ENSC835: COMMUNICATION NETWORKS

SPRING 2011

FINAL PROJECT

Mobile IP versus IPsec Tunneling with MOBIKE: A Comparison Under Wireless Vertical Handover With NS-2

http://www.sfu.ca/~cdk4

Christopher Kilgour

301106137

cdk4@sfu.ca

Team #1

Abstract

Mobile devices are increasingly including support for multiple heterogeneous wireless networks like 3G cellular, 4G, and IEEE 802.11. When an IP-equipped mobile device attaches to a network, it typically obtains a temporary network address allocated by the visited network provider. One approach to provide a permanent IP address to a mobile device is Mobile IP. Mobile IP has some objectionable aspects: it often requires network provider support, and it can drop data during vertical handover. IPsec tunneling with IKEv2 Mobility and Multihoming Protocol (MOBIKE) may be used as an alternative to Mobile IP. IPsec tunnels do not require any special support from the network provider. Because it supports multi-homing, MOBIKE can provide make-before-break operation, eliminating the data interruption during vertical handover. The ns-2 simulation tool is enhanced, and a comparison of vertical handover scenarios is performed, in this report.

Table of Contents

List Of Figures

List of Tables

Introduction

Modern internet-enabled computers, like smart phones, PDAs, and laptops, include multiple radios that provide access to heterogeneous wireless networks. A vertical handover occurs when switching between these different networks. Often a vertical handover results in the internet attachment point changing, with a new IP address assigned to the mobile's wireless link.

Vertical handover IP mobility scenarios may be studied with network simulation tools. The ns-2 (network simulator 2) software package provides support for Mobile IP, but does not provide support for alternate mobility and tunneling strategies such as IPsec. This paper describes enhancements to ns-2 (version 2.34) for rudimentary Internet Key Exchange version 2 (IKEv2), and then, using this new support, demonstrates vertical handoff simulation under these different tunneling strategies.

IP Mobility And Tunneling

This section describes the pertinent IP mobility and tunneling standards to support the later sections of this document. This section is intended for readers familiar with internet protocol networking, but unfamiliar with the details of Mobile IP, IPsec, IKEv2, or MOBIKE.

Mobile IP

Mobile IP for IPv4 is described in [10] and a sample topology is depicted in Figure 1 (heavy black lines indicate IP tunnels). IP mobility is provided by allowing a mobile node (MN) to retain a permanent IP address, and by maintaining the configuration of certain fixed internet hosts responsible for datagram delivery.

A fixed host on the internet acts as the home agent (HA) for the for the mobile node, where internet routing tables ensure packets destined for the MN are delivered to the HA.

Visited networks supporting Mobile IP advertise such support with broadcast datagrams, and provide at least one foreign agent (FA) for the mobile node. When changing attachment, the MN interacts with the local FA and the HA to update datagram delivery parameters. That way, datagrams forwarded to the home agent, but destined for the MN, may be tunneled to the foreign agent, where they are ultimately delivered to the mobile node via its temporary address. Datagrams transmitted to the internet by the MN need not be tunneled to the HA, but do need to be formatted specially so the visited network will forward them to the intended internet destination.

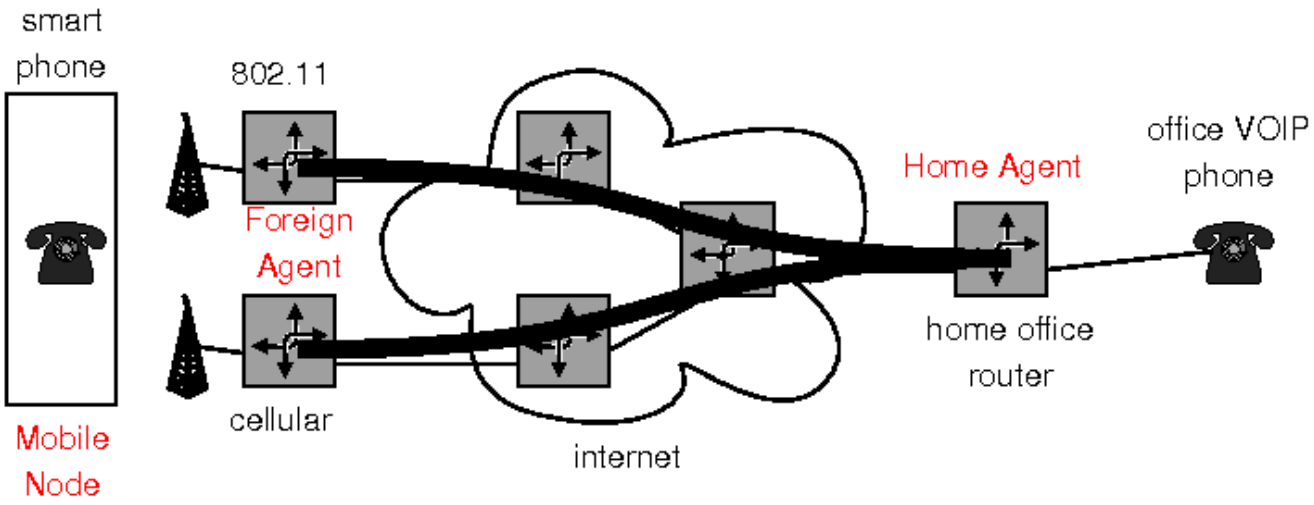


Figure 1: Example Mobile IP Topology

An optional variation of Mobile IP is to have the mobile node effectively act as its own foreign agent. Mobile IP support by network providers varies, so often it may be necessary for a MN to forgo external FA support. This can complicate the logic, and therefore increase the required sophistication of the MN, its software, and its user.

Data drops occur during vertical handover when using Mobile IP. When a mobile node supporting

Mobile IP changes network attachment, the update interchange between the MN, FA, and HA can take quite some time. Normally this interchange is carried across the new visited network, with the mobile node dropping the connection to the previous visited network. While the FA and HA are being updated on the new visited network, and the agents continue to use the previous visited network, datagrams cannot be exchanged between the MN and other internet hosts. This results in a data drop out period affecting any active network applications on the mobile node. Certain applications, especially streaming media applications, halt operation during such data drops.

In addition to inconsistent network support and data drops, Mobile IP operates entirely in the clear. This means that datagrams exchanged with the mobile node are subject to various security threats. A MN is free to use secure methods at the application layer, but Mobile IP itself, and often many applications' datagrams, will contain clear payloads. Given that Mobile IP is often applied in wireless networks, the security risks include passive sniffing, replay attacks, and man-in-the-middle attacks.

IPsec with IKEv2

The internet protocol security architecture (IPsec) is described in [11] and a sample tunneling topology depicted in Figure 3. Two modes of operation are defined: transport mode and tunneling mode. Transport mode is primarily concerned with security provided at (fixed) internet endpoints. The IP mobility aspects discussed in this paper focus on IPsec tunneling mode (the heavy black lines in Figure 3 indicate tunnels).

Two security protocols apply to IPsec datagrams: authentication header (AH) and encapsulating security payload (ESP) [12]. Of these, only ESP provides data confidentiality, and is the primary protocol considered in this paper. Figure 2 shows an example IPsec/ESP datagram. Prior to transmission, the original datagram gets encrypted and is shown in grey. IPsec/ESP generates authentication and management fields shown in yellow, and transmits the result as a new IP datagram with the destination address set to the tunnel endpoint.

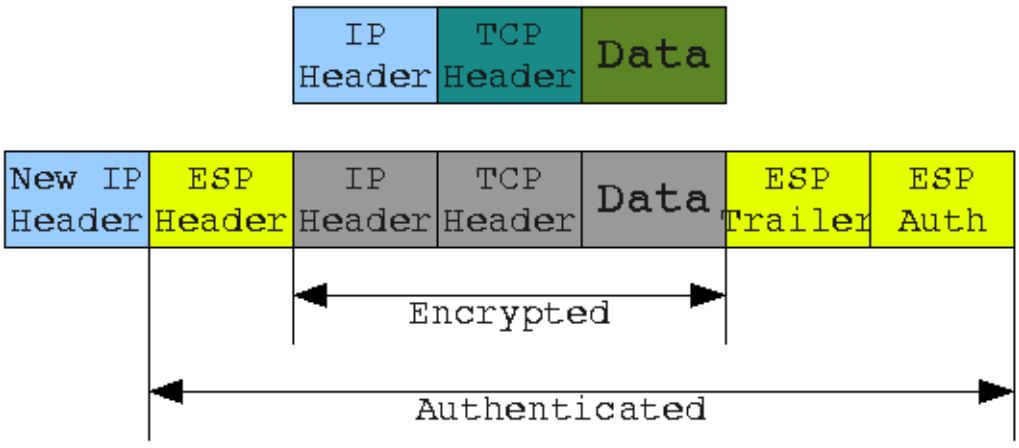


Figure 2: IPsec Encapsulating Security Payload Example

In order for IPsec to provide the intended authentication and confidentiality guarantees , specific selections from the large body of well-known security procedures are negotiated between peers before traffic flow begins. Fundamental to the selection of security procedures and parameters is the Internet Key Exchange (IKEv2) [13]. A security association (SA) between IPsec peers represents a set of security parameters in active use, and IKEv2 is used to establish the SA.

IKEv2 distinguishes between the two IPsec peers by labeling one the *initiator* and the other the *responder*. As implied their names, the initiator initiates the establishment of each security association, and the responder complements the initiator.

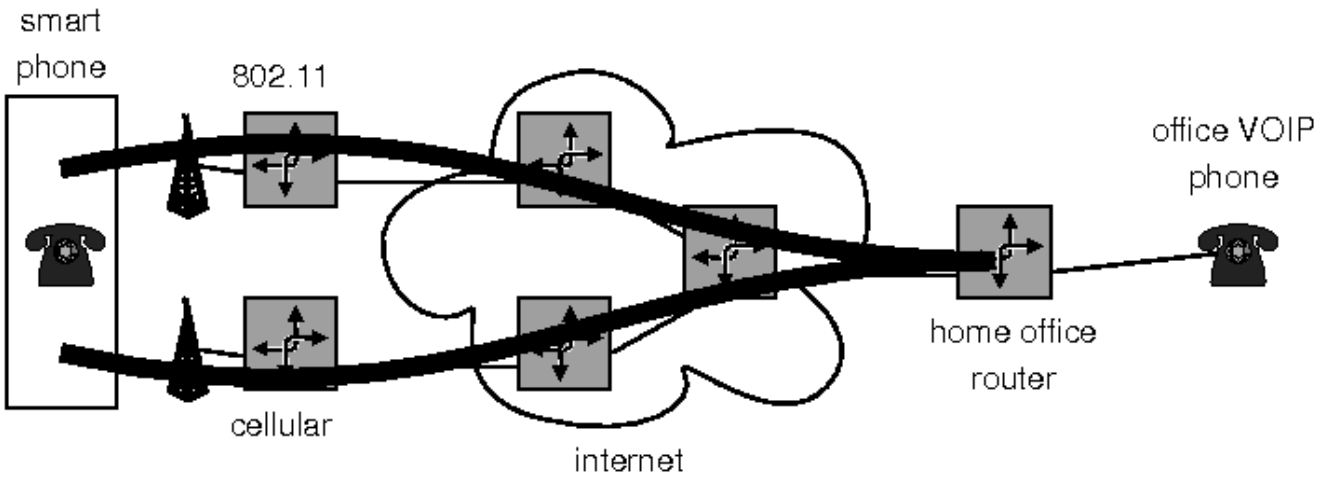


Figure 3: Example IPsec Tunnel Topology: Smart Phone Initiator, Home Office Router Responder

In the most straightforward situation, six IKEv2 exchanges are required to establish each new security association. An example of this straightforward situation is shown in Table 1. The first four exchanges establish the peers' authenticity, generate a shared-secret, and complete an initial IKE-only security association. The final two exchanges generate a child SA that is applicable to for example the tunneled internet traffic of the peers.

Step	IKEv2 Initiator Request		IKEv2 Responder Response
1	IKE_SA_INIT	►	
2		◄	IKE_SA_INIT
3	IKE_AUTH	►	
4		◄	IKE_AUTH
5	CREATE_CHILD_SA	►	
6		◄	CREATE_CHILD_SA

Table 1: Example IKEv2 Exchanges Leading To Security Association Establishment

IKEv2 exchanges are carried over the User Datagram Protocol (UDP), and are therefore susceptible to unreliable delivery. Consequently, IKEv2 procedures apply timer-based and state-based retransmission to ensure delivery of IKEv2 exchanges. The IKEv2 exchange names are consistent with protocol engineering terminology: the initiator transmits *requests*, and the responder transmits *responses*.

The SA established by the IKEv2 exchanges determines the security procedures and parameters used for the IPsec traffic between the peers. When ESP tunneling is employed, the SA determines the cryptographic algorithms and keys employed for this IPsec traffic.

All IKEv2 exchanges and the associated IPsec traffic are protected by specified procedures, and are therefore not susceptible to the security flaws apparent in Mobile IP. However, IKEv2 and IPsec tunnels do not inherently support mobility. Indeed, the UDP-based IKEv2 exchanges, and the computational overhead required to establish security associations, can be more burdensome than Mobile IP procedures. For example, establishing a new security association in a vertical handover situation can be even more time consuming than Mobile IP.

MOBIKE

The IKEv2 Mobility and Multihoming (MOBIKE) Protocol is described in [14]. The MOBIKE specification addresses mobility by providing constraints and describing use cases for IKEv2, as applied to IPsec tunneling mode.

MOBIKE also defines connectivity tests that are used to monitor individual network paths. The IKEv2 initiator is responsible for selecting which network paths are active, reacting to path establishment and loss according to the path tests.

When both IKEv2 peers recognize MOBIKE support, multiple address-pairs may be simultaneously used for IKEv2 and IPsec tunnel traffic. This multi-homing is the key feature of MOBIKE that allows make-before-break operation during the vertical handover. Consequently, during vertical handover, MOBIKE can mitigate the burden of IPsec and IKEv2 procedures. The MOBIKE extension to IKEv2 was added in 2006.

Previous Work

Ns-2 has been used extensively by others to simulate mobility, especially with wireless networks. Especially interesting are previous approaches to simulating the mobility scenarios [7, 9] including vertical handoff [8].

Mobile IP support was added to ns-2 by Sun Microsystems in 1998, then enhanced over time by others [17]. The data drops apparent in the ns-2 Mobile IP implementation have been previously noted in [5].

IPsec support for ns-2 was examined previously in 2000 [1], but this examination was based on out-of-date IPsec and IKE specifications, and the authors did not publish their implementation. However, several of the authors' insights were valuable in the preparation of the ns-2 enhancements described in this report.

To this author's knowledge, modern IPsec packet formats and procedures, IKEv2, and MOBIKE have not been previously studied with ns-2. Further, the more modern ns-3 network simulator does not currently offer support for Mobile IP, and was therefore rejected for this project.

NS-2 Enhancements and Application

Two aspects of IPsec/ESP tunneling are required for ns-2: IPsec data traffic and IKEv2 security associations. Following the approach described in [1], IPsec data packet processing was simulated in ns-2 by adding processing delay at the IPsec nodes, and bloating the size of packet payloads.

Ns-2 was further enhanced to provide rudimentary IKEv2 agents. Both the initiator and responder were implemented as finite state machines. For each peer, each stable state within a mainstream six-exchange security association establishment was modeled. The exchanges are depicted in Figure 4.

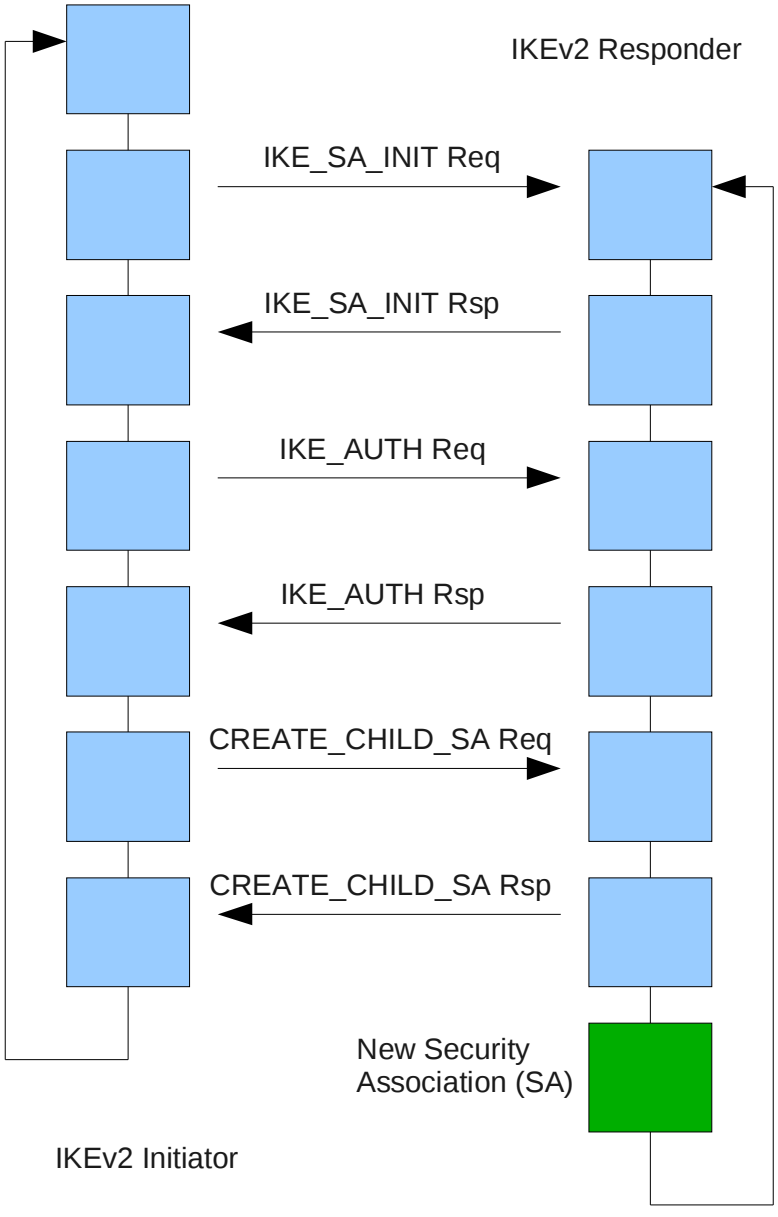


Figure 4: NS-2 IKEv2 Finite State Machine Model

To more accurately model IKEv2 exchanges, a processing delay is included in the state machine transitions. A nominal six-exchange process is modeled assuming a simple basic set of security parameters: IKEv2 base mode with mandatory protocol components only.

IKEv2 Initiator

The canonical IKE_SA_INIT exchange includes a Diffie-Hellman (D-H) key-generation phase which is relatively time consuming [1]. Generating the shared-secret dominates the delay time and is several orders of magnitude longer than verifying the shared-secret from the responder. The processing delay for the remainder of the exchanges are nominal and taken to be equal to the D-H shared-secret confirmation delay.

As per the protocol design in [13], only the IKEv2 initiator implements a retransmission timeout. A nominal value of 500ms is selected for retransmission. Each initiator request is considered confirmed when the IKEv2 responder's response is received.

IKEv2 Responder

Like the initiator, the IKEv2 responder simulates the D-H key-generation with a significant time delay. It also provides a processing delay for the remainder of the exchanges by adopting the D-H shared-secret confirmation delay.

Unlike the initiator, the IKEv2 responder does not utilize a retransmission timer. Instead, the responder will retransmit its last response whenever it receives a repeated request from the initiator (which the responder takes to indicate data loss).

Parameter Derivation

To estimate IPsec and IKEv2 processing delays, a reference PC platform was selected and benchmarked. That PC platform was compared to the performance of a typical smart phone to extrapolate the performance for the desired simulation scenarios [18]. The results of this comparison are shown in Table 2.

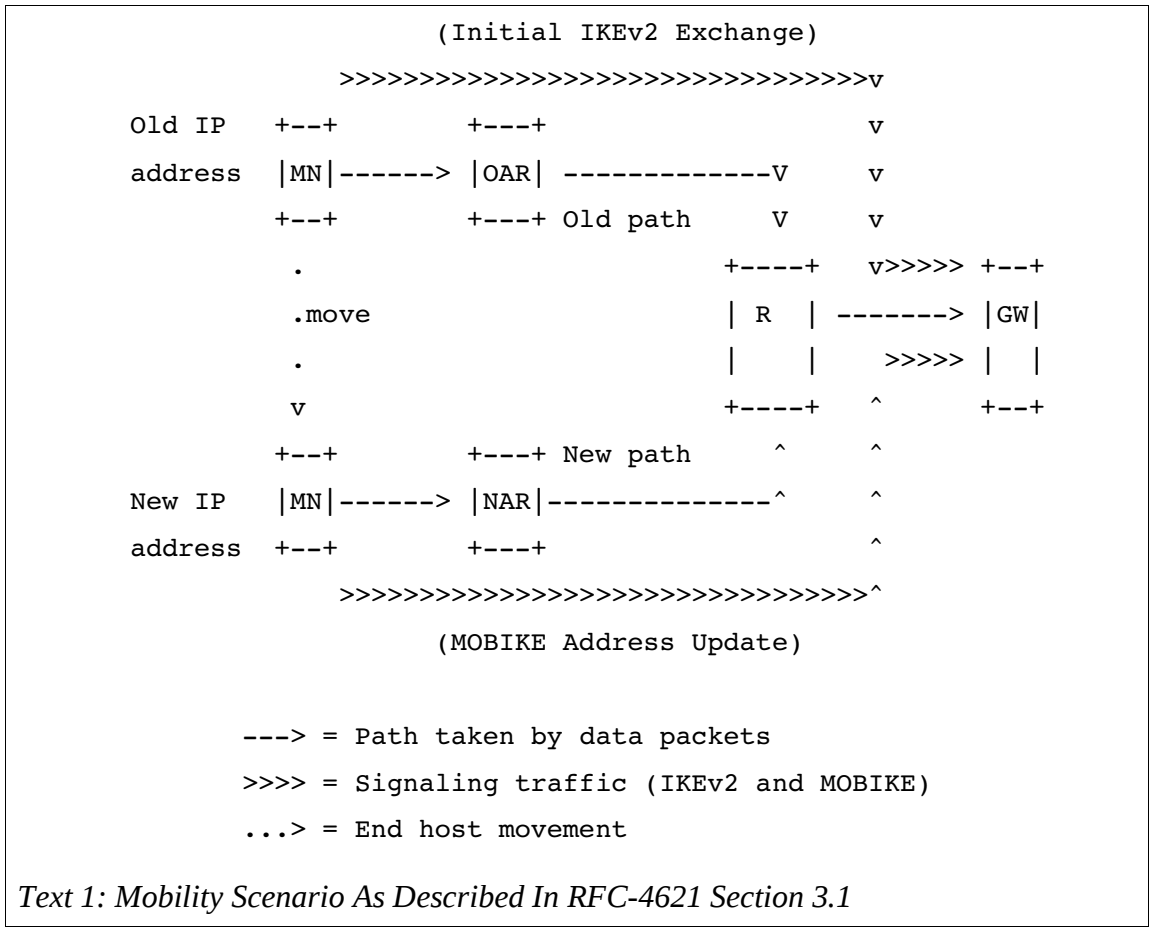
Platform	Diffie-Hellman Key Generation Duration	Diffie-Hellman Shared-Secret Check Duration
Reference PC	98.5 ms	0.092 ms
ARM-based Smartphone	3940 ms	3.85 ms

Table 2: NS-2 IKEv2 Finite State Machine Delay Parameters

The parameters derived in Table 2 were made the defaults for the new ns-2 IKEv2 implementation, but exposed as variables to allow for easy changes to the simulation. Increasingly accurate simulations could therefore be performed with actual device benchmarks as they become available.

Simulation Topology

The general simulation topology used in this report is shown in Figure 5. It is based on the scenario described in [15] section 3.1, which is reproduced below as Text 1.



Text 1: Mobility Scenario As Described In RFC-4621 Section 3.1

Constant-bit-rate (CBR) traffic representative of a VOIP connection was introduced between the office phone and the mobile smart phone of Figure 5. The coloured bar indicates the vertical handover pathway. The simulations all considered the mobile node initially connected to the cellular base station, migrating to the 802.11/WiFi access point.

In each case the CBR traffic was monitored at all simulated nodes. After a vertical handover simulation run, the ns-2 trace files were post-processed with a custom script to extract the CBR data for nodes demonstrating the traffic at the office phone, cellular network segment, and 802.11/WiFi network segment. The post-processed data was then used to generate the traffic graphs shown later in this report.

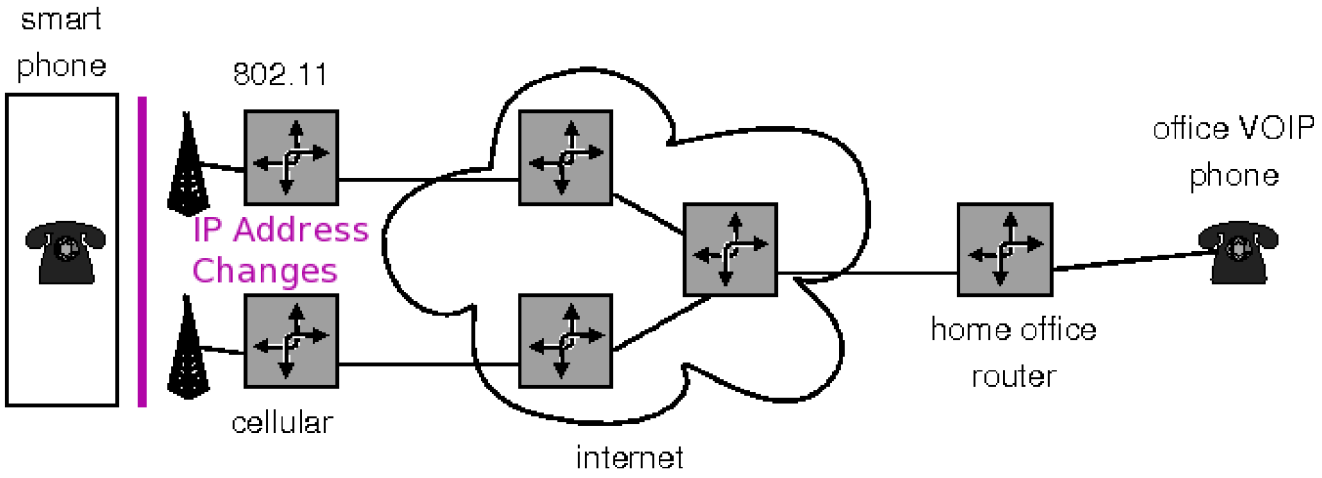


Figure 5: NS-2 IP Mobility Simulation Topology

Mobile IP

The stock Mobile IP support from ns-2 was used to provide a comparative reference for vertical handover. The topology used is shown in Figure 6. The simulation includes a smart phone wireless node that is initially within the coverage of the cellular base station, then migrates to the coverage of the 802.11/WiFi access point. The vertical handover occurs as the Mobile IP procedures detect the WiFi access point, and switch the active connection to WiFi.

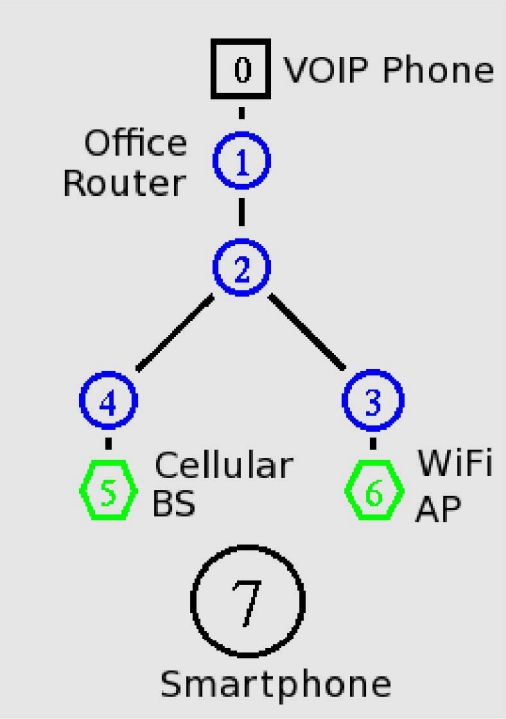


Figure 6: NS-2 Mobile IP Topology

IPsec with IKEv2

A similar topology to the Mobile IP simulation was utilized for vertical handover with IPsec using IKEv2, and is shown in Figure 7. The same topology was used for legacy IKEv2 break-before-make, and MOBIKE make-before-break scenarios.

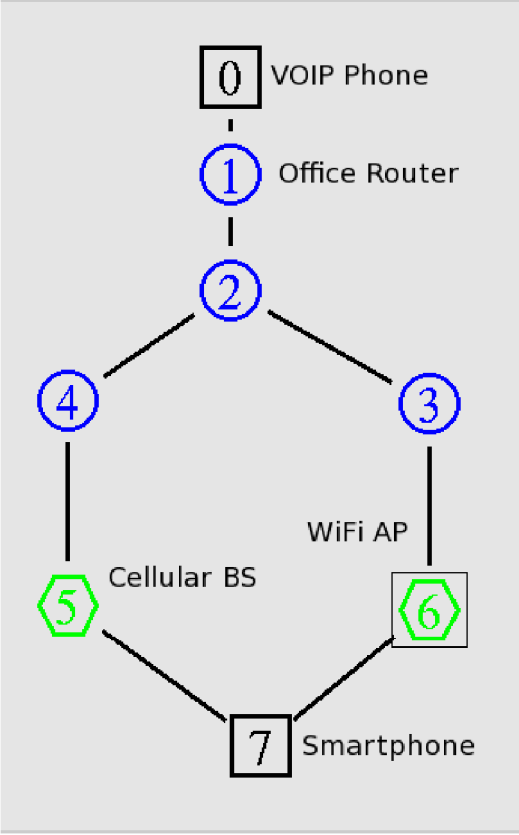


Figure 7: NS-2 IPsec: IKEv2 and MOBIKE Topology

A significant difference between the IPsec topology and Mobile IP is wired links being used for the smart phone. The simulation was not meant to demonstrate wireless performance under vertical handover, so a pseudo-wireless network was used. The pseudo-wireless links were taken to offer equivalent datalink performance to a wired system. The vertical handover was accomplished by manipulating these fixed links into up and down states at appropriate times.

The appropriate times for manipulating the links in the simulation were the start and end events of the IKEv2 security association exchange. The implementation of the IKEv2 initiator and responder agents provided for simulation script commands to be invoked at those state transitions. With simple modifications, this allowed the simulation script to determine whether break-before-make (legacy IKEv2) or make-before-break (MOBIKE) operation was applied.

Simulation Results

Vertical handovers were simulated in ns-2 for the three scenarios described above: Mobile IP, legacy IKEv2 break-before-make, and MOBIKE make-before-break. Of interest are the data drop periods that occur when the mobile node hands over from the cellular link to the 802.11/WiFi link. The respective simulation results generated by post-processing the simulation traces are shown in Figure 8, Figure 9, and Figure 10. The data drop periods revealed by simulation are listed in Table 3.

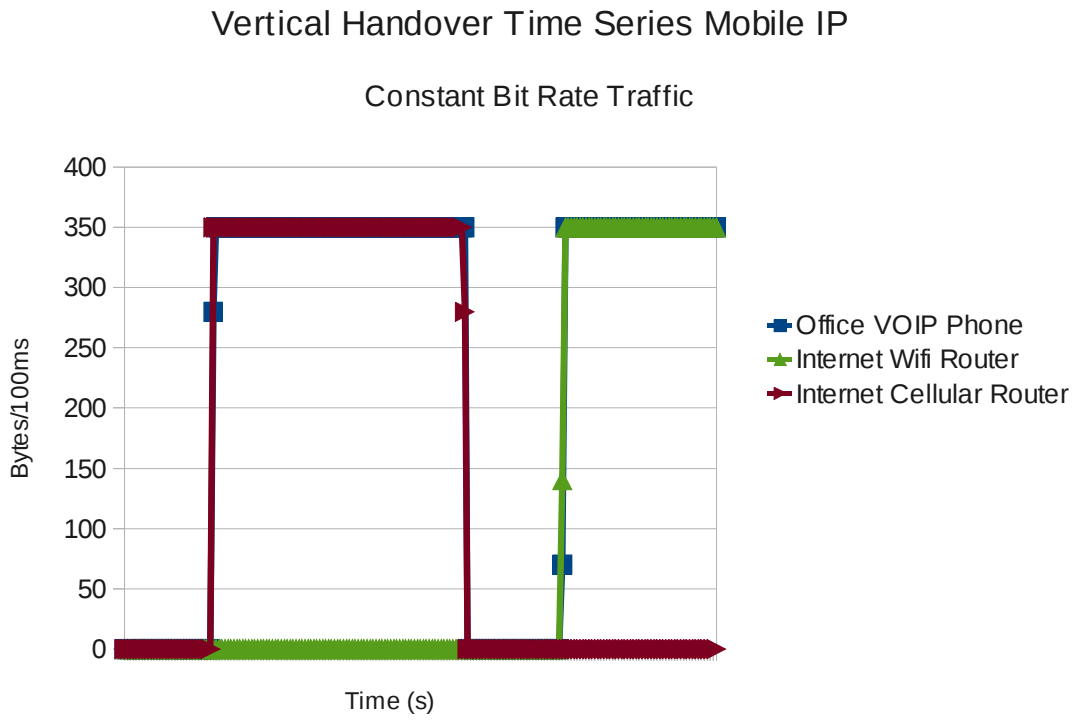


Figure 8: NS-2 Simulated Vertical Handover (Mobile IP)

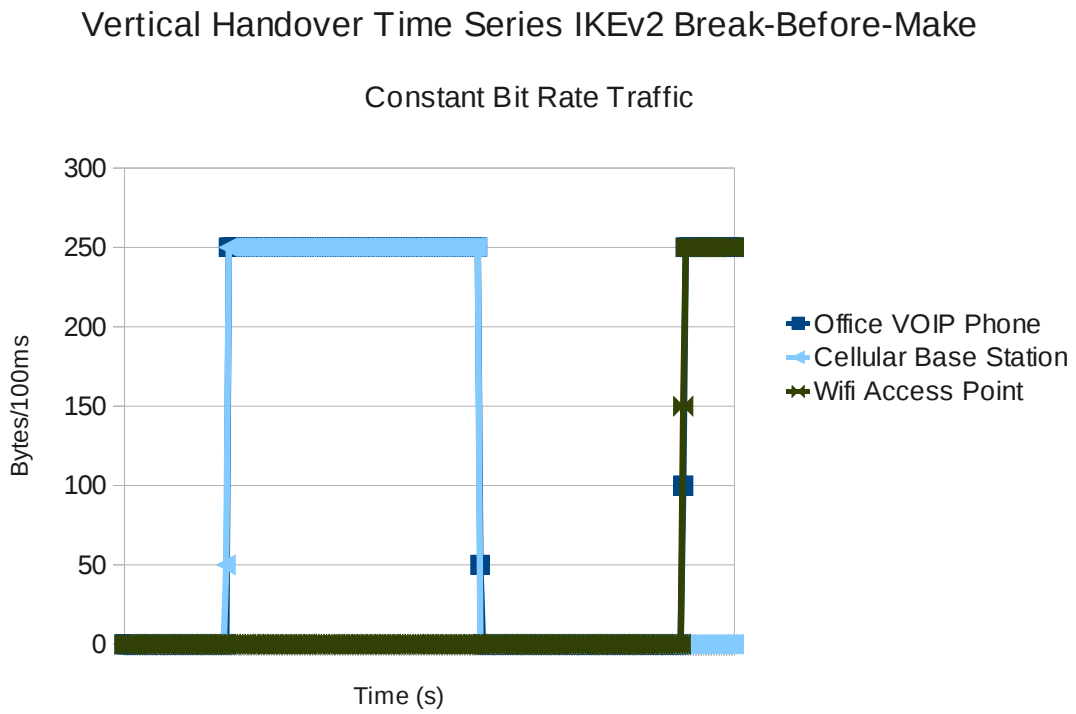


Figure 9: NS-2 Simulated Vertical Handover (IPsec, IKEv2)

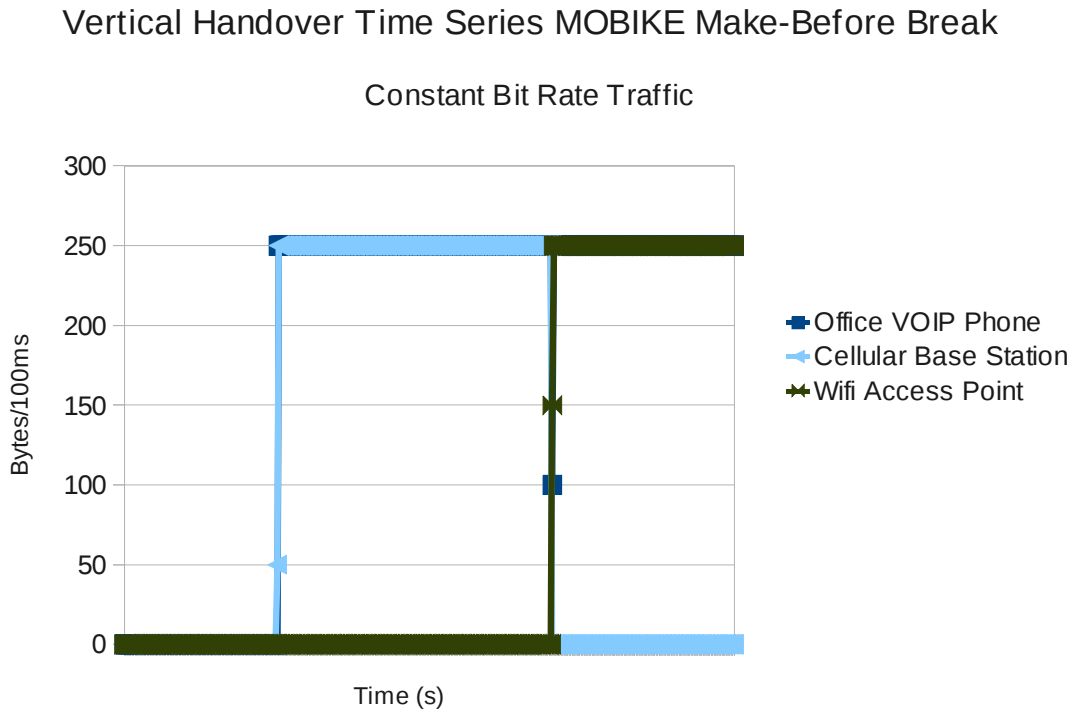


Figure 10: NS-2 Simulated Vertical Handover (IPsec, MOBIKE)

Topology	Data Drop Period
Mobile IP	3870 ms
IKEv2 break-before-make	8030 ms
MOBIKE make-before-break	0 ms

Table 3: NS-2 IP Mobility Data Drop Period Summary

Discussion

Several simulation runs were performed with ns-2 to demonstrate the three vertical handover scenarios of interest. The simulation results reveal that vertical handover under Mobile IP exhibits a data drop period of nearly four seconds. The break-before-make IKEv2 vertical handover simulation reveals that the extra processing overhead of IKEv2 security associations, and the minor delays imposed by IPsec, result in a data drop of over eight seconds. Finally, the make-before-break MOBIKE vertical handover simulation indicates that no data is dropped: a seamless handover is achieved. This verifies the enhancements to ns-2 allow the simulation of the expected results of the three vertical handover scenarios.

The author has real-world experience with IPsec tunnels and MOBIKE. Using Linux-based network nodes, and open-source IPsec IKEv2 daemons, seamless make-before-break vertical handover can be demonstrated. However, it is difficult and expensive to deploy large test beds, especially when including diverse wireless scenarios. A simulator-based approach is an enticing alternative, and the project described in this report is a step towards that capability.

The enhancement to ns-2 offered in this report can be used to simulate the performance of IPsec datagrams, and the overhead of security association establishment with IKEv2. Indeed, this model can demonstrate seamless vertical handover in the MOBIKE scenario. However, the ns-2 model described is basic, and only roughly captures the behaviour of IKEv2 in a straightforward operational sense. In reality, IKEv2 offers much more sophistication than captured in the current model. Further refinements may be made to the ns-2 model in order to improve the accuracy and applicability. Specifically:

- more sophisticated IKEv2 agents would allow the specific security association proposals and counter-proposals to be implemented, and this would lead to a more accurate simulation of IKEv2 overhead,
- a true model of IPsec/ESP tunneling would allow for the impact of various cryptographic algorithms to be studied,
- both the IKEv2 agents and IPsec/ESP tunnel simulations could be made to operate on multiple interfaces to better reflect real-world operation,
- the IKEv2 agents could specifically implement the procedures of MOBIKE, including path establishment and loss discovery, to study protocol details, and
- support for including the wireless ns-2 subsystems with IPsec could be added to support the study of datalink performance on the IPsec tunnels and IKEv2.

Conclusion

Vertical handover, especially in wireless environments, is an increasingly common occurrence on the internet, but data drops are common. Various tunneling strategies are available to facilitate IP mobility, and some strategies like MOBIKE facilitate seamless vertical handover. However, the ns-2 simulator support for these tunneling strategies has been lacking.

A rudimentary implementation of IKEv2 agents for ns-2 was described in this paper. The implementation is capable of representing the overhead of IKEv2 as well as the break-before-make and make-before-break tunneling capabilities of IPsec with MOBIKE. Combined with the native Mobile IP support, this paper demonstrated the use of ns-2 in studying vertical handover IP mobility scenarios, including the seamless scenarios as facilitated by MOBIKE.

References

1. J. Caldera, D. de Niz, and J. Nakagawa, "Performance Analysis of IPSec and IKE For Mobile IP on Wireless Environments", Information Networking Institute, Carnegie Mellon University, 2000
2. S. Itani, "Use of IPSec in Mobile IP", Engineering Term Paper, American University Of Beirut, Lebanon, 2001
3. X.P. Costa and H. Hartenstein, "A simulation study on the performance of Mobile IPv6 in a WLAN-based cellular network", *Computer Networks*, vol 40, pp191-204, 2002
4. X.P. Costa, M. Torrent-Moreno, and H. Hartenstein, "A Performance Comparison Of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their combination", *Mobile Computing and Communications Review*, vol 7, no 4, 2004
5. T. Janevski, "Analysis of Mobile IP for NS-2", *16th Telecommunications Forum TELFOR 2008*, in Belgrade, Serbia, November 2008
6. Q.Qui, D. Zhang, J. Ma, "GPRS network simulation model in NS-2", *Communications, 2004 and the 5th International Symposium on Multi-Dimensional Mobile Communications Proceedings*, 29 August – 1 September, 2004
7. A. Gurtov, S. Floyd, "Modeling Wireless links for Transport Protocols", *ACM CCR*, 34(2):85-96, April 2004
8. A. Gurtov, J. Korhonen, "Effect of Vertical Handovers on Performance of TCP-Friendly Rate Control", *ACM Mobile Computing and Communications Review*, 8(3):73-87, July 2004
9. C. Palazzi, B. Chin, P. Ray, G.Pau, M.Rocetti, "High Mobility in a Realistic Wireless Environment: a Mobile IP Handoff Model for NS-2", *Proc. of IEEE TRIDENTCOM 2007*, Orlando, FL, USA, May 2007
10. C.Perkins et al, "IP Mobility Support for IPv4", IETF RFC-3344, The Internet Society, 2002
11. S. Kent et al, "Security Architecture for the Internet Protocol", IETF RFC-4301, The Internet Society, 2005
12. S. Kent et al, "IP Encapsulating Security Payload (ESP)", IETF RFC-4303, The Internet Society, 2005
13. C. Kaufman et al, "Internet Key Exchange (IKEv2) Protocol", IETF RFC-4306, The Internet Soceity, 2005
14. P. Eronen et al, "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", IETF RFC-4555, The Internet Society, 2006
15. T. Kivenen et al, "Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol", IETF RFC-4621, The Internet Society, 2006
16. S. Frankel, Demystifying the IPsec Puzzle, Norwood, MA, Artech House, 2001, pp 87-127
17. "The Network Simulator - ns-2", http://www.isi.edu/nsnam/ns/ [accessed April 2011]
18. "eBACS: ECRYPT Benchmarking of Cryptographic Systems", http://bench.cr.yp.to/results-dh.html [accessed April 2011]