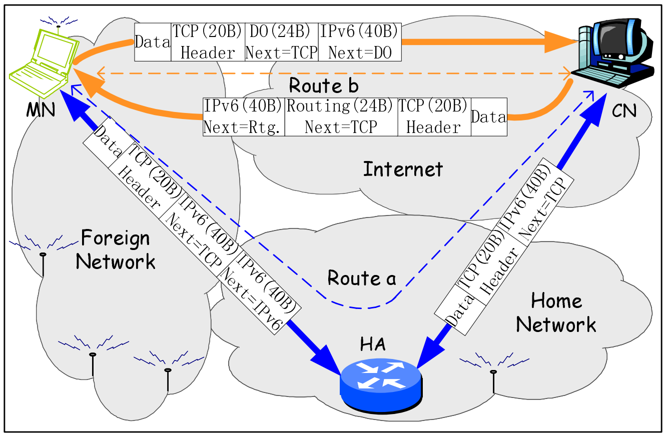


Fig. 1. The mobile packet routing mechanisms in MIPv6

In the BT, packets from the CN to MN are routed to the home address of MN, the HA shall uses proxy Neighbour Discovery [14] to intercept any IPv6 packets addressed to the MN's home address on the home network. Each intercepted packet is tunnelled to the MN's current CoA [8]. Packets to the CN are tunnelled from the MN to the HA, which is called the reverse tunnelling [15], and then routed normally from the home network to the CN (see figure 1, route a).

In the RO, the HA no longer exclusively deals with the address mapping, but each CN can have its own binding cache. In the direction from the MN to CN, packets sent by the MN are delivered to the CN with the Home Address option in the Destination Option Extension header when the MN is away from its home network. In this case, the MN sets the IPv6 header's source address to its CoA and adds a Home Address option with the MN's home address to the IPv6 header. In the opposite direction, when sending packets to the MN, the CN checks its cached bindings for an entry for the packets' destination address. If a cached binding entry for this destination address is found, the CN uses the Type 2 Routing header to route packets to the MN by specifying the CoA as the destination address in the IPv6 header and the MN's home address as the final destination in the Routing header (see figure 1, route b).

B. *Problems of Standard Routing Mechanisms*

As described in the previous Subsection, the RO as well as BT specifies messages and extensions to the basic protocol for mobile packet routing between the MN and CN. This Subsection will investigate the effect of the standard MIPv6 routing mechanisms on performance.

Overhead is a critical issue in wireless environments, where spectrum is a scarce resource and must be used with care. In the RO, when the MN wishes to let the CN communicate directly with it in its visiting location, the CN sends the packet with a Type 2 Routing header. the corresponding packet from the MN to CN utilizes a Home Address option. When both the MN and CN are away from their home networks, packets delivered between the MN and CN need additional messages of both the Type 2 Routing header and the Destination Option extension header for correct functioning of routing. Therefore, the use of this direct data path incurs the cost of both Routing header and Home Address options in each direction, whereas the BT employs the tunnel header for packets forwarding between the MN and the HA, which suffers from the overhead of tunnel header [16].

The end-to-end traffic delay is also directly affected by the MIPv6 routing mechanisms. We assume that the two routing mechanisms are applied under the same Internet status including the same process time of routers and the same delay of link etc., so the traffic delay between two endpoints that are on the Internet mainly depend on the delivery distance. Then, from the figure 1 , we can see that the distance between the MN and HA plus the distance between the HA and CN is longer than the distance between the MN and CN. Therefore the end-to-end traffic delay with the RO is reduced compared to the case using the BT.

C. *Objectives for Routing Enhancement*

The motivation behind the enhancement of the mobile routing mechanisms is to improve the delivery of IP-based multimedia data over MIPv6, which requires properties of low transmission delay, high wireless bandwidth utilization and scalability. In recent years, multimedia applications like the Voice over IP (VoIP), video conference and networked music are gaining momentum in the mobile Internet. Its traffic mix is subject to dramatic changes due to the ever-increasing proportion of packet-switch multimedia contents. Such applications are well recognized as delay sensitive and resource demanding. Therefore, any efforts that help to reduce the delay at any point from end to end will be much appreciated. Besides, since in the wireless environments, the radio link is typically constrained in bandwidth, a better mobile routing approach with less overhead is obviously critical to high bandwidth utilization and scalability, in particular, with the increase of the traffic volume.

Therefore, the need of the optimal end-to-end traffic delay as well as routing overhead turns out to be increasingly important, which is thus the objectives for routing enhancement in this paper.

III. E^{2}T: End-to-End Tunnelling Extension To Mobile IPv6

Motivated by these objectives, we present an E^{2}T mechanism between the MN and CN. We propose to use a tunnel header to replace the Home Address option and Type 2 Routing header when both of the MN and CN are in the foreign networks.

A. *Protocol Architecture for E^2T at Endpoints*

To support the use of the E^{2}T mechanism, IPv6 encapsulation must be implemented at the MN and CN, namly they both act as the tunnel endpoints (i.e. the tunnel entry-endpoint and tunnel exit-endpoint). In addition, we extend the IPv6 tunnel engine [8] with a E^{2}T manager. Figure 2 shows the architecture for E^{2}T at the endpoints.

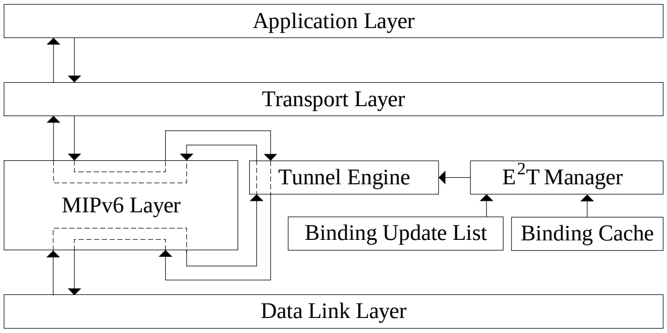


Fig. 2. The architecture for E^{2}T at the endpoints

Here, the E^{2}T Manager module implements configured tunnels depending on the information of Binding Update List (BUL) and Binding Cache (BC) and invokes the tunnel engine based on the configure tunnels. The Tunnel Engine module processes the data packets by performing encapsulation or decapsulation according to the configured tunnel [8]. The detailed operations of the extended modules can be found in [17].

B. *Adaptive Tunnel Setup*

Because the proposed E^{2}T is an extension to MIPv6 and acts as an alternative beside the current routing mechanisms (i.e. the BT and RO), especially for the scenario where the communicating endpoints are mobile, for compatibility and adaptability, the endpoints should distinguish the standard routing mechanisms from the E^{2}T, so that it can adaptively decide whether to route packets to the CoA directly by the standard routing mechanisms or to use the E^{2}T, depending on the moving scenarios.

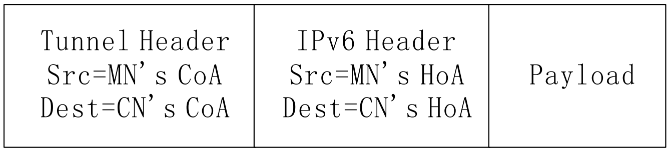
For adaptive tunnel setup, before the entry-endpoint (i.e. sending node) sends any packet, the E^{2}T examines the BUL and BC for an entry for the destination address to which the packet is being sent. If the entry-endpoint has both a BC entry and a BUL entry for this destination address, it configures the CoA of the destination address in the entry as the tunnel exit-endpoint address and enables the tunnel engine perform the encapsulation procedure.Otherwise, if the entry-endpoint has no a BUL entry or BC entry for the destination address, the entry-endpoint does not create a tunnel exit-endpoint at the entry-endpoint, and the entry-endpoint simply sends the packet normally, with standard routing mechanisms.

C. *Data Packets Routing*

After establishing a configured tunnel between the MN and CN, data packets sent between the MN and CN will be routed through the ”virtual route” represented by the configure tunnel using IPv6 encapsulation/decapsulation [8].

IPv6 encapsulation consists of prepending to the original packet an IPv6 header, which is called tunnel IPv6 header. The encapsulation takes place in an IPv6 tunnel entry-endpoint node, as the result of an original packet being forwarded onto the ”virtual route”. The original packet is processed during forwarding by decrementing the IPv6 original header hop limit by one.

When the MN encapsulates the packet for delivery to the CN, the MN sets the source address field in the new tunnel IPv6 header to the MN’s CoA and sets the destination address field in the tunnel IPv6 header to the CN’s CoA (see Figure 3). When the packet is received at the CN, the encapsulation will be stripped away, yielding the original IP packet, whose payload is then delivered to the upper layer protocols of the CN, and finally processed by the upper layer protocols as if it had been routed to the CN’s home address.



Tunnel Header
Src=MN's CoA
Dest=CN's CoA
	IPv6 Header
	Src=MN's HoA
	Dest=CN's HoA
		Payload

Fig. 3. The IPv6 headers in E^{2}T tunneled packets

Similarly, at the CN, in order to send the packet to the MN, the source field of the tunnel IPv6 header is filled with the CN’s CoA and the destination field with the MN’s CoA for encapsulation. Subsequently, the tunnel packet resulting from encapsulation is routed towards the MN. Upon receiving an packet destined to the MN, the tunnel protocol engine discards the tunnel header and passes the resulting original packet to the IPv6 protocol layer for further processing.

D. *Security Considerations*

The extension proposed in this paper are subject to the security considerations presented in MIPv6 [2]. For authenticity , the endpoint needs to insure that the encapsulating packet comes from an authentically identified, trusted source. The authenticity of the source could be obtained by Return Routability check.

By using the CoA as the source address in the tunnel header, with the MN’s home address instead in the original packet header, the packet will be able to safely pass through any router implementing ingress filtering [18].

Besides, for a secure IPv6 tunnel, an E^{2}T tunnel itself can be secured by securing the IPv6 path between the tunnel endpoints (i.e the MN and CN) based on [19], [20], [21]. The degree of integrity, authentication, and confidentiality and the security processing performed on a tunnel packet at the MN and CN of a secure E^{2}T tunnel depend on the type of security header - authentication (AH) [19] or encryption (ESP) [20] - and parameters configured in the Security Association for the tunnel. There is no dependency or interaction between the security level and mechanisms applied to the tunnel packets.

IV. Simulations and Evaluations

In this Section, we evaluate the performance of the proposed routing mechanism through simulation using the OPNET simulator [22]. The simulation models are built by incorporating the proposed routing mechanism into the standard MIPv6 model [23]. The simulation results demonstrate how enhancement to routing performance can be achieved in our approach.

A. Simulation Setup

Without loss of generality, we design the scenario, where the communicating endpoints on the mobile Internet are point to point, that is to say, the connection may be originated at any one endpoint to another, and either can be mobile. The simulation network model, depicted in Figure 4, is composed of the IP cloud model, Access Routers (ARs), and communicating endpoints (i.e the MN and CN). The IP cloud model represents the Internet, through which the IP traffic can be modelled. ARs represent wireless access networks, among which the ARs of the HA (i.e. HA_MN and HA_CN) act as the home networks with home agent function and other ARs (i.e. AR1-AR6) act as foreign networks. Each AR consists of two interfaces, among which the wireless interface supporting IEEE802.11b provides Internet access for mobile endpoints and the wired interface is connected to the Internet IP model through wired 100Mbps duplex link with 10ms delay. The AR provides a coverage area with a radius of approximately 300 meters. The MN and CN are mobile and they move within the coverage area of the ARs.

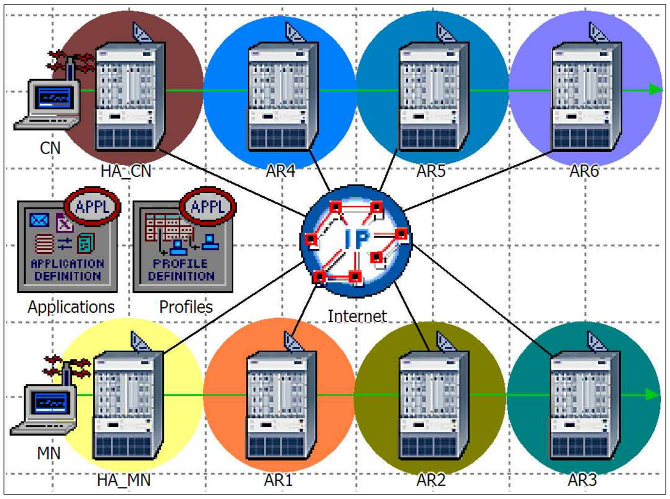


Fig. 4. The simulation network model

B. Simulation Results and Evaluations

In this Subsection, we evaluate our approach through measuring the performance metrics of the overhead and end-to-end traffic delay.

In order to evaluate the introduced overhead due to different MIPv6 routing mechanisms, we measure the overhead ratio by simulating the real-time voice application with different packet sizes. We define the performance metric of overhead ratio [17] as follows:

$$Overhead\_Ratio = \frac{Mobility\_Addition\_Size}{Original\_Packet\_Size} \qquad (1)$$

In this simulation, the CN and MN establish the voice sessions while they both roam in the range of ARs, the MN starts out from its home network (HA_MN), and moves to the AR1, AR2 and AR3 in the deterministic path with the velocity of 10m/sec; the CN begins at its home network (HA_CN), and passes one by one through the AR4, AR5, AR6 in the deterministic direction with the velocity of 20m/sec (see Figure 4). This case allows for full control of the mobility and handover rate of the concerned nodes.

Figure 5 shows the traffic overhead ratio versus the packet sizes of traffic for different MIPv6 routing mechanisms, namely RO, BT and E^{2}T. In this figure, MIPv6_Testbed_RO represents the traffic overhead ratio due to the addition of the IPv6 extension headers when routing data traffic using the MIPv6 RO mechanism. The MIPv6_Testbed_BT represents the traffic overhead ratio due to the additional tunnel header when routing data traffic through the MIPv6 BT mechanism. The MIPv6_Testbed_E^{2}T represents the traffic overhead ratio due to the tunnel header encapsulation with the proposed E^{2}T mechanism.

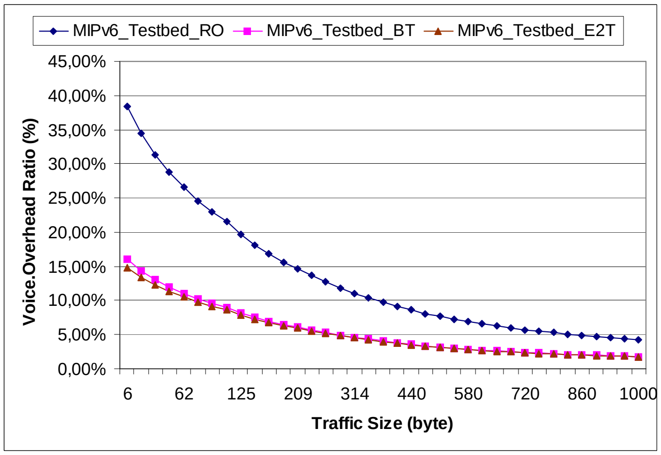


Fig. 5. The overhead ratio in MIPv6

It can be observed from the above figure that when the traffic packet sizes are 1000bytes, the overhead ratios of above routing mechanisms (i.e. RO, BT and E^{2}T) are 4.32%, 1.79%, 1.79% respectively; when the traffic packet sizes are 10bytes, the overhead ratios of above routing mechanisms are 38.36%, 15.89%, 14.98% respectively. Although the overhead ratios of all routing mechanisms increase along with the decrease of traffic packet sizes, the RO mechanism shows significantly higher overhead than the BT and E^{2}T, especially when small traffic packet sizes are used. The BT and E^{2}T introduce the same overhead since they all employ tunnelling technique for packet routing and have the same mobility addition messages of tunnel header. As many real-time applications have very small packets sizes, for example, the packet size is only 32bytes in VoIP with G.711 encoder [24], the optimization of overhead shows high importance.

We also study the differences in the end-to-end traffic delay. We measure the packet end-to-end delay between the MN and CN by running a video conferencing application. It provides constant traffic over UDP for a constant bit rate. In this simulation, the incoming packet frame sizes and the outgoing packet frame size of the individual encoded video frames were configured with the constant value of 1024bytes as input for the real time video traffic application. The incoming stream interarrival time and the outgoing stream interarrival time were configured for constant 10ms. In order to emulate Internet conditions, we specify the IP cloud with the packet delay, which randomly varies between 90ms and 100ms, and the links and devices in the network model were all configured with background traffic of G711Voice. We set the same mobility pattern as that used in the previous simulation scenario.

Figure 6 shows the end-to-end traffic delay with the RO, BT and E^{2}T, where the horizontal axis indicates the time in seconds (sec) in which the video conferencing traffic is being transmitted between mobile devices while they are moving and the vertical axis indicates the packet end-to-end delay in seconds (sec). As illustrated in the figure, from 20sec to 34sec when both the MN and CN move within the home network, the end-to-end transmissions with all above routing mechanisms have the similar delays (i.e. about 0.12sec); from 34sec to 52sec when the CN has moved into the foreign network while the MN still moves within the home network, the average end-to-end traffic delay for the BT rises up to about two times (i.e. about 0.25sec) of its previous values whereas the average end-to-end traffic delays for the RO and E^{2}T do not increase significantly. This is because that in case of BT, the end-to-end traffic delay will mainly be produced by two times the delay that the data packets pass through the Internet, and in case of the RO and E^{2}T, the end-to-end traffic delay will mainly be produced only when the data packets pass through the Internet. Similarly, from time 54sec to 180sec, when both the MN and CN move out of their home networks, the average end-to-end traffic delays for the RO and E^{2}T are only about one third of that for the BT.

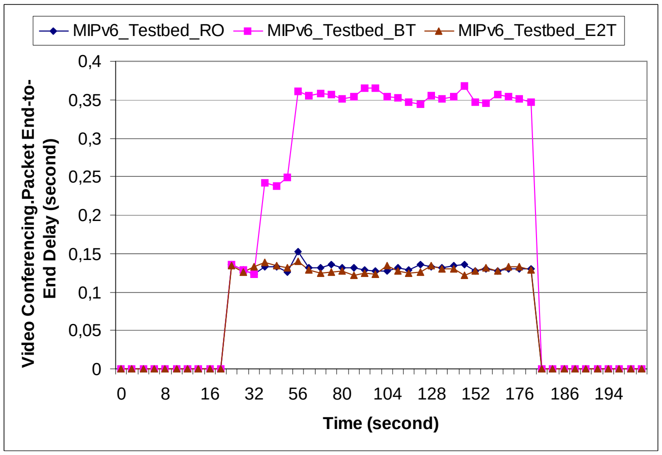


Fig. 6. The end-to-end delays of video conferencing traffic

V. Conclusions and Future Work

In this paper, we analyzed the standard routing mechanisms in MIPv6 on their pros and cons. Based on this, we proposed the E^{2}T, an alternative routing mechanism as an extension to MIPv6 routing mechanisms for routing packet when the MN and CN are away from the home networks. The proposed E^{2}T combines the less overhead of BT with the low transmission delay of RO. Simulation results show that our approach is optimal for both the traffic overhead and routing delay, which is suitable for real-time multimedia applications for mobile communicating endpoints. In the future, we will study its impact on other mobility optimization approaches, and consider the minimal encapsulation for further optimization and the tradeoff between performance and complexity.

Acknowledgements

This work is partially supported by the EC FP6 IST ENABLE project. The use of OPNET Modeler in the research was facilitated through OPNET's university program.

References

[1] D. Le, X. Fu, and D. Hogrefe, "A review of mobility support paradigms for the internet," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 1, pp. 2–15, 2006.

[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, IETF, June 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3775.txt

[3] S. J. Vaughan-Nichols, "Mobile ipv6 and the future of wireless internet access," *IEEE Computer*, vol. 36, no. 2, pp. 18 – 20, February 2003.

[4] M. Samad and R. Ishak, "Deployment of Wireless Mobile IPv6 in Malaysia," in *Proceedings of RF and Microwave Conference (RFM'04)*, 2004, pp. 256–259.

[5] D. Le, D. Guo, B. Wu, and G. Parr, "Mobile IPv6 in WLAN mobile networks and its implementation," in *Proceedings of 14th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'03)*, vol. 2, 2003, pp. 1430 – 1433.

[6] E. Natalizio, A. Molinaro, and S. Marano, "Reducing packet loss in hierarchical mobile IPv6," in *Proceedings of 15th International IEEE Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'04)*, vol. 3, 2004, pp. 1876 – 1880.

[7] D. Sivchenko, B. Xu, J. Habermann, and V. Rakocevic, "On the Performance of Enhanced Hierarchical Mobile IPv6," in *Proceedings of 16th International IEEE Symposium on Personal Indoor and Mobile Radio Communications (PIMRC'05)*, 2005.

[8] A. Conta and S. Deering, "Generic Packet tunneling in IPv6 Specification," RFC 2473, IETF, Dec. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2473.txt

[9] C. Perkins and D. B. Johnson, "Route Optimization in Mobile IP," Internet Draft (work in progress), IETF, Sept. 2001. [Online]. Available: http://www.ietf.org/proceedings/02mar/I-D/draft-ietf-mobileip-optim-11.txt

[10] C. Vogt, R. Bless, M. Doll, and T. Kuefner, "Early Binding Updates for Mobile IPv6," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC'05)*, vol. 3, 2005, pp. 1440 – 1445.

[11] C. E. Perkins, "Securing Mobile IPv6 Route Optimization Using a Static Shared Key," Internet Draft (work in progress), IETF, Oct. 2005. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-mip6-precfgkbm-04.txt

[12] F. Bao, R. Deng, Y. Qiu, and J. Zhou, "Certificate-based Binding Update Protocol (CBU)," Internet Draft (work in progress), IETF, Mar. 2005. [Online]. Available: http://www.ietf.org/internet-drafts/draft-qiu-mip6-certificated-binding-update-03.txt

[13] S. Trumpy and M. Gagnaire, "Evolution of internet technologies," *Proceedings of the IEEE*, vol. 92, no. 9, pp. 1355 – 1359, September 2004.

[14] R. Hinden and D. Thaler, "IPv6 Host-to-Router Load Sharing," RFC 4311, IETF, Nov. 2005. [Online]. Available: http://www.ietf.org/rfc/rf4311.txt

[15] G. Montenegro, "Reverse Tunneling for Mobile IP (revised)," RFC 3024, IETF, Jan. 2001. [Online]. Available: http://www.ietf.org/rfc/rfc3024.txt

[16] G. Daley, E. Wu, A. Sekercioglu, and S. Narayanan, "Packet Tunneling for Route Optimization in MN-to-MN Communications," Internet Draft (work in progress), 2005. [Online]. Available: http://ftp.apnic.net/ietf/internet-drafts/draft-ewu-mip6-mn-mn-tunnel-00.txt

[17] D. Le, X. Fu, X. Gu, and D. Hogrefe, "E^{2}T: End-to-End Tunnelling Extension To Mobile IPv6," *Institute for Informatics, University of Goettingen, Technical Report IFI-TB-2005-05*, May 2005.

[18] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827, IETF, May 2000. [Online]. Available: http://www.ietf.org/rfc/rfc2827.txt

[19] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402, IETF, 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2402.txt

[20] S.Kent and R. Atkinson, "IP Encapsulation Security Payload (ESP)," RFC 2406, IETF, 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2406.txt

[21] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, IETF, 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2401.txt

[22] OPNET Modeler, OPNET Technologies, Inc., OPNET Modeler, 2006. [Online]. Available: http://www.opnet.com/products/modeler/home.html

[23] D. Le, X. Fu, and D. Hogrefe, "Evaluation of Mobile IPv6 Based on an OPNET Model," in *Proceedings of The 8th International Conference for Young Computer Scientists (ICYCS'05)*, 2005, pp. 238 – 244.

[24] "ITU-T Recommendation G.711," Pulse Code modulation (PCM) of voice frequencies, ITU-T, 1988.