Secure and Multihomed Vehicular Femtocells

Suneth Namal, Jani Pellikka, Andrei Gurtov
Centre for Wireless Communications
University of Oulu, P.O. Box 4500, FI-90014 Oulu, Finland
Email: [namal, jpellikk, gurtov]@ee.oulu.fi

***Abstract*—Operators must ensure seamless voice and data session continuity even when subscribers are on move. Service continuity is one of the most critical quality parameter in a cellular system. QoS during handover is always hindered by the handover latency and packet loss. Among several approaches, IP multihoming is a promising solution to achieve throughput increment and packet loss reduction. Theoretically, it can ensure no interrupt or packet loss during the handover. In this paper, we present a novel Host Identity Protocol (HIP) based secure vehicular femtocell scenario. For the evaluation, we have developed a simulation model on top of HIPSim++ framework (simulation framework for HIP) integrated into INET/OMNeT++. Finally, we investigate the feasibility to use HIP in a vehicular femtocell which is new in the context and measure the performance in terms of handover latency, packet loss and throughput to compare multihomed and singlehomed communication.**

I. Introduction

There is a growing expectation among subscribers that they should be able to access internet and other media wherever they move. Service continuity is a technological challenge especially when subscribers move on public transport services in urban areas with irregular constructions. In mobile communication, backhauling is a major consideration due to non line-of-sight and frequently changing channel conditions. Solutions introduced by operators include several backhauling methods, such as satellite, UMTS, HSDPA, and also WiFi for stationary and walking mobile subscribers [1]. Most of the current solutions use satellite backhaul for high speed data transfer, though it has poor latency and fails in underground tunnels, covered areas and bad weather conditions [1], [2], [3].

IP multihoming is an approach to ensure service continuity. With multihoming, operators can cut-off the cost born due to expensive handover buffers by establishing new associations before depreciating the current associations. Further, multihoming maintains a stable throughput during the handover. However, packet rearrangement is required in either ends due to the transmission delay over different routes. According to generic IP rules, changing an IP address also happens to disconnect the sockets that are bounded to them. When applications are not bounded to IPs, readdressing can be performed without disconnecting the transport and upper layer associations. Thus, the session continuity can be retained.

In the other hand, operators prefer small cells due to low cost, unique differentiated services and monetization opportunities for the connected environments. Femtocell is a cellular hotspot that adopts 3G security protocols [4], [5], [6]. Security consultants with "Trustwave" have uncovered software and hardware vulnerabilities to gain root access to femtocells by sniffing the traffic, guessing passwords, changing IP address range and investigating hardware printouts [7]. A security research group, "The Hacker's Choice" has reverse-engineered the femtocells operated by a British mobile operator and discovered that it could be used to make illegal calls and send text messages [8].

Femtocells automatically poll for software updates upon being powered up. Home eNodeB Management System (HeMS) is responsible for the software updates. By compromising HeMS, an attacker can spread forged software updates to the femtocells that happens to takeover the complete operation. Moreover, gateways are also targeted to flooding IKE_SA_INIT, IKE_AUTH or legitimate tunnels and malforming IKE_SA or authentication credentials. Naturally, gateways come-across resource exhaustive situations after sudden power-cuts in large scales due to storms of authentication requests. HIP nodes can stay stateless until initiators are successfully authenticated and addresses are verified. HIP authentication based on elliptic curve cryptography is stronger and efficient compared to RSA cryptography. Further, protocol provides integrity, confidentiality and data origin authenticity. Also HIP provides IP independency to enable flexible mobility with cryptographically verified hash strings as identifiers.

In this paper, we present a secure vehicular femtocell scenario and investigate the feasibility of using HIP in femtocells. Further, we compare singlehomed and multihomed approaches in terms of throughput and drop rate. The paper is organized as follows. In Section II, we briefly discuss the background information of 3GPP femtocell authentication based on IKEv2. Section III introduces the certificate based femtocell authentication with HIP. We present our vehicular femtocell scenario in Section IV, the evaluation model and the results are given in Section V. Finally, Section VI concludes our research and presents the future works.

II. 3GPP Femtocell Authentication

In the femtocell architecture, Security Gateway (SeGW) is the first contact element in the core network. Femtocell mutually authenticates with SeGW using Internet Key Exchange protocol version 2 (IKEv2) with certificates. Femtocell's certificate is provided by a mobile operator, manufacturer, vendor or by a trusted third party. Similar type of certificate is configured at the SeGW which is provided by an operator trusted Certificate Authority (CA). Security credentials, such as private key of the certificate and other critical cryptographic

978-1-4673-0990-5/12/$31.00 ©2012 IEEE

functions including authentication make use of femtocell's Trusted Environment (TrE) to store sensitive information. TrE is responsible for performing cryptographic operations during the boot-up and authentication with the SeGW.

The IKEv2 based certificate exchange is described in the RFC 4306 [9]. In this paper, we will not discuss message parameters and procedures. Femtocells perform mandatory IKEv2 based device authentication with or without optional hosting party authentication. The tamper resilient Hosting Party Module (HPM) contains the credentials for identification and authentication. This module has a contractual agreement between the hosting party and the network operator that can be replaced or inserted into another femtocell. Hosting party authentication is performed using Extensible Authentication Protocol (EAP-AKA). Thus, SeGW acts as an EAP authenticator forwarding EAP messages to AAA server in order to retrieve an authentication vector from Authentication Centre (AuC) via Home Subscriber Server (HSS). Upon successful authentication, pair of unidirectional IPsec tunnels is established. Furthermore, supported ESP authentication and encryption transforms are also negotiated over IKEv2 signaling.

However, IKEv2 associations are bounded to IP addresses and must be built from the scratch each time during the handover. Though, IKEv2 supports IP multihoming with MOBIKE, simultaneous mobility (rendezvous mechanism) and route optimization [10] are not supported. Further, it does not have a protocol level design to improve the resilience against DoS and MiTM attacks. In IKEv2, nodes are exposed to active attackers such as MiTM. However, protocol hides the identities from the passive attackers. In the other hand, operation at the responder is expensive with IKEv2 compared to HIP. Moreover, HIP offers a puzzle to the initiator (cryptographic challenge) which should be solved before responder creates a state. It protects the responders from DoS attacks.

III. HIP Certificate-based Femtocell Authentication

A. An Overview of Host Identity Protocol

HIP introduces a new name space which is statistically and globally unique. Base Exchange (BEX) is the core of the protocol that mutually authenticates initiator (I) and responder (R) to each other. BEX consists of four messages that are exchanged between the peers. The first packet (I_1) includes source Host Identity Tag (HIT-I) and destination HIT (HIT-R) in non-opportunistic mode (refer Fig. 2). Second packet (R_1) includes Diffie-Hellman (DH-R) key, cryptographic puzzle, public key (HI-R) and supported transforms that are signed by the responder's public key. Initiator replies the puzzle over third packet. If an initiator successfully solves the puzzle, responder decrypts HI-I, verifies the signature on I_2 and computes the session keys for the Security Payload Index (SPI-I). In the forth packet (R_2), SPI (R) value and an Hash-based Message Authentication Code (HMAC) which is computed over the session key and signed by a responder are sent to the initiator [11]. HIP multihoming enables configuring multiple addresses simultaneously on a single device [12]. HIP inserts the "Locator" parameter into BEX or UPDATE exchange during the handover. This parameter carries the information of additional locators over which a node can be reached. To avoid conflicts, HIP recommends using separate ESP (Encrypted Security Payload) anti-replay windows for individual interfaces or addresses to receive packets from the peers when multiple locators are used.

B. HIP Authentication with Certificates

Device authentication is an essential pre-request in femtocell security. Besides that, authentication must validate device integrity. Femtocells perform mandatory device authentication and optional hosting party authentication. The Figure 1 presents the network elements that are involved in device and hosting party authentication. Device authentication during the boot-up happens only between the SeGW and the femtocell. However, hosting party authentication contacts both AAA (Authentication, Authorization and Accounting server) and HSS. Femtocell is a plug and play device which can be directly connected to a broadband access router. It tunnels traffic across the public Internet which is insecure and prone to attacks.

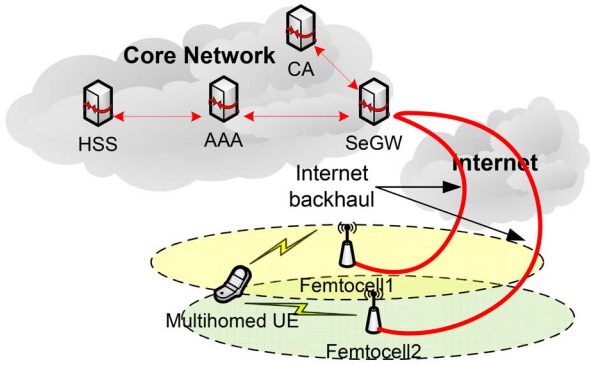

Fig. 1. Femtocell authentication and related network elements.

Authentication based on BEX alone is not sufficient enough to guarantee perfect security. A skillful MiTM attacker can still manage the BEX authentication. Thus, BEX with certificates is used to validate each other and to ensure that there are no intermediate interventions. HIP uses CERT parameter which is a container for digital certificates to transport them over the control packets during authentication and handover [13]. Certificate Authority (CA) is responsible for issuing and managing security credentials and public keys for message encryption. CA issues a certificate as part of a Public Key Infrastructure (PKI) after checking with the Registration Authority to verify the provided information by a requester [14].

Certificates can be exchanged during BEX or UPDATE exchange. The SeGW inserts its certificate into third BEX packet. Conversely, femtocell inserts its certificate into the replying message (forth packet). With certificates, they can verify the messages are originated at the clamed parties. Thus, an attacker who is trying to impersonate a legitimate user can be avoided. They also sign the message content with

their signatures in order to verify their identities. Hence, this scenario can be considered as a specific use case of HIP certificates. Femtocells can also associate with neighboring femtocells using the same certificate based authentication which is presented in the Figure 2. Moreover, this approach can be used for signaling right delegation among femtocells.

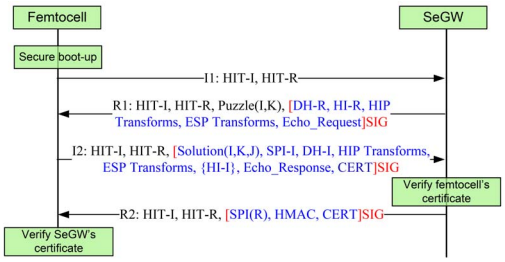

Fig. 2. HIP based authentication with certificates.

HIP has limited exposure of node identities to different form of DoS and MiTM attacks. It is a significant advantage of using HIP in femtocell technology. However, SeGWs are targeted to non-intentional DoS attacks after sudden power-cuts in large scale. During the next boot-up after a power-cut thousands of femtocells may send authentication requests to the SeGW. It may result a storm of authentication requests in the form of a resource exhaustive attack. With HIP, cost of setting-up a state at the responder is cheap compared to the cheapness at the initiator. Further, difficulty of setting up a state can be adjusted according to the level of trust. Moreover, the received "start of transport" (TCP_SYN) without prior authentication will be rejected in order to ensure protection from such attacks. Thus, it is an opportunistic negotiation which demands authentication in first place. By sending a simple pre-made packet which is fixed and easily replayable, SeGWs can be protected from TCP_SYN flooding that exhausts gateway resources.

IV. HIP-Based Multihomed Vehicular Femtocells

There are several ongoing research works that investigate the possibility of implementing high-speed mobile internet access and ground-to-train communication [1], [2], [3]. One such solution was to set-up WiFi access points inside train carriages that are connected to Worldwide Interoperability for Microwave Access (WiMAX) base stations along the route. This system can also be reverted to use with 3G cellular systems with 10-15 seconds gaps in between. We are suggesting to set-up HIP based vehicular femtocells in train carriages instead of wireless access points in order to provide internal cellular coverage. However, typical handover techniques may not fit in this scenario due to frequent handovers. Using public/private key pairs as identities, HIP decouples transport layer form internetworking layer and introduces new solutions for network-layer mobility, session continuity and multihoming. The optional "LOCATOR" parameter allows HIP nodes to notify the connected nodes of alternative addresses that they can be reached.

HIP uses IP addresses for packet routing and HITs for node identification. The IP addresses must be paired with Security Payload Indexes (SPIs) for successful packet forwarding. A femtocell with multiple interfaces can simultaneously establish several associations with the SeGW. Femtocell and SeGW use separate SPIs on each individual interfaces to avoid the problem of ESP anti-replay windows. Theoretically, IP multihoming can ensure no packet loss during the handover. The Figure 3 presents authors' HIP based vehicular femtocell architecture. HIP uses rendezvous mechanism (RVS) to update simultaneously moving HIP nodes. The femtocells inside the carriages are connected to a relay antenna on top of the roof in order to forward traffic to the neighboring base stations besides the route. Base stations backhaul this traffic towards the core network over the transport infrastructure.

In general, 3GPP femtocells are not designed to be mobile. However, setting-up them on trains with proper modifications assures better cellular coverage and high bandwidth. Thus, passengers can be offered advanced location-aware services and sensitive context-aware applications. In this scenario, the femtocells must get registered before a train starts to move from a station. The proposed HIP based vehicular femtocells support identity/locator separation and IP multihoming. Since upper layer associations are bounded to HITs, they can renew IP addresses without tearing down the current associations. Femtocells utilize IP multihoming to establish new associations before depreciating the current associations. Also, they maintain at least one network layer association at a time without totally isolating them from the core network.

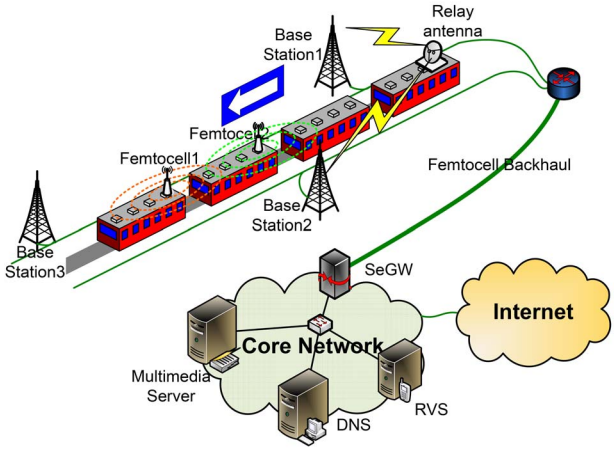

Fig. 3. HIP based vehicular femtocell communication.

Each time when they renew the associations, new keying material is exchanged and a session key is derived out of the same keying material to encrypt the communication. ESP delivers the session key to the target femtocell with added confidentiality, data origin authenticity, connectionless integrity and anti-replay protection. Multihomed femtocells with multiple interfaces can configure an address on each of the interfaces which is subjected to be changed when device is moving. However, they must rewrite the packet headers

with own identities before forwarding. Thus, femtocells must have an internal mapping technique to multiplex/de-multiplex packets from/to User Equipments (UEs), since they may have several UEs associated at a time.

Security Parameter Index multiplexed Network Address Translation (SPINAT) is a mechanism to de-multiplex multiple IP addresses on a single IP address [15]. However, SPINAT nodes cannot transparently translate the SPIs, since integrity protection keys are only shared between the end-nodes. Moreover, femtocells must inform UEs the presence of SPINAT in order to sustain ESP header integrity. To enable SPINAT, no additional signaling messages are required except SPI mapping information which is added to the control signaling messages that are received over a private link (femtocell⟶UE). Further, it does not introduce new security vulnerabilities, since the actual security only depends on the shared session key. After receiving ESP packets from UEs, femtocells must rewrite the source addresses with its address. Conversely, femtocells replace the destination addresses on the return path according to the established mapping statues.

V. Simulation Results

In this section, we present an evaluation scheme for the proposed architecture that is described in the Sections III and IV. Femtocells get registered with the SeGW and share common keying material which is used to encrypt the communication. UEs must allow the SPINAT nodes (femtocells in our case) to modify the header parameters to enable mobility support. Thus, mobile nodes do not rekey the associations unless the keying material is expired or the user moves to a new location. For evaluation, we use the OMNeT++ network simulation tool which is an open-source, component-based application that is used to model the communication networks [16]. Further, we use a HIP based simulation framework (HIPSim++) on top of INET version 20090325 [17].

For the measurements, two different applications (voice, file transfer) with different Quality of Service (QoS) profiles were used. The VOIP application policy is defined to reduce the number of handovers with an intension to minimize handover latency, packet loss and jitter. It is configured with a 15Kbytes/s Continuous Bit Rate (CBR) stream. In the other hand, file transfer application is designed to maximize the TCP throughput using the highest available bandwidth between the connections. The Figure 4 presents the simulation topology and the wireless profile that is modeled using OMNeT++. The simulation is also an indication to the behaviors of the femtocell backhaul which is partly wireless (UMTS) and partly wired. The following measurements were obtained assuming the background traffic does not interfere the traffic originated from the femtocells. We use long-range WLAN in the wireless potion of the backhaul between the relay antenna and the base station. For the evaluation, we assume an average distance of 0.5km between two consecutive base stations. The base stations besides the track make a corridor of radio coverage. The Brighton to London express trains also use WiMAX in the wireless backhaul with 10-15 seconds of gaps in between [18].

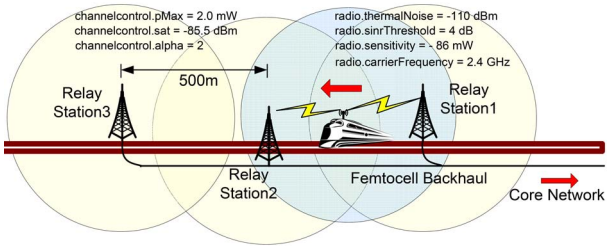

Fig. 4. Simulation model.

However, this solution is expensive and needs WiMAX base stations that are installed besides the rail tracks. WiFi is an inexpensive and flexible wireless access technique compared to WiMAX. The simulation results make out the fact that WiFi can also provide a satisfactable service with 10-15 seconds gaps during the consecutive handover. In the following text, we present the results that are obtained based on the simulation model.

The actual handover delay mainly consists of the time to configure an IP address by means of stateless auto-configuration. HIP uses UPDATE exchange that is of three messages to re-configure new addresses. Followed by the third update packet, femtocell begins to transmit ESP encapsulated data encrypted with the session key generated out of the same keying material shared during the BEX. The Router Advertisement (RA) interval critically affects on the handover latency. Mobile IP and HIP makes use of the existing RA and Router Solicitation (RS) messages. The graphs in Figure 5 were obtained over a simulated vehicular femtocell which was moving at a average speed of 72kmph (20mps). We have defined the handover latency as the time elapsed between loosing connection from one associated base station to send out the third update packet. In this kind of dilemma, RA interval must be optimized, since smaller intervals can result flooding network with unnecessary RAs. The Figure 6 depicts

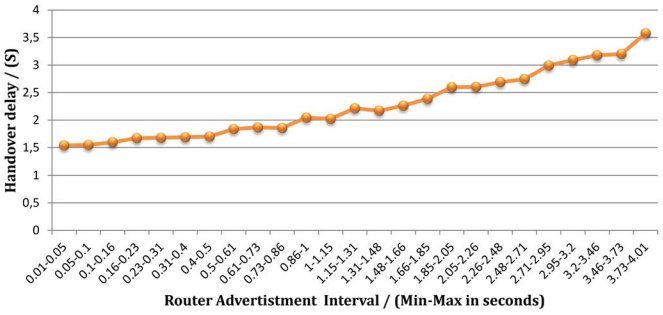

Fig. 5. Handover latency vs. Router Advertisement Interval (Min/Max).

UDP packet loss behavior of vehicular femtocell. We use the described VOIP application to generate 80 bytes packets. The measurements were obtained repeating the simulation over hundred 1000s sessions. We assume the maximum allowable backhaul capacity for single user to be 2.6Mbps. The performance evaluation was done for an user who was connected with the vehicular femtocell. From the results, we notice the

handover frequency has a huge impact on the packet loss. The second set of simulations was obtained by assuming a multihomed backhaul. Multihoming reduces the packet loss by establishing several associations at a time. Thus, termination of an association at a time does not significantly affect the packet loss, since the remaining associations can still transfer the data. At last, the Figure 7 presents the relationship between

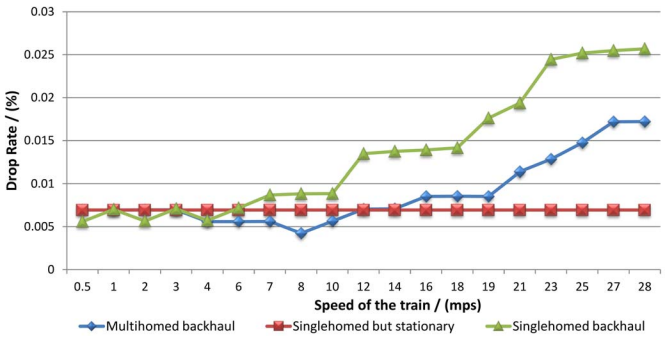

Fig. 6. Drop rate vs. speed of the train.

throughput and speed. We have used a TCP file transfer application in OMNeT++ to generate packets. The results reflect the average throughput behavior over a period of 1000s. The same network topology is used with singlehomed and multihomed approaches. We also compare the throughput for stationary and mobile users. However, throughput is hindered by the handover. We notice a drastic drop of throughput with singlehomed approach. In the other hand, a slight drop is noticed with the multihomed approach. It must be stated here that the throughput is always higher with multihomed approach. Further, it reflects an interesting linear relationship between throughput and the speed of the femtocell.

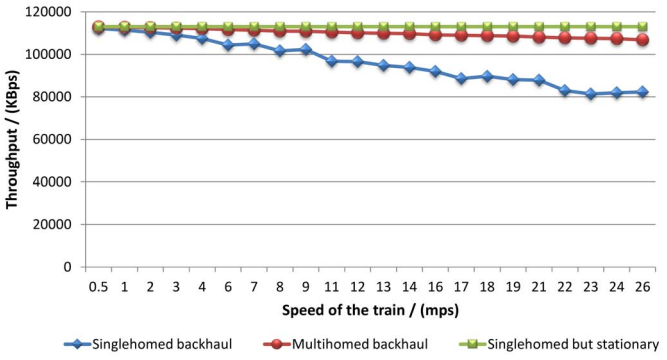

Fig. 7. Throughput vs. speed of the train.

VI. Conclusion

In this paper, we introduce a HIP based secure vehicular femtocell scenario. HIP supports secure authentication, fast re-authentication, key-exchange, replay protection and protection against certain DoS and MiTM attacks. With multihoming, we could improve the consistency of throughput. As of the results, we notice a 123% of throughput increment and 40% of decrement in packet drop compared to the singlehomed approach for a vehicular femtocell which is moving at an average speed of 72kmph (20mps). Furthermore, we notice this difference is more significant when speed is high. In future, we will investigate a fast re-authentication mechanism for vehicular femtocells to reduce the packet loss and handover latency.

Acknowledgment

The authors would like to thank the partners of the Celtic MEVICO project for all fruitful discussions and their valuable advice on writing this paper.

References

[1] N. S. Networks. (2011) Thalys high speed train passengers enjoy broadband internet access. [Online]. Available: http://www.nokiasiemensnetworks.com/sites/default/files/document/45396726766.pdf

[2] S. Gingichashvili. (2009) High-speed internet intrains. [Online]. Available: http://thefutureofthings.com/news/6297/high-speed-internet-in-trains.html

[3] A. Tung. (2011) Internet to be available on high-speed trains. [Online]. Available: http://usa.chinadaily.com.cn/us/2011-03/10/content_12150489.htm

[4] 3GPP, *33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB), ver 11.0.0 (2010-12)*.

[5] I. Bilogrevic, M. Jadliwala, and J. Hubaux, "Security Issues in Next Generation Mobile Networks: LTE and Femtocells," in *2nd International Femtocell Workshop, Luton, UK*. Citeseer, 2010.

[6] D. Knisely, T. Yoshizawa, and F. Favichia, "Standardization of Femtocells in 3GPP," *Communications Magazine, IEEE*, vol. 47, no. 9, pp. 68–75, 2009.

[7] B. Ray. (2010) Femtocells wilt under attack. [Online]. Available: http://www.theregister.co.uk/2010/02/02/femtocell_security/

[8] P. Bright. (2011) Insecure vodafone femtocells allow evesdropping, call fraud. [Online]. Available: http://arstechnica.com/security/news/2011/07/insecure-vodafone-femtocells-allow-eavesdropping-call-fraud.ars

[9] C. Kaufman *et al.*, "Internet key exchange (ikev2) protocol, draft-ietf-ipsec-ikev2-17. txt," *IETF, work in progress*.

[10] T. Kivinen and H. Tschofenig, "Rfc 4621: Design of the ikev2 mobility and multihoming (mobike) protocol," *Network Working Groupt, August*, 2006.

[11] T. Aura, A. Nagarajan, and A. Gurtov, "Analysis of the hip base exchange protocol," in *Information Security and Privacy*. Springer, 2005, pp. 481–493.

[12] P. Nikander, A. Gurtov, and T. Henderson, "Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks," *Communications Surveys & Tutorials, IEEE*, vol. 12, no. 2, pp. 186–204, 2010.

[13] T. Heer, "Host Identity Protocol Certificates," 2011.

[14] U. Maurer, "Modelling a public-key infrastructure," in *Computer SecurityESORICS 96*. Springer, 1996, pp. 325–350.

[15] J. Melen, P. Salmela, and J. Ylitalo, "Security parameter index multiplexed network address translation (spinat)," *IETF Draft, April*, 2010.

[16] A. Varga, "OMNeT++," *Modeling and Tools for Network Simulation*, pp. 35–59, 2010.

[17] L. Bokor, S. Novaczki, L. Zeke, and G. Jeney, "Design and evaluation of host identity protocol (HIP) simulation framework for INET/OMNeT++," in *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*. ACM, 2009, pp. 124–133.

[18] B. Wilson. (2005) Rail internet access picks up speed. [Online]. Available: http://news.bbc.co.uk/2/hi/business/4363196.stm