

國立交通大學

資訊學院 資訊學程

碩士論文

MIPv6 透過選擇性起始位址及路徑之位置更新認證研究



Binding Update Authentication through Selective Source Address
and Routing Path in MIPv6

研究生：呂威德

指導教授：蔡文能 教授

中華民國九十六年七月

MIPv6 透過選擇性起始位址及路徑之位置更新認證研究
Binding Update Authentication through Selective Source
Address and Routing Path in MIPv6

研究生：呂威德

Student : Wei-De Lu

指導教授：蔡文能

Advisor : Wen-Nung Tsai

國立交通大學

資訊學院 資訊學程



碩士論文

A Thesis

Submitted to College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Computer Science

June 2006

Hsinchu, Taiwan, Republic of China

中華民國九十六年七月

國立交通大學資訊學院 資訊學程碩士班

中文摘要

MIPv6 是下一代的行動 IP 網路通訊協定，它是在 IPv6 網路通訊協定下所作的延伸，有鑑於 MIPv4 在傳統 IPv4 的網路架構下的複雜延展，MIPv6 在路徑繞送做了相當的簡化，由改良 MIPv4 的客端代理 (Foreign Agent) 的間接轉送，轉變為移動點 (Mobile Node) 與本籍代理者 (Home Agent) 的直接聯繫，因為少掉了客端代理的轉送機制，相對簡化了移動點與本籍代理及通訊節點 (Correspond Node) 間，溝通時的複雜度及延遲。MIPv6 繼承了 IPv6 的特性，除了在 IP 位址不足的問題做了解決之外，對其安全性、擴充性、服務品質等方面的弱點也做了改善，並針對 MIPv4 做了許多改進。

在行動設備高速成長趨勢之下，將對現行的網際網路帶來衝擊。讓人類的從溝通型態、娛樂方式、交易/消費行為有了戲劇性的變革，進而改變了許多現代人的生活模式；而這些變革也同時對網際網路帶來不斷推陳出新、且非實體性的攻擊與資訊竊奪，成為網路科技進步下的的陰影，造成人們對於網際網路的安全有著莫大的恐慌和疑慮。有

鑑於此，許多專家學者紛紛提出防禦及保護的技術及研究，特別是針對行動技術的安全性研究上。畢竟，IP 網路的未來是 Mobile IP 的世界，而因應 MIPv6 的安全性所做的防禦措施是必要且急迫的。事實上，MIPv6 在設計之初，便考量援用 IPv6 內建的安全性協定(IPSec)，然而在 PKI 發展遲滯的狀態之下，讓專家學者不得不尋求過渡性方案，或者是替代性的方案。然而，在沒有周慮的安全考量下，對許多的新興的網路服務而言，都可能會是個很大的障礙。

本篇論文將針對已發覺 MIPv6 位置更新時的安全性弱點提出解決方案，讓移動中的行動點能夠透過 Multiple source address 及 Seletive routing path 的 RR Test 認證機制，來防止駭客偽造行動點，及進行 Man in the middle 方式的攻擊，裨益 CN(Correspond Node)在更新 CoA 的位置資訊快取時，得到可靠的確認；在相容於現有之 RR Test 認證機制並整合 SCTP multi-homing 技術之研究下，提出一些新的概念及想法，冀望對於 MIPv6 在安全性的研究上能有所貢獻。

關鍵字：MIPv6，Binding Update，安全性。

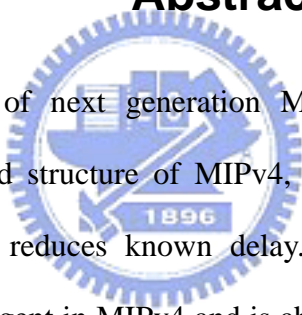
Binding Update Authentication through Selective Source Address and Routing Path in MIPv6

Student : Wei Der Lu

Advisor : Prof. Wen-Nung Tsai

Degree Program of Electrical Engineering Computer Science
National Chiao Tung University

Abstract

The logo of National Chiao Tung University is a circular emblem with a gear-like border. Inside the circle, there is a stylized blue figure holding a torch, with the year '1896' written below it.

MIPv6 is the protocol of next generation Mobile IP, extending from IPv6. In consideration of complicated structure of MIPv4, MIPv6 makes a progress in routing optimization which greatly reduces known delay. Through simplifying routing path, MIPv6 eliminates Foreign Agent in MIPv4 and is able to communicate with Home Agent and Correspondent Node directly. MIPv6 inherits characteristics from IPv6, like solving insufficient address problem, improving vulnerability in IPv4 security, enhancing extensibility, reforming several Qualities of Services issues and, above all, greatly changing the infrastructure of MIPv4.

Rapid growing of mobile devices brings great impact to current Internet ecosystem and dramatically changes our lifestyle, such as the way we communicate, entertain, conduct business and consume. At the same time, this kind of change brings out non-physical Internet attack and information stealing that cast the shadow on human beings for the fear of unsecure trading, privacy prying and even personal properties tampering as Internet technology grows. In response to this fear, experts and scholars devote their researches to

the protection and the defensive mechanisms against known weaknesses, especially those on mobile networks. Eventually, the future of IP network is mobility. It's imperative to work out a good way for resolving security issues while facing the future of mobility. In fact, at the very beginning of designing IPv6, researchers already envision of what future network will be. There are numerous IAs (Intelligent Appliance) with a variety of functions: autoconfiguration, network sensibility, infrastructureless, mobility, and carrying multimedia capability. Those infinite creativity encourages us to develop more and more products and features. Nevertheless, without sound security, all of them will become mere nightmares.

This thesis aims at solving the known vulnerability of current MIPv6. By changing source IP address and selecting routing path, our approach prevents the hacker from forging the source IP address or eavesdropping packets through Man-in-the-middle attack. This kind of enhanced RR Test results in a more stringent authentication which inherits the original RR Test and integrate Multi-homing feature of SCTP. Consequently, this thesis has certain contributions toward academic research.

誌 謝

這篇碩士論文能夠完成，首先感謝我的指導教授——蔡文能教授。在我論文寫作期間，給予我許多知識上的啟發以及學業上的指導。此外，謝謝明傑學長、同學們熱心的討論與幫忙，以及內人兆慧、小犬庭羽及我的母親這段時間來給我的支持與體諒。



Index

| | |
|--|------|
| 中文摘要..... | iii |
| Abstract..... | v |
| 誌謝..... | vii |
| Index..... | viii |
| List of Tables..... | ix |
| List of Figures..... | i |
| Chapter 1 Introduction..... | 1 |
| 1.1 Motivation..... | 1 |
| 1.2 Research focus..... | 3 |
| 1.3 Thesis Organization..... | 3 |
| Chapter 2 Background..... | 5 |
| 2.1 Mobile IPv6 overview..... | 5 |
| 2.1.1 Mobile IPv6..... | 5 |
| 2.1.2 Route Optimization..... | 9 |
| 2.1.3 Return Routability..... | 10 |
| 2.2 SCTP (Stream Control Transmission Protocol)..... | 14 |
| 2.3 Threat and Defense in MIPv6..... | 17 |
| 2.3.1 Current Threat in MIPv6..... | 18 |
| 2.3.2 Defense in MIPv6..... | 21 |
| Chapter 3 Related Work..... | 25 |
| 3.1 Self-Certifying Address..... | 25 |
| 3.2 Enhancing Return Routability..... | 31 |
| 3.3 Mobile SCTP (mSCTP) for IP mobility..... | 33 |
| Chapter 4 Selective Source and Routing Path..... | 38 |
| 4.1 Message Flow..... | 38 |
| 4.2 Protocol Specification..... | 40 |
| 4.3 Processing Bindings..... | 45 |
| 4.4 Reduce probabilities of compromise..... | 48 |
| Chapter 5 Simulation and experimental result..... | 53 |
| 5.1 Environment and simulation scenario..... | 53 |
| 5.2 Experimental Result..... | 55 |
| 5.3 Discussion and Limitation..... | 67 |
| Chapter 6 Conclusion and Future Work..... | 70 |
| 6.1 Conclusion..... | 70 |
| 6.2 Future work..... | 71 |
| References..... | 73 |

List of Tables

| | |
|--|----|
| Table 1 Mobility Header | 40 |
| Table 2 Mobility Header Type..... | 41 |
| Table 3 Hit ratios by increasing nodes | 49 |
| Table 4 Hit ratios by increasing HA nodes | 50 |
| Table 5 Hit ratios by increasing HA nodes but by fixing MN to 3..... | 51 |
| Table 6 Wired format..... | 60 |
| Table 7 Symbol explanation..... | 61 |
| Table 8 Collection of successful RR Test..... | 61 |
| Table 9 Binding latency of two different interfaces | 62 |
| Table 10 Collection of multi-homed interface- interface 1 | 64 |
| Table 11 Collection of multi-homed interface- interface 2..... | 64 |
| Table 12 Latency of HoTI-HoT/CoTI-CoT for interface 1 and interface 2..... | 65 |
| Table 13 Comparison of successful BU to CN between single-homed and multi-homed interface..... | 67 |



List of Figures

| | |
|--|----|
| Figure 1 Environment of MIPv6 | 6 |
| Figure 2 Route Optimization..... | 10 |
| Figure 3 Return Routability of MIPv6 | 12 |
| Figure 4 SCTP in transport layer..... | 14 |
| Figure 5 multiple message-streams of SCTP | 15 |
| Figure 6 Byte-stream vs. message-stream | 15 |
| Figure 7 SCTP protocol stack | 16 |
| Figure 8 CGA packet format | 27 |
| Figure 9 CAM structure | 28 |
| Figure 10 CGA format with sec fields..... | 28 |
| Figure 11 HIP packet structures | 36 |
| Figure 12 HIP establish connection..... | 36 |
| Figure 13 message flow..... | 39 |
| Figure 14 Structure of the Mobility extension header | 41 |
| Figure 15 Home Test Init message | 42 |
| Figure 16 Care of Test Init message | 42 |
| Figure 17 Care of Test message..... | 42 |
| Figure 18 Binding Update message..... | 43 |
| Figure 19 the structure of the new Type 2 Routing header (from cisco) | 44 |
| Figure 20 Packet between two Mobile Nodes (from cisco) | 45 |
| Figure 21 Selective Source address and Routing Path | 47 |
| Figure 22 Equation..... | 48 |
| Figure 23 Hit ratios by increasing node | 49 |
| Figure 24 Hit ratios by increasing HA and by fixing MN to 1 | 50 |
| Figure 25 Hit ratios by increasing HA and by fixing MN to 3 | 51 |
| Figure 26 Scenario of MN movement..... | 54 |
| Figure 27 Data packets sent by CN to MN indirectly via HA..... | 55 |
| Figure 28 Binding process dump | 58 |
| Figure 29 raw data of trace file | 58 |
| Figure 30 Latency of HoTI-HoT and CoTI-CoT..... | 62 |
| Figure 31 Latency of RR Test | 63 |
| Figure 32 Latency between RR Test and movement registration to HA | 64 |
| Figure 33 Latency of HoTI-HoT/CoTI-CoT for interface 1 and interface 2 | 65 |
| Figure 34 BU variance of interface 1 and interface 2..... | 66 |
| Figure 35 Latency between interface1 and interface 2..... | 67 |
| Figure 36 Comparing complete BU during specific time period of single and multi-homed interface..... | 67 |

Chapter 1 Introduction

Due to the popularization of numerous portable devices and the desire of having continuous Internet connectivity regardless of the mobile device's physical position, location information update and management of mobile network are becoming increasingly important. Accordingly, Mobile IPv6 [1] is developed as a subset of Internet Protocol version 6 to support the mobile capability. Mobile IPv6 is now a standard which allows mobile devices whose IP addresses are associated with one network to stay connected when moving to another different network. Unlike traditional devices with fixed attachment to the network, mobile devices may change their point of attachment frequently. Since a mobile device frequently moves among secure private networks and highly unguarded public networks, the security issue is much more significant. This thesis reveals the current threats in Mobile IPv6 networks and proposes an approach that mitigates some of these threats.



1.1 Motivation

IT industry is now facing the challenge of mobility revolution, where the spread of mobile and ubiquitous services have a more significant effect on commercial and social life than Internet revolution. Besides, the introduction of new communication protocol (WiMAX) technology brings a significant influence to Telecom industry, speeds up the growth of mobile devices and blurs the boundary between 3G and Wi-Fi. Users expect services that are unique and fully mobility ready, which mean that the roles of the operators will change, new business models will emerge and new methods for developing and marketing services will surface. Nevertheless, those services will reside on the widespread IP based network, because IP based infrastructure had gradually shared the

telecom market and been an essential part of communication. Not only datacom, but telecom industry also assumed IP based services as the roadmap at present or in the future.

Internet Engineering Task Force (IETF) noticed this trend and designed Mobile IP version 4 in 1996. However, MIPv4 has not been deployed widely enough and has several major shortcomings, including a cumbersome communication process and a limited number of IP addresses. A limited address space is an important issue because the number of mobile devices is increasing rapidly and without enough IP address, they cannot access Internet or communicate with peers. In order to overcome these deficiencies and introduce new capabilities, the IETF has been developing MIPv6. Therefore, MIPv6 increases the available IP addresses, introduce lots of new features and retains mobile users' connections to the Internet as they move between networks.

Once our computing devices are mobile, they are exposed to the same kinds of vulnerabilities as public networks. Compared to fixed attachment network, mobility brings many new security issues that need to attend to. Even though IPv6 [2] introduced many mechanism(AH and ESP of IPsec) for securing IP packets, new mechanism of Mobile IPv6 causes some other issues, such as false binding update. How to overcome these issues becomes an important next step for MIPv6 implementation.

After the successful story of Youtube, the potential market for sharing and watching videos through the Internet cannot be ignored. Some manufacturers are considering embedding media players in handheld devices for watching videos provided by Youtube and Joost. In addition, more and more vendors are developing new audiovisual streaming technology to integrate into mobile devices. Consequently, researches, such as Stream Control Transmission Protocol (SCTP), that supports multiple streams in an attempt to boost throughput for multimedia application, are now underway.

1.2 Research focus

Our research focuses on the security enhancement of RR Test in MIPv6. MIPv6 enables a Mobile Node to move from its home network to another network while retaining its IPv6 address. That is, a Mobile Node can always be reached through its home address. Packets are routed to the Mobile Node's home address when MN is away from home. This is due to the fact that whenever Mobile Node changed its attached network, Home Agent (HA) will be notified through Binding Update messages containing Mobile Node's Care-of-Address (CoA).

Return Routability (RR) is the basic technique for authenticating MIPv6 Binding Updates (BUs). Because RR can choose to apply any data encryption mechanism or not and the exchanged messages for weak authentications in RR are through known static routes, it is possible for attackers to launch Man-in-the-middle attacks. Thus, we would like to make some changes to MN/HA/CN that reduces the opportunities against such attacks.

We also find a way to enhance the throughput for massive multimedia data transfers by modifying SCTP over MIPv6. In order to increase routing path diversity, we considered introducing multiple HAs (Home Agent), multi-homed HA or distributed HAs as selective intermediate nodes when Mobile Nodes request for Return Routability authentication. Through the ideas proposed above, we are able to enhance RR authentication mechanism by making a few changes yet substantially reduce the probability of being compromised due to the weaknesses of original RR Test. At the same time, we would like to gain the benefit of applying SCTP for better throughput between MN and CN.

1.3 Thesis Organization

This thesis consists of 6 chapters. Chapter 2 describes MIPv6 in general, and highlights

some of its threats and defenses. Chapter 3 presents an overview of related works in the field. Chapter 4 describes our proposal of enhancing Return Routability (RR) by using selective routing paths and employ multihomed feature of SCTP with selective source addresses. In Chapter 5, we use NS2 with additional Mobiwan module to demonstrate the security improvement and to analyze the performance of our scheme through simulation results. Conclusions and future work are addressed in Chapter 6.



Chapter 2 Background

2.1 Mobile IPv6 overview

Mobile Internet Protocol has been proposed by IETF to supply IPv6 nodes with mobility. Mobility means that when devices change their network attachment, they still keep existing connections. When a conventional IPv6 node changes its location, its address may need to be changed. However, because of the change, the IPv6 node cannot maintain connectivity with its correspondent prior to the change.

Although IPv6 nodes can travel between different links and change their addresses without intervention, the existing connections using the address assigned by previous network cannot be maintained or even forcefully terminated with the change of their address. Therefore, two important concepts of Mobile IPv6 mechanism will be introduced. One is “Location Update” and the other is “Location Management”. Location Update means that Mobile Node should initiate the update of location change to the related parties when move to another network. With location Management, Mobile Nodes can be reached wherever the current location is. MIPv6 specification defines Location Management by assigning a Home Address to the mobile node and through which the mobile node is always reachable. With the two features described earlier, an IPv6 node then becomes mobile.

2.1.1 Mobile IPv6

Without support for mobility in IPv6, packets cannot reach the destination Mobile Node while it is away from the home network. In order to continue communicating, a Mobile Node could change its IP address from time to time while moving to a foreign network, but it would not be possible to maintain transport and higher-layer connections.

Mobility support in IPv6 is increasing in importance, as mobile devices are gradually

dominating the network access device market originally belonged to PCs and in the near future, they are likely to account for the majority of Internet access machines. From the concept of last section, we can know that Mobile IPv6 allows a Mobile Node to move from one network to another without changing the Mobile Node's IP address and keep Mobile Node always addressable by its Home Address (An IP address assigned to the MN within its home subnet prefix on its home link).

Packets may be routed to the MN (Mobile Node) using its home address regardless of the mobile node's current point of attachment to the Internet. Thus, the mobile node is able to communicate with other nodes, either stationary or mobile, after moving to a new network. And the movement of a mobile node away from its home link is also transparent to transport layer and higher-layer protocols applications.

In the following paragraphs, we introduce some components and terminology [3] used by Mobile IPv6.

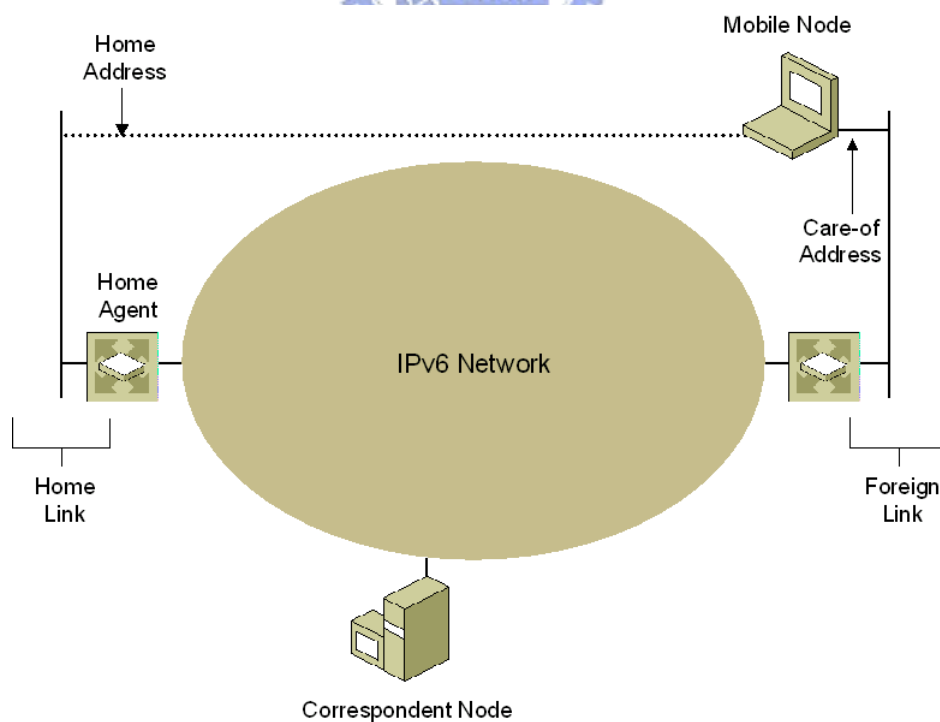


Figure 1 Environment of MIPv6

(Adopted from "Understanding Mobile IPv6" of Microsoft co.)

- Home link : the link that is assigned the home subnet prefix of mobile node
- Home address (HoA) : an address assigned to the mobile node and through this address the mobile node is always reachable. A Mobile Node can have multiple home addresses. When the mobile node is away from home, packets destined to the mobile node's home address are intercepted by the home agent and tunneled to the mobile node's current location. The same as above, when the mobile node is at home network, MIPv6 processes are not used.

- Home agent (HA) : a router on the home link that maintains registrations of Mobile Nodes' CoA (Care-of Address). When the MN (Mobile Node) is away from home, it registers its current address to home agent. The home agent tunnels data sent to the mobile node's home address to the mobile node's CoA (Care-of-Address) and forwards tunneled data sent by the MN (Mobile Node).

- Mobile Node (MN) : an IPv6 node that can change links and maintain reachability using its home address. A mobile node is aware of its home address and CoA (care-of address), and indicates its home address/care-of address mapping to the home agent and Correspondent Node with which it is communicating.

- Foreign link : a link other than MN's home link.
- Care-of address : a unicast routable address used by a Mobile Node while it is attached to a foreign link. For stateless address configuration, the care-of address is a combination of the foreign subnet prefix and an interface ID determined by the mobile node. A mobile node can be assigned multiple care-of addresses. Only one care-of address is registered as the primary care-of address with the mobile node's home agent. The association of a home address with a care-of address for a mobile node is known as a binding. CN (Correspondent Nodes) and HA (home agents) keep information on bindings in their binding cache.

- Correspondent Node : a peer node communicating with a MN (Mobile Node) is named as Correspondent Node. A correspondent node does not have to be Mobile IPv6-capable. A CN (Correspondent Node) can be either mobile or stationary.

- Binding Update : the process to update the home agent with a new primary care-of address is known as a home registration binding update. There is also a binding of correspondent registration which runs between Mobile Node and Correspondent Node. The home agent uses the home address in the Home Address option and the care-of address in a Care-of Address mobility option to update its Home Address/ Care-of Address binding cache entry for the mobile node.

Binding Cache : the table maintained by Home Agents and Correspondent node with Home Address of Mobile Node, Care-of address for mobile node and lifetime of binding cache entry.

MN will update its new location to an actively communicating Mobile IPv6-capable correspondent node with a binding that maps the home address of the mobile node to its care-of address. This process is known as a correspondent registration binding update. To update cache entry for Mobile Node's Home Address/Care-of Address, the correspondent node uses the home address in the Home Address option and the source address of the packet.

Mobile IP protocol can handle movement in both wired and wireless local area and wide area of both wired and wireless networks. However, Mobile Node is required to notify its change of location to its home network. When moving to a foreign network, the care-of address (CoA) of Mobile Node has to be registered with its home agent. If there is a far distance between the foreign network and the home network of the mobile node, the signaling delay for these registrations may be long. This is why we have a proposal for distributed HA (Home Agent) which may be located in different geographical region to reduce the delay because of the distance.

To reduce the latency for real-time applications, a route optimization option will be necessary in Mobile IP. Therefore, Mobile IPv6 introduced a way for eliminating triangle routing by allowing Correspondent Nodes (CN) to cache bindings of the mobile nodes' current locations. CN can then send packets for the mobile node directly to its care-of address without going through the home network. In the next section, we will give more details of Route Optimization feature of MIPv6.

2.1.2 Route Optimization

Mobile IP is designed to provide mobility support on top of existing IP infrastructure. Also, supporting route optimization [4] is a fundamental part of Mobile IP protocol, even though it may cause some security issue (discussed in later chapter). In route optimization, a correspondent node (CN) learns a binding between the mobile node's stationary home address and its current temporary care-of-address.

A correspondent should be MIPv6 capable so that the data traffic can be sent directly between Correspondent Node and Mobile Node. Route optimization gives the chance for directly communication through shortest path. It not only avoids the possible failure of home network or home agent but also eliminates the congestion at mobile node's home network. When routing data traffic directly to Mobile Node using Mobile Node's care-of address, correspondent set type 2 routing header as an extension of IPv6 header to indicate mobile's home address. Similarly, the Mobile Node set the source address to its current care-of address and includes the Home Address destination option to indicate its home address.

As mentioned above, the "Route Optimization" requires correspondent registration. That is Mobile Nodes should register its current binding before sent directly with correspondent. The Correspondent Node maintains a table of current binding of Mobile Node and will check its binding cache entries for the Mobiles address mapping (CoA and

HoA), last binding request and lifetime. If the entry being founded, Correspondent Node sends the packet carrying mobile node's home address and direct to Mobile Node's care-of address, when mobile is away from home.

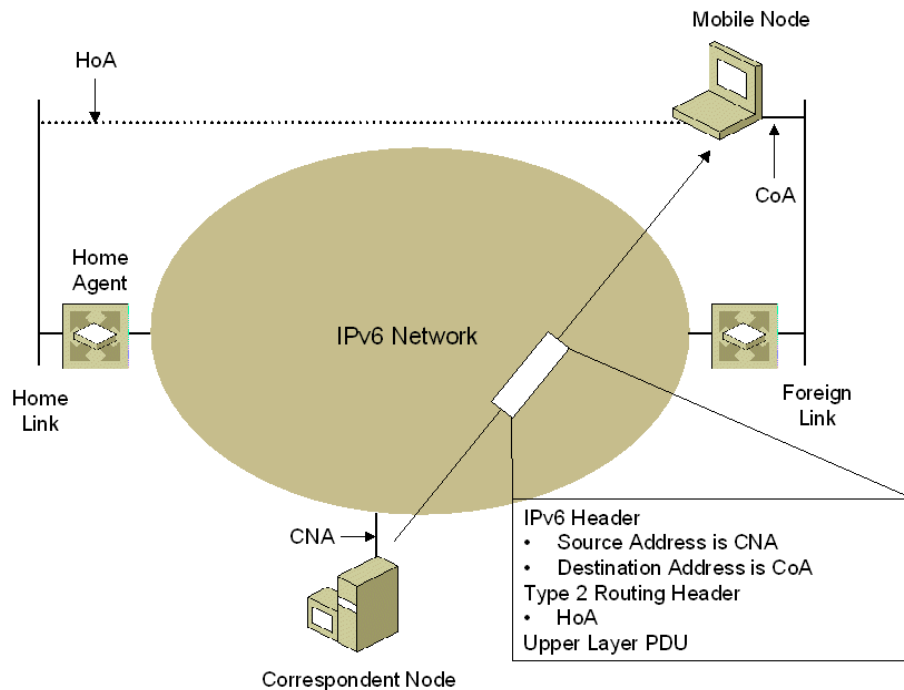


Figure 2 Route Optimization

In most cases, Mobile IPv6 packets are sent using IPv6 routing header rather than IP encapsulation in order to reduce the overhead. It is expected that route optimization can be deployed without the PKI infrastructure. Besides, Mobile IPv6 route optimization can still operate securely even without pre-arranged security associations.

2.1.3 Return Routability

Return Routability is the process devised to provide a weak authentication procedure for binding update, in Mobile IPv6. RR is a weak authentication scheme since its authentication messages are sent unencrypted. Any intermediate nodes along the routing path can have full access to the authentication messages exchanged between them without doing any cryptographic work whatever.

The Message Data field contains a mobility message.

The following types of mobility messages are defined:

- Binding Refresh Request : sent by a correspondent node or the home agent to request the current binding from a mobile node.

If a mobile node receives a binding refresh request, it responds with a binding update. A correspondent node sends a binding refresh request when a binding cache entry is in active use and the lifetime of the binding cache entry approaches expiration. A home agent sends a binding refresh request when the lifetime of its binding cache entry approaches expiration.

- Home Test Init (HoTI) : sent by the mobile node to initiate the Return Routability procedure and test the indirect path from a mobile node to a correspondent node via the home agent.

- Care-of Test Init (CoTI) : sent by the mobile node to initiate the Return Routability procedure and test the direct path from a mobile node to a correspondent node.

- Home Test (HoT) : sent by the correspondent node to respond to the HoTI message during the Return Routability procedure. The response packet will carry Home Nonce Index, Home Init Cookie, and Home keygen Token.

- Care-of Test (CoT) : sent by the correspondent node to respond to the CoTI message during the Return Routability procedure. The response packet will carry Care-of Nonce Index, Care-of Init Cookie, and Care-of keygen Token.

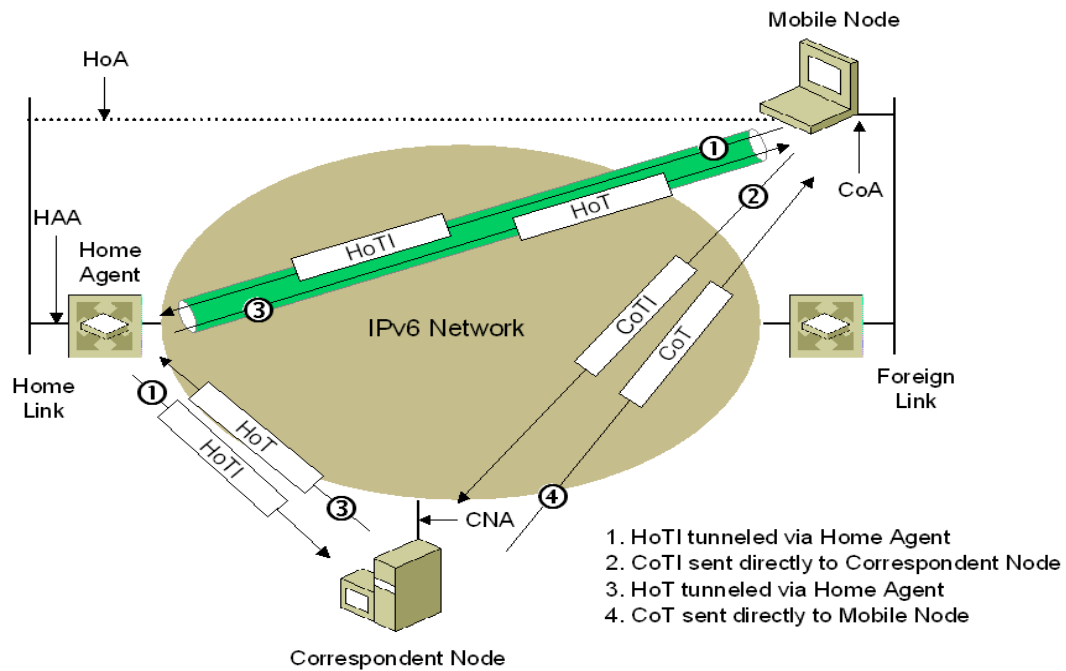


Figure 3 Return Routability of MIPv6

After Home Test Init and Care-of Test Init are acknowledged, Mobile Node might send Binding Update to Correspondent Node to complete authentication procedure.

Binding Acknowledgement (BA): Binding Update message will be responded with BA from Correspondent Node to MN's care-of address. This response message carry sequence number as the Binding Update. There is a hash added to replying parameter which include "First (96, HMAC_SHA1 (Kbm, (care-of address | correspondent | BA)))" in a Binding Acknowledgement message as a means to weak authentication.

The process described above is known as a home registration binding update. There is also a binding of correspondent registration which runs between Mobile Node and Correspondent Node. The home agent uses the home address in the Home Address option and the care-of address in a Care-of Address mobility option to update its Home Address/Care-of Address binding cache entry for the mobile node.

Binding Refresh Request (BRR): A correspondent node uses this request to re-establish its binding with a Mobile Node, when the binding's lifetime in Correspondent Node's cache is about to expire. This is also a way to limit the number of attackers and their

targets intending to test the return routability (RR) of the HoA and CoA.

In RR protocol, MN will send HoTI and CoTI to CN. The HoTI message will go through HA to CN and CoTI will be sent to CN directly. After CN received these two messages, CN use its private secret (K_{cn}) and nonces to generate a pair of Home-keygen-token and Care-of-keygen-token. CN put this Home-keygen-token into HoT targeting MN but going through HA. Care-of-keygen-token will be put into CoT and go directly to MN.

After the MN receives both (Home-keygen-token and Care-of-keygen-token messages, it generate a secret (K_{bm}) known only by MN and CN. MN sends a BU to CN using K_{bm} as an authentication. Once CN receive BU, it calculates K_{bm} and then use K_{bm} to process authentication. If accept, CN will commit 'Binding Update' to Binding Cache. However, if not, CN will reject this binding update. The RR test is, in fact, a variation of the cookie exchange, which has been used as part of the TCP handshake and in authentication protocols, including Photuris and IKE.

The binding management key derived from correspondent is sent to both claimed routing paths to assure reachability. Two token values are then retrieved from individual path carried by HoT and CoT message. If malicious entity is able to capture packet or access the path between Correspondent Node and Home Agent, it can only learn home token in the HoT message. Should tokens in separate paths be captured by an attacker, it will be possible for him/her to calculate the binding management key. However, most Internet users do not have such capability. A typical attacker is able to attack only the correspondents and mobile node in his/her own local network. These kinds of verifications should be able to prevent spoofing of binding update and denial-of service attacks for most cases.

2.2 SCTP (Stream Control Transmission Protocol)

In this section, we would like to introduce SCTP (Stream Control Transmission Protocol) [13], for our thesis will employ this protocol together with Mobile IPv6. By incorporating the multi-homing feature from SCTP, we can masquerade source addresses by picking one or more IP addresses randomly for RR authentication. Moreover, we also want to utilize other features, such as multi-streaming, for boosting the throughput.

The IETF Signaling Transport (SIGTRAN) working group defined the Stream Control Transmission Protocol (SCTP) in 2000. Originally, SCTP designers wanted to create a protocol that duplicates in IP some of the reliability attributes of the SS7 signaling network.

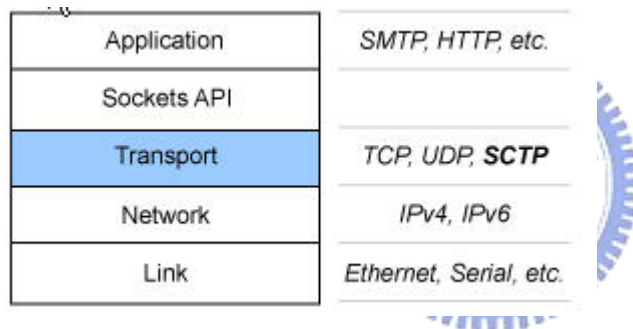


Figure 4 SCTP in transport layer

Stream control transmission protocol (SCTP) is an end-to-end, connection-oriented protocol that transports data in independently sequenced streams. SCTP endpoints support multi-homing, multi-streaming, initiation protection, message framing, configurable unordered delivery and graceful shutdown. SCTP provides applications with enhanced performance, reliability, and control functions. This protocol is essential where detection of connection failure and associated monitoring is mandatory. Furthermore, SCTP could be implemented in network systems and applications that deliver voice/data supporting real-time services, such as streaming video and multimedia services.

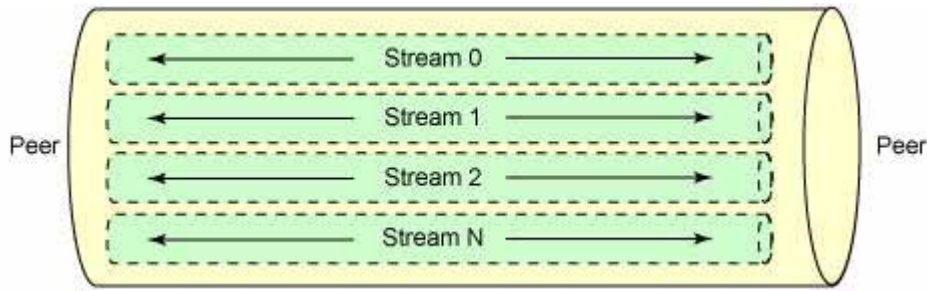


Figure 5 multiple message-streams of SCTP

TCP transports a single byte-stream at a time, whereas SCTP can transport multiple message-streams. TCP send packets in bytes and all bytes must be delivered in order. A byte transmitted first must safely arrive at the destination before a second byte can be processed even if the second byte manages to arrive first. SCTP in contrast, conserves message boundaries by operating on whole messages instead of single bytes.

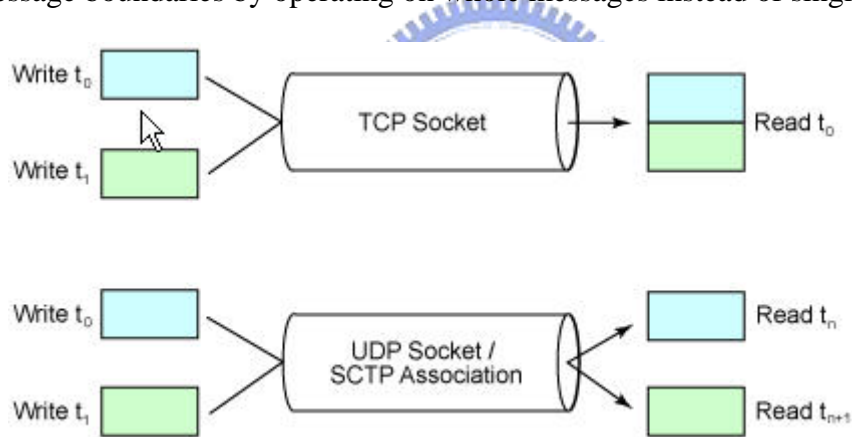


Figure 6 Byte-stream vs. message-stream

SCTP is able to transmit several independent streams of messages in parallel which it terms “multi-streaming”. You can imagine multi-streaming as several bundling TCP-connections in one SCTP association operating with messages instead of bytes when transmitting few video streaming in RTP application in parallel over the same SCTP association.

TCP ensures the correct order of bytes in the stream by conceptually assigning a sequence number to each byte sent and ordering these bytes based on that sequence

number when they arrive. SCTP, on the other hand, assigns different sequence numbers to messages sent in a stream. This allows independent ordering of messages in different streams. However, message ordering is optional in SCTP. If the user application so desires, messages will be processed in the order they are received instead of the order they were sent, should these differ.

However, signaling in PSTN (Public Switched Telephone Networks) requires message-based delivery. Multi-Streaming is one of SCTP feature which provides an advantage over PSTN services. An SCTP connection can be set up to carry multiple phone calls within one call stream. Therefore, if a single message is lost in only one phone call, the other calls will not be affected. Due to the limitation of TCP, while handling multiple phone calls in TCP, certain form of multiplexing would be necessary to put all phone calls into a single byte-stream. The drawbacks will be that once a single packet for phone call n is lost, the following packets could not be processed until the missing bytes are retransmitted, thus causing unnecessary delays and effecting voice quality.

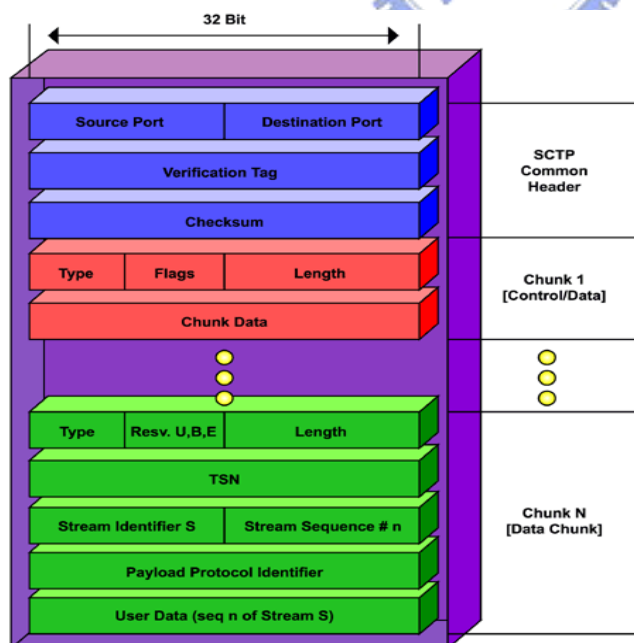


Figure 7 SCTP protocol stack

An SCTP association is similar to a TCP connection except that it can support multiple IP addresses at either ends. This feature is also an important function which we will

discuss at Chapter 4 of this thesis. Besides, an SCTP association is comprised of multiple logical streams, ensuring the sequenced delivery of user datagrams within a single stream. SCTP make use of its multistreaming feature to speed up the transfer of data. Sequencing of data is done within a stream, even if a datagram is lost in one stream does not affect datagrams in other streams. This feature results in a better response time for applications.

2.3 Threat and Defense in MIPv6

We would like to discuss and describe some attacks against Mobile IPv6 in this section. In my opinion, it seems that all the vulnerabilities can be attributed to the “Binding Update”. Various protocols and mechanisms are used to manage mobile nodes’ movements. To ease our discussion, we define “False Binding Update” as the ones that provide offensive opportunities for attackers. In the following sections, we assume the threats of MIPv6 in some sense synonymous to “False binding Update”. Thus, we categorize the causes of “False Binding Update” and describe them in more details in the sub-sections. We also consider to compensating those threats.

Although the process of route optimization reduces the communication delay between MN and CN, this process also exposes more vulnerability to attackers at the same time. By sending false BUs, the attacker can forge false entries in the CN's (correspondent node) Binding Cache and cause IP packets to route to designated destinations. Without protection of cryptographic mechanism, data transmit between CoA and CN easily lead to compromise of secrecy and integrity. The most annoying part will be DoS (Denial-of-service) attack which bomb target host or network with unwanted data.

In order to prevent those kinds of attacks[4], several of Binding Update authentication mechanisms has been proposed, such as CGA or RR. We will introduce CGA or RR after explaining current threats in Mobile IPv6.

2.3.1 Current Threat in MIPv6

In this section, we would like to introduce several known attacks which should be considered when designing a protocol for authenticating BUs. They are categorized and described in several sub-sections.

Replaying and Blocking Binding Updates

Any protocol for authenticating BUs will have to consider replay attacks. That is, an attacker may be able to replay recent authenticated BUs to the correspondent and, in this way, direct packets to the mobile host's previous location. Like spoofed BUs, this can be used both for capturing packets and for DoS. The malicious node can capture the packets and try to impersonate the MN if it reserves MN's previous address after the MN has moved away and then replays the previous BU to redirect packets back to the previous location.

By jamming the radio link, by launching a flooding attack, or by taking over a mobile node's connection at the old location, the attacker could block binding updates from the mobile node at its new location. If an attacker stays between MN and CN, they will be able to capture the packets sent to the mobile and to impersonate the mobile until the correspondent's Binding Cache entry expires.

We believe that these kinds of attacks are not so serious as ones that can be mounted from remote sites, for both of the above attacks require the attacker to be on the same local network as the mobile node, where the attacker can easily observe packets and can block them even if the mobile does not move to a new location.

Man in the middle attack

An attacker can redirect packets between two IP hosts to it by spoofing Binding

Updates [5]. That is, the attacker can send spoofed BUs to both Alice and Bob and insert itself to the middle of all connections between them. Therefore, the attacker is able to see and modify the packets sent between Alice and Bob. If the target host or its correspondent supports Route Optimization and the attacker happened to know their IP addresses, this attack is possible.

Bombing Attack

An attacker will keep sending spoofed BUs, while the Binding Updates are not authenticated. We cannot identify the mobile host that sent spoofed BUs. Thus, all Internet hosts are vulnerable to this kind of attack because they all might support the correspondent functionality.

For example, if a host, Alice, sends IP packets to another host Bob, the attacker can redirect the packets to an arbitrary address Carl by sending to Alice a Binding Update where the home address (HoA) is Bob and the care-of address (CoA) is Carl. After receiving this BU, Alice will send all packets intended for Bob to the address Carl. The attacker may select the CoA to be either its own current address or any other IP address. If the attacker selects a local CoA where it can receive packets, it will be able to send further packets to a correspondent, which the correspondent believes to be coming from the mobile.

The attacker can bomb an arbitrary Internet address with excessive amounts of data or target a network by redirecting data to one or more IP addresses within the network. Therefore, CoA and HoA are easily to be victims, because they are the one providing services and, for the most time, known to everyone.

Bombing CoA with unwanted data

An attacker could learn that there is heavy data stream from media server, say Alice, to some client Bob. An attacker then subscribes to a data stream from Alice, such as a video

stream, pretending itself as Bob and then redirects this to the target address Carl. This kind of attack might be destructive because the target can be any host or network, not only mobile one which without powerful computation capability. Moreover, it is particularly serious compared to the other attacks .The target itself cannot do anything to prevent the attack.

Bombing HoA with unwanted data

Another type of bombing attack targets the HoA instead of the CoA. The attacker could initiate a video data stream download from a media server, and then sends a BU cancellation to delete the previous binding from the Binding Cache, or simply allows the cache entry to expire, which will cause the data stream to be redirected to the HoA. At first sight, you may not think it will be a serious event. However, just like bombing the CoA, the attacker can keep the stream alive by spoofing acknowledgments and this will result in a denial of service (DoS) attack.

In the beginning, the attacker needs to find a correspondent that is willing to send data streams to unauthenticated recipients. By observation, lots of popular web sites provide such video or other media streams. After the success of YouTube, this kind of web site is getting more and more popular. The attacker needs to know or guess the target's IP address, if the target is a single host. On the other hand, if the target is an entire network, the attacker can also congest the link toward that network by bombing random addresses within its routing prefix or group of prefixes. Although a firewall on the gateway of the target network may be able to filter out data that is sent to nonexistent addresses, we can not only depend on this way that network are managed or rely on addressing privacy features of IPv6 would include such filtering.

Exhausting State Storage

In this section, we describe defenses against denial-of-service attacks that exploit features of the BU protocol to exhaust the target host's resources. The better approach is to

increase the cost and difficulty of the attacks and to mitigate impact, as you know, it is hardly impossible to completely prevent DoS attacks.

A general way of attack is to exhaust the memory resource for storing protocol state. Hosts like Home Agent (HA) or CN (Correspondent Node) keep this kind of Binding Message entries in their memory cache to accelerate access speed. Binding Cache will store “Binding Update” and include Correspondent Registration and Home Registration.

2.3.2 Defense in MIPv6

In order to prevent the corruption of routing tables, Binding Update has to be authenticated. The later subsection will deliver few authentication methods. Two of them are strong, public-key authentication and the other will be weak authentication through independent routing path. Current solutions, such as Cryptographically Generated Address (CGA) and Return Routability (RR) tests, are regarded as promising for BU authentication. In certain situations, public key cryptography is considered too expensive; the best solution may be through routing path.

Public Key Authentication

IPv6 had included IP Security which acts at the network layer, protecting and authenticating IP packets between participating IPSec peers. With IPSec, data can be sent across a public network without being observed, modified, or spoofed. Moreover, a key management protocol, Internet Key Exchange (IKE) can be used in conjunct with IPSec. Mobile IPv6 authentication would use this suite of strong authentication mechanisms.

This level of strong encryption in MIPv6 can prevent all kinds of attacks against data secrecy and integrity. When the data is encrypted with public key, the spoofed BUs can only result in denial of service but not in disclosure or in corruption of sensitive data. Thus, the attack like man-in-the-middle will not be easily to crack or modify packets

between Mobile Node, Home Agent, or Correspondent Node. If correspondent can authenticate requester by IPSec, that will ensure the BU cancellation must be from requester itself and the request for deleting the binding from binding cache is real. When attackers spoof BUs to redirect heavy streaming data to specific host or arbitrary address, they cannot easily cheat Correspondent Node (CN) under strong public key authentication.

Nevertheless, the reasons why the PKI is not as prevalent as expected may be the consequence of the failure of commercializing PKIs and the slow pace of the IPSec standardization process. They could also explain the current lack of a standard BU authentication protocol.

There are some reasons that the generic protocol suites may not be suitable for BU authentication. First of all, just like the power technology is not at the same pace as the requirement of lots light weight devices. The generic authentication protocols have usually been designed with general-purpose computers and application-level security. However, it's too expensive for low-end mobile devices, such as PDA or smart phone for this kind of computation and communication overhead. Secondly, the researchers intend to design Mobile IPv6 protocol with the capability to accommodate any node with mobility and every kind of hosts as correspondents. When even local infrastructures have failed to emerge at the expected rate, it is thought a clearly formidable goal that a single PKI should cover the entire Internet. Therefore, it is necessary to look for alternative solutions that do not rely on such global infrastructures.

Return Routability for HoA and CoA

A BU authentication scheme that uses two independent routes has been proposed. In this approach, a mobile node will initiate the Return Routability procedure by direct and indirect path to the correspondent node. After that, the correspondent, which receives both

initial messages through different paths, responds to both addresses, and then recognizes Binding Updates only from mobiles that are able to receive both returned messages. Some malicious entities residing on the correspondent's local network may be able to capture one or both packets. To a typical attacker, the best place to intercept both messages is to stay in end point's local network. In fact, the RR test also includes a variation of the cookie exchange, which has been used in many authentication protocols such as IKE.

As a weaker alternative to CGA or other public key authentication, the RR test provides a light weight authentication mechanism for HoA and CN. The RR test prevent bombing attack against CoA and HoA by periodically checking expired the binding cache entries Thus, an effective attack will be under a situation that the attacker must have recently visited the target network (CoA or CN's local network) during the time when the entry in binding cache is valid. This is a way of checking that the mobile is not lying about its location and, in fact, a frequently location change makes attack difficult. This provides a level of authentication but is not entirely secure because the attacker could be somewhere on the path from correspondent to CoA. That's why we raise our enhanced Return Routability idea by making the routing paths hard to guess.

Cryptographically Generated Address (CGA)

A Cryptographically Generated Address (CGA) is an IPv6 address, which the last 64 bits of interface identifier is generated by hashing the IPv6 address with owner's public key. The binding can be verified by re-computing and comparing the hash value and other parameters sent in the specific message.

A one-way hash function makes it difficult for attacker to match a given address and to spoof BU. Using CGA has some advantages. CGA provides public-key authentication without the need of a global PKI or any trusted third parties. CGA protocol can reduce signaling overhead and handoff latency. CGA makes the spoofing attack much harder and

allows signing messages with the owner's private key. Even though an attacker can create its own CGA address, the attacker cannot spoof someone else's address since he/she does not know the private key of the address owner.



Chapter 3 Related Work

Mobile IPv6 brings innovations to current Mobile IP network; however, it did raise quite a few issues with added complication. Many researchers ponder over them to ensure that Mobile IPv6 is more secure and efficient than that in Mobile IPv4. In the following sections, we group some proposed ideas into 3 major categories: Self-Certifying Address, Return Routability Enhancement and Mobile SCTP for IP mobility.

3.1 Self-Certifying Address

In order to provide a transition to comprehensive IPsec infrastructure, Cryptographically Generated Address (CGA) and CAM (Child-Proof Authentication) [15] were proposed. Without a PKI or other security infrastructure, the address owner uses the correspondent's private key to assert address ownership by hashing address owner's public key and using that hash to generate some address bits of their own IPv6 address. Nowadays, many researchers consider CGA (Cryptographically Generated Address) [16] as one of the most promising authentication solution for Binding Update. The attractive part of this technique is that it provides public-key authentication independent of any trusted third parties, PKI, or other global infrastructure. That is, CGA can work even without global infrastructure so that it can provide peer to peer communication under certain security.

We cannot forgo CAM (Child-Proof Authentication), an initial work of CGA, if we want to talk about Cryptographically Generated Address (CGA). Greg O'Shea and Michael Roe presented CAM (Child-Proof Authentication) for Mobile IPv6 in [16]. Their work makes a mobile node use a partial hash of its public key for its IPv6 address to prevent falsification of network address.

When a mobile node employ CAM mechanism, it creates a (public, private) key pair,

derives the low order 64 bits from the MAC (EUI-64 identifier) address and listens to router advertisement to obtain its high order 64-bit address prefix. Generally, the lower 64 bit from interface's MAC address but ,in CAM or CGA, it generates the interface id from cryptographic one way hash by SHA1 algorithm of node's public key.

CAM protocol requires the hash algorithm used to be one way so that inversion of hash becomes infeasible. Messages sent from an IPv6 mobile node can be protected by attaching the public key and those parameters. This kind of solution can work without a certified authority or other security infrastructure.

Besides, it is important to note that CAMs themselves are not certified. CAM protocol cannot prevent against an attacker who deliberately generates address with its own or some other's public key and communicate with victims, such as Mobile Node or Correspondent Node, but it can, for sure, to provide non-repudiation proof in this protocol. That is, attacker cannot take a generated address by someone else and then send the signed messages to pretend to be the owner of that address.

Even though using a 62-bit value may be a tough requirement for most low-end devices, such as handheld PDA and cell phone, it is better to change keys several times during a day. Generally, a given key must be retained for the duration of any existing TCP connections, so that Mobile Node can operate without Home Agent during lifetime of this key and can safely communicate with correspondent without security infrastructure. In addition, during the transition to a new key, the previous key (and associated Home Address) can remain in use.

Except for CAM, CGA is also a technique that provides an intermediate level of security which is below public-key authentication but above routing-based weak methods (RR). The idea, originally introduced in CAM, is to form the last 64 bits of the IP address (the interface identifier) by hashing the host's public signature key. Through generated public key pair of mobile, Binding Updates can then be signed with this key. A secure

one-way hash function makes it difficult for the attacker to come up with a key that matches a given address and to forge signed BUs. The attraction of this technique is that it provides public-key authentication independent of any trusted third parties, PKI, or other global infrastructure.

Let us take a look at CGA format:

Modifier : With 128 bit unsigned integer, this value adds randomness to the address during CGA generation.

Subnet Prefix: 64 bit subnet prefix of CGA

Collision Count: During CGA generation, collision count increase by detecting duplicated address.

Public Key: A variable length field containing the public key of the address owner

CGA is associated with above parameters and comprised of Hash1 and Hash2 by those parameters.

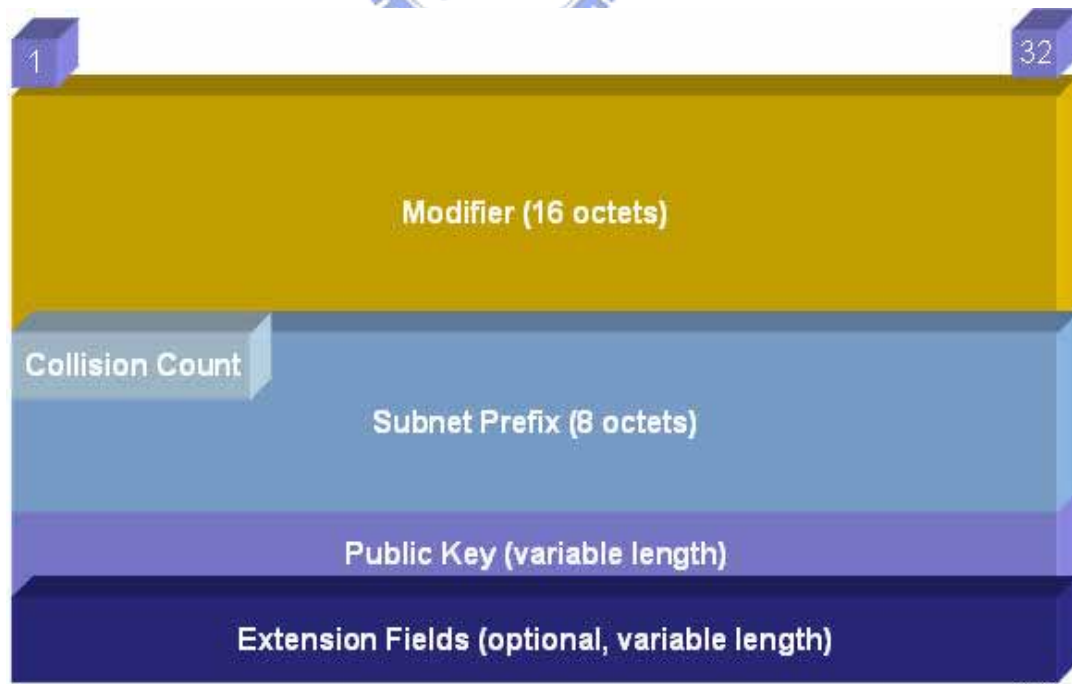


Figure 8 CGA packet format

CGA generation

To generate CGA, we need several input values: modifier, subnet prefix, collision count, public key and security parameter. To prevent attacker from using pre-computed database of subnet prefixes, subnet prefix was include as a parameter in hash computation. Using modifier, 9 zero octets, and public key, a Hash2 value can be computed. By comparing the 16xsec leftmost bits of Hash2 with zero to check if sec=0, the procedure should go back to Hash2 generation if sec is not equal to zero. By concatenating modifier value, the subnet prefix, collision count and public key, a Hash1 value can be derived by apply SHA1 algorithm.

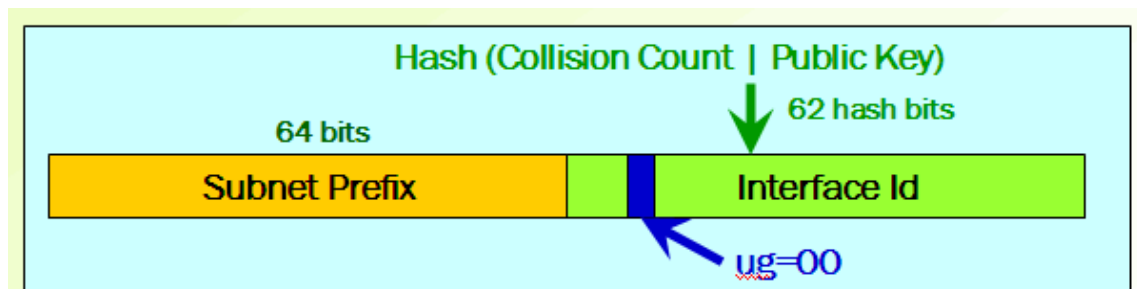


Figure 9 CAM structure

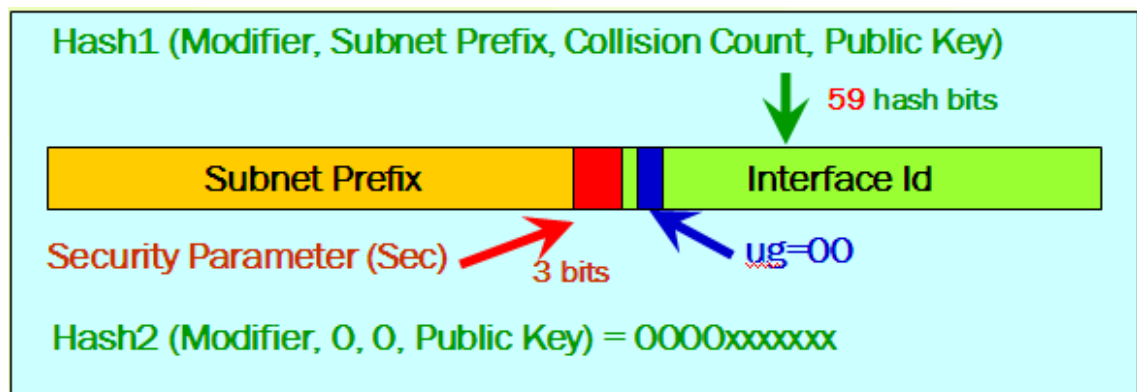


Figure 10 CGA format with sec fields

The main weakness of the CAM scheme is that only 62 bits of the IP address can be used for the hash. Thus, it is vulnerable to brute force attack as attackers could easily find a matching signature key with current computing power. That is why CGA proposed a way for extending hash by counting subnet prefix in hash. This forces the attacker to

perform the search separately for each subnet prefix. The attacker may create a database of global table which hash values and their corresponding keys, even if that seems out of practical for the large storage needed. The side effect of the idea is that only for globally routable address but not for link local addresses. It is relatively expensive to for a Mobile Node to recomputed hash when it move to other network and change its subnet.

CGA Signaling Diagram

Although the correctness of claimed address is assured, CGA still need a minimal address testing procedure for both home and care-of address. However, one of main goals for CGA is to reduce the latency caused by signaling.

The CGA protocol provides two kinds of signaling: initial contact establishment and subsequent messaging. The initial signaling should be rerun at least once every 24 hours.

The signaling process for initial contact is listed below.

1. MN to CN (via HA): Pre Binding Update
- 2a. CN to MN (via HA): Pre Binding Acknowledgement
- 2b. CN to MN (directly): Pre Binding Test
3. MN to CN (directly): Binding Update + ESN + CGA Key + SIG + BAD
4. CN to MN (directly): Binding Acknowledgment + ESN + SKey + BAD

The signaling diagram for subsequent messaging shows as below.

1. MN to CN (directly): Care-of Test Init [+ ESN + KeepFlow + BAD]
2. CN to MN (directly): Care-of Test
3. MN to CN (directly): Binding Update + NI + ESN + BAD
4. CN to MN (directly): Binding Acknowledgment + ESN + BAD

ESN (extended sequence number): a 64 bit unsigned integer, increased by the mobile node when sending a new message to the correspondent.

SIG (signature): SIG option contains the signature signed by the mobile node with CGA's private key.

BAD (Binding Authorization Data option): an authentication code generated by MN to prevent replay attacks

Skey (Shared key): Binding acknowledgment messages sent by the correspondent node use Skey option to carry key encrypted by mobile node's public key.

Signature option: The Signature option is calculated with the mobile node's private key.

CGA Key Option: CGA Key Option is used to carry the mobile node's CGA public key and other parameters. Binding Update sent by Mobile Node having this option signed with CGA corresponding private key.

Readers can notice that the Home address Test doesn't show up in the subsequent messaging process. It is not needed anymore for continuing messages exchange. The correspondent node will respond Binding Acknowledgment after receiving the signature and verification of address owner's public key in BU message. Through ESN sent with Binding Update, Correspondent Node can prevent replay attacks using past BU message.

Generating new public keys and changing addresses at regular intervals should also discourage brute-force attacks. You might know that, CGA themselves are not certified, so the malicious node may create a new CGA from any subnet prefix and its own public key. This concept addresses the limitation of the cryptographically generated addresses (CGA). Although CGA prevent the theft of another host's address, they do not stop the attacker from inventing new false addresses with an arbitrary routing prefix. The attacker can generate a public key and a matching IP address in any network and use it to launch bombing attacks. So, there is a trade off that the stronger the complex of key, the computing consuming for the resource limited mobile devices.

We can conclude that, for both PKI-based and CGA-based mechanism, while the

public-key protocols provide a reasonable protection against unauthentic BUs, they are computationally intensive and therefore the participants are exposed to denial-of-service attacks.

3.2 Enhancing Return Routability

In this section, we present some other approaches for Binding Update Authentication. Return Routability is a light weight authentication approach using independent routing path to authenticate the sender's identification. Here, we would like to introduce a paper called "Buddy Enhanced Return Routability for authentication in mobile IPv6" [17] which based its method on the foundation of "Return Routability" and extend the technique by making use of stochastic route selection. Our idea is somewhat similar to the solution provided by ERR. Without adding strong cryptographic security and significant overhead, ERR chooses the path randomly and relies on the buddy node which may be any node in the network.

Return Routability protocol enables correspondent node (CN) to obtain a reasonable assurance that claimed CoA (Care of Address) of Mobile Node (MN) is addressable as well as at its home address (HA). Accordingly, correspondent node (CN) is able to accept both Return Routability Test direct from MN's (MN) care-of-address (CoA) and indirect from MN's Home Agent and able to response to them through different but static routing paths. Only Mobiles who can receive both of message is able to send binding update (BU) to CN (Correspondent Node) as an identity authentication. Return Routability was intentionally developed as an authentication without strong cryptographic based protection, so that is why this paper eager to find an improvement for it.

According to [17], the security of RR is assumed under two premises. (1) The independent messages through different route (CN \leftrightarrow HA \leftrightarrow MN, CN \leftrightarrow MN) will not be

intercepted simultaneously. Basically, there is option that the message between CN and MN can be protected using IPSec. (2) If we take serious check to RR mechanism, we can find there is no much authentication mechanism.

The goal of “Buddy enhanced return routability for authentication in mobile IPv6” is to overcome the weak authentication of legacy Return Routability protocol without applying any cryptographic method. Enhanced return routability, ERR, was designed with these weaknesses of RR in mind. ERR, attempts to overcome the problems with RR without adding strong cryptographic security or other overhead. Making the authentication paths between MN and CN as secret as possible was one motivating factor of ERR.

ERR keeps authentication paths secure by letting MN select a stochastic path. In [17], MN selects a group of random paths to the CN. There are two different ways for selecting random paths. First, MN use buddy node as a relay point which might be any node in the network. However, this is under the assumption that most nodes in the network are trustworthy. Thus, attacker won't know which paths are being selected. The other way for random selection is from the entry in binding cache. Authors of “Buddy enhanced return routability for authentication in mobile IPv6” think those entries in binding cache are assumed to be trustworthy and are more suitable than random intermediate nodes which selected randomly from network.

In conclusion, since these paths are selected randomly at the time of binding update, an attacker would be unable to determine the selected paths, and therefore be unable to launch an attack against ERR. However, ERR is designed under an assumption that most nodes in the network are trustworthy. But, when the binding cache is empty, selecting any node at random is nothing short of high risk. In other word, choosing intermediate node without a mechanism to assure the trustworthy level might be worse than simply using a legacy static routing path.

3.3 Mobile SCTP (mSCTP) for IP mobility

Stream Control Transmission Protocol (SCTP) is a new transport protocol featuring multi-streaming and multi-homing. In the beginning of this thesis, our research focuses in the utilization in mobility. In what follows, we would like to pay more attention to the use of SCTP for IP mobility support in the transport layer.

Seok J. Koh and Qiaobing Xie [19] discussed how to make use of SCTP for IP handover support in “Mobile SCTP (mSCTP) for IP Handover Support”. Through the way of the dynamic address reconfiguration, the SCTP with the ADDIP extension (mSCTP) would provide soft handover for the mobile node without any additional network layer support of routers or agents. As to location management, mSCTP could be used along with Mobile IP, SIP (Session Initiation Protocol) or Reliable Server Pooling. At latter, this document will also discuss mSCTP along with Mobile IP for mobility support.

The mSCTP[18] may be used as an alternative scheme against the handover schemes based on Mobile IP v4 and Mobile IPv6. The mobile SCTP provides the handover management at the transport layer without the support from routers, not like Mobile IP based handover schemes which rely on the support of network agents or routers for tunneling between access routers,.


The mSCTP is targeted for the client-server services such that mobile client initiates an SCTP session with a fixed server. For peer-to-peer services, in which a session is terminated at the mobile host, the mSCTP must be used with another location management scheme such as Mobile IP, Session Initiation Protocol (SIP), Reliable Server Pooling (Reproof) or Dynamic DNS (DDNS).

SCTP intrinsically provides the multihoming feature which allows a mobile node to bind multiple IP addresses simultaneously. Recent works on the SCTP include the ADDIP extension which enables the SCTP to add, delete and change the IP addresses during

active SCTP association. Mobile SCTP, so-called (mSCTP), implemented SCTP with the ADDIP extension can be used for soft handover while the mobile node is moving foreign network during the session. Besides, mSCTP provides a way for Route Optimization without using any Binding Update Procedures.

The following depicts the procedure for mSCTP Handover:

1. Session Initiation by Mobile Client
2. Obtaining an IP Address in the New Location
3. Adding the New IP address to the SCTP Association
4. Changing the Primary IP Address
5. Deleting the Old IP Address from the SCTP Association
6. Repeating the mSCTP Handover Procedures



Accordingly, mSCTP with MIP is focused on the mobile sessions that are initiated by CN to MN. Only Mobile needs to be aware of MIP, whereas CN do not need use of MIP. Namely, Mobile IP will be used only for location management, by which the CN can locate the location of MN and establishes an SCTP association. HoA will be used for location management either, but after SCTP session establishment, HoA won't be used for following data transfer. Once the SCTP association has been established, the on-going SCTP session will be supported by the mSCTP soft handover procedures and CoA is employed as continuing data transfer. Specifically, MIP functionality for data transport will not be used in SCTP. Once the association is established, the data transport between MN and CN relies on SCTP over IP.

The home address (HoA) of MN is not involved in the data transport between CN and MN in the proposed scheme. No additional route optimization procedures are required, that is, no binding update is needed between MN and CN. The reason for this is to exploit

the intrinsic route optimization feature of mobile SCTP. Once CN gets the current location of MN, the basic SCTP initialization completes. HoA is just a backup IP address in case of the failure of reachability to the primary address (CoA).

For location management, the mSCTP may be used along with MIP or SIP. In case of using MIP for location management, only the MN needs to be aware of MIP, whereas the CN need not use MIP. Using mSCTP with MIP, the MN must also be able to bind the CoA as well as HoA to its applications. The HoA will be used only for location management. After establishment of an SCTP session, the HoA will not be used for data transport. Instead, the CoA is employed for the SCTP data transport. On the other hand, in MIP, only HoA is bound to the applications of MN regardless of the different CoAs.

The MIP provides the location management in the network layer, and it can support seamless handover with the support from network devices. In related papers, SIP is introduced as a signaling protocol that supports the location management for user or personal mobility. SIP itself does not provide seamless handover but it can be used together with mSCTP for seamless handover.

Mika Ratola [10] made a comparison of Mobile IPv6, HIP, and SCTP even though they are in different layer. He compared the protocols by architecture, security and problems in the paper “Which Layer for Mobility? Comparing Mobile IPv6, HIP and SCTP”. Ratola pointed out that the key factor in functioning MIPv6 is Binding Update. Therefore, binding messages must be authenticated and protected against replay attacks. IPsec Security Association (SA) between MN and Home Agent can be pre-installed. However, in IPv6 [14], IPsec framework, Authentication Header (AH) or Encapsulated Security Payload (ESP), is employed as a build-in security function. An alternative authentication, RR (Return Routability) procedure is used.

Host Identity Payload (HIP) by Robert Markowitz introduces a new Host Identity layer between the IP layer and upper layers. HIP avoid the situation where binding sockets to IP

addresses forces the address into dual role of endpoint and forwarding identifier. In HIP, upper layer sockets are bound to Host Identities (HI) instead of IP addresses.

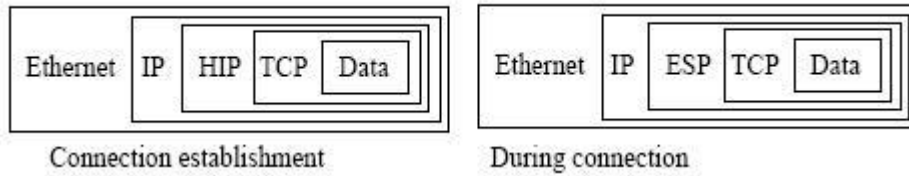


Figure 11 HIP packet structures

HI is represented via its 128 bit (SHA-1) hash which is known as Host Identity Tag (HIT) or 32 bit Local Scope Identity (LSI). However, HITs should be unique in the whole IP universe. HIP protocol is used to authenticate the connection. The HIP protocol uses a four-way handshake with Diffie-Hellman key exchange. Following figure illustrates the exchange. With HIT, it is easy to achieve multi-homing by binding multiple IP addresses to a host, thus correspondent can identify hosts by their HIT instead of IP addresses.

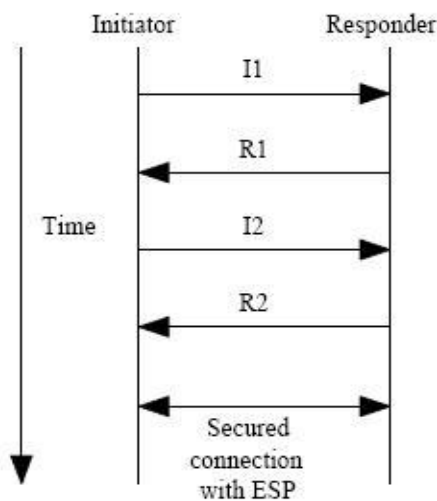


Figure 12 HIP establish connection

SCTP provides a general purpose transport protocol for message-oriented applications. A key difference to TCP is the concept of several streams within a connection which are known as associations. The association establishment in SCTP uses four-way handshake.

While establishing association, CN sends INIT chunk to trigger association setup by way of HA. MN responds with INIT-ACK chunk by put MAC into a COOKIE and returned in an INIT-ACK chunk. Correspondent using the received COOKIE assemble a COOKIE-ECHO chunk and return it to Mobile Finally, the MN verifies with the MAC, that the COOKIE is the same as it sent, and replies with a COOKIE-ACK chunk.

mSCTP is targeted for client-server services. Once supporting peer to peer services, SCTP must use along with additional location management scheme. HIP is designed to solve the problem of location and identity of a node in order to achieve mobility. However, it needs to make change to operation system kernel and adds new layer to existing communication model which the architecture remain for decades.

There is no straight-forward solution while considering both mobility and security issues. Nevertheless, lots of alternative solutions have been proposed.



Chapter 4 Selective Source and Routing Path

Our proposal is aimed at enhancing the current Return Routability scheme which just employed route authentication through static routing path. In this chapter, we would like to present a novel idea which may greatly increase ability at preventing attackers from eavesdropping or launching Man-in-the-Middle attack.

Similar to return routability, we do not rely on some pre-existing security relationship (including security properties tied to the IPv6 addresses) or apply complicated cryptographic computation in order to reduce excessive computation overhead on portable or mobile devices.

4.1 Message Flow

In this section, we borrowed the existing multihoming feature of SCTP which we need for switching packet sources. Also, we implemented load-balanced Home Agent (HA) or distributed Home Agent (HA) to give a more selective intermediate node for advanced authentication.

We make use of these features to perform authentication before transferring data to the Correspondent Node. Once MN (Mobile Node) changed its location, MN (Mobile Node) will send binding update to Correspondent Node in order to maintain binding with Correspondent. But, before that, a Return Routability procedure has to complete first for proofing Mobile Node is reachable through direct path and indirect path as we mentioned in Chapter 2. Readers can refer to Figure 13 for the difference to conventional way. MN1 and MN2 stand for the two different interface of Mobile Node, and HA1 and HA2 represent independent Home Agent in home link or other place. Home Test Init (HoTI) and Care-of Test Init (CoTI) are sent simultaneously through two different interfaces and go through each routing path as described of conventional Return Routability individually.

Thus, multiple messages are sent out by different source IP addresses and pass through different intermediate node (Home Agent). Besides, when the source addresses and intermediate nodes are selected randomly by application, it forms a way of new authentication except conventional Return Routability.

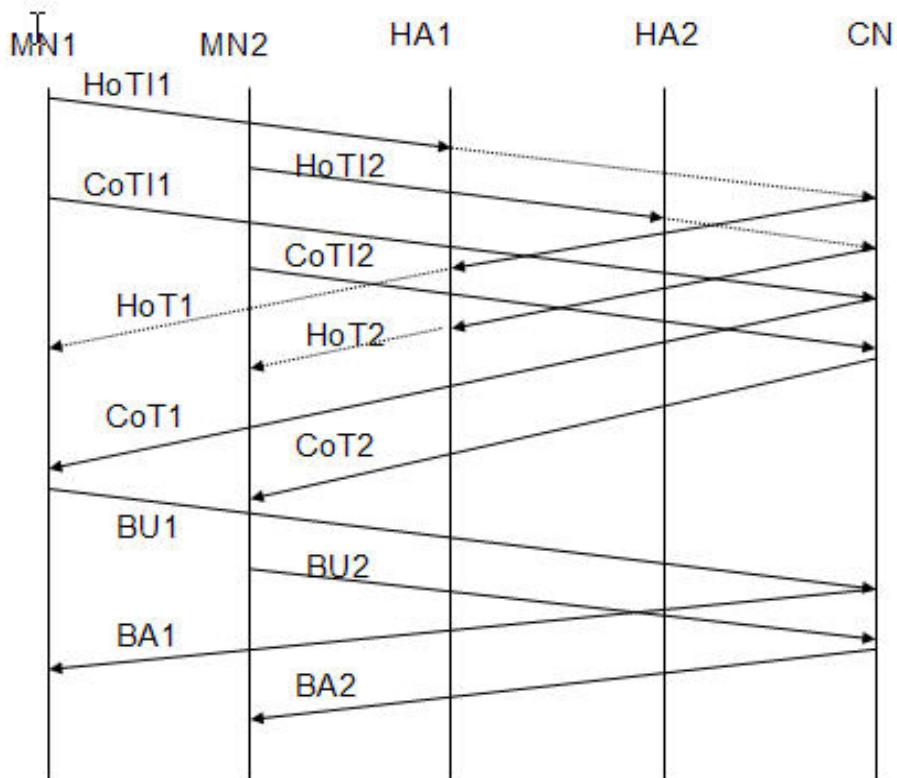


Figure 13 message flow

The Correspondent Node responds to HoTI1, HoTI2, CoTI1, and CoTI2 individually either directly or indirectly through HA1 and HA2. By exchanging the binding management key during Binding Update and Binding Acknowledgement, each node gets proof of participating Return Routability procedure.

Correspondent Node will discard packets if they can't be matched Home Address option in a Destination Option header with its binding cache entry. This is a kind of protection to resist attacker attempting to impersonate Mobile Node when it is away from home.

In conclusion, we do not need to change authentication message format of original Return Routability. We apply this kind of check to prevent nodes that are not on the path between CN, HA, MN and CN from injecting spoofed binding updates.

4.2 Protocol Specification

In this section, we implement two kinds of algorithms and describe our novel idea for securing Mobile IPv6 Binding Update. We explain in detail about how to combine the merits of SCTP and Return Routability and introduce our idea of integrating both algorithms to prevent man-in-the-middle attack through selective source address and routing path.

Mobility Header and Messages

The Mobility header[19] is an extension header used by mobile nodes, correspondent nodes and home agents in all messaging related to the creation and management of bindings. Message Data has variable length field containing the data specific to the indicated Mobility Header type. Readers can see following table which show the extension header after IPv6 header

Table 1 Mobility Header

| | | | |
|-------------------|--------------------|------------------------|-------------|
| MAC header | IPv6 header | Mobility Header | Data |
|-------------------|--------------------|------------------------|-------------|

Mobility Header

The length of the Mobility Header must be a multiple of 8 bytes. The new Mobility extension header is dedicated to carrying mobility messages and has the structure as shown in Figure 14. Setting the previous header's Next Header field to the value of 135 identifies the Mobility extension header.

| | | | |
|---------------|---------------|--------------|----------|
| Payload proto | Header Length | MH Type | Reserved |
| Checksum | | Message Data | |
| | | | |

Figure 14 Structure of the Mobility extension header

This new header can contain one of several defined mobility messages to perform specific functions. Binding messages all use the Mobility header and do not convey any upper-layer information. The Mobility header appears in two different flows, the binding flow, and the return routability (RR) procedure that secures the MIP route optimization. The Mobility Header Type field identifies the particular mobility message:

| Type | Description | References |
|------|-------------------------------|---|
| 0 | BRR, Binding Refresh Request. | RFC 3775 |
| 1 | HoTI, Home Test Init. | RFC 3775 |
| 2 | CoTI, Care-of Test Init. | RFC 3775 |
| 3 | HoT, Home Test. | RFC 3775 |
| 4 | CoT, Care-of Test. | RFC 3775 |
| 5 | BU, Binding Update. | RFC 3775 , RFC 4140 |
| 6 | Binding Acknowledgement. | RFC 3775 |
| 7 | BE, Binding Error. | RFC 3775 |
| 8 | Fast Binding Update. | RFC 4068 |
| 9 | Fast Binding Acknowledgment. | RFC 4068 |
| 10 | Fast Neighbor Advertisement. | RFC 4068 |

Table 2 Mobility Header Type

(Type=0) Binding Refresh Request Message

The Binding Refresh Request (BRR) message requests a mobile node to update its mobility binding.

(Type=1) Home Test Init message

A mobile node uses the Home Test Init (HoTI) message to begin the RR procedure and

to request a Home keygen token from a correspondent node.

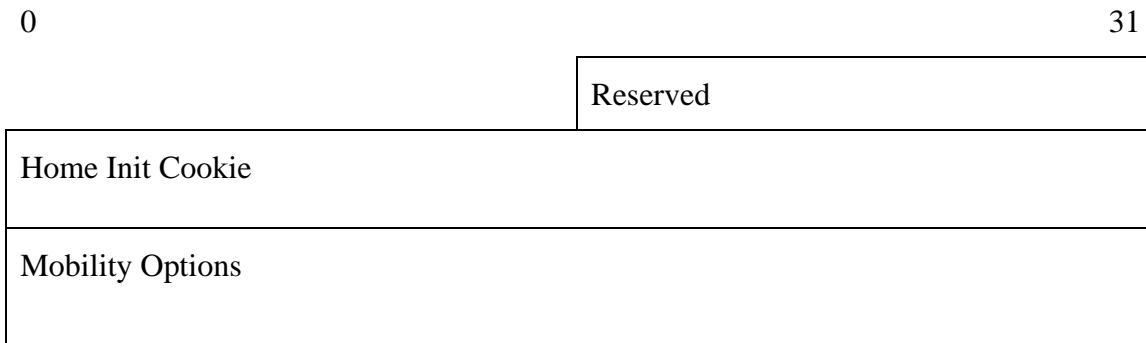


Figure 15 Home Test Init message

(Type=2)Care-of Test Init message

Mobile node uses the Care-of Test Init (CoTI) message to begin the return routability procedure and to request a care-of keygen token from a correspondent node.

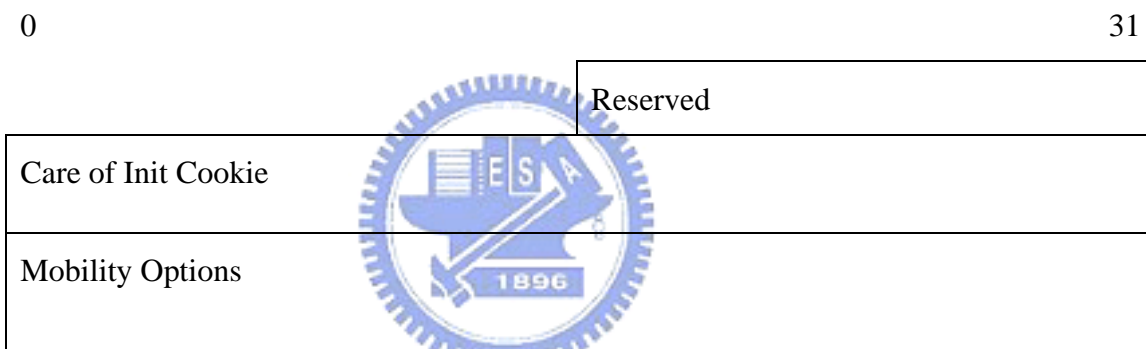


Figure 16 Care of Test Init message

(Type=3)Home Test message

The Home Test (HoT) message is a response to the Home Test Init message from the correspondent node to the mobile node.

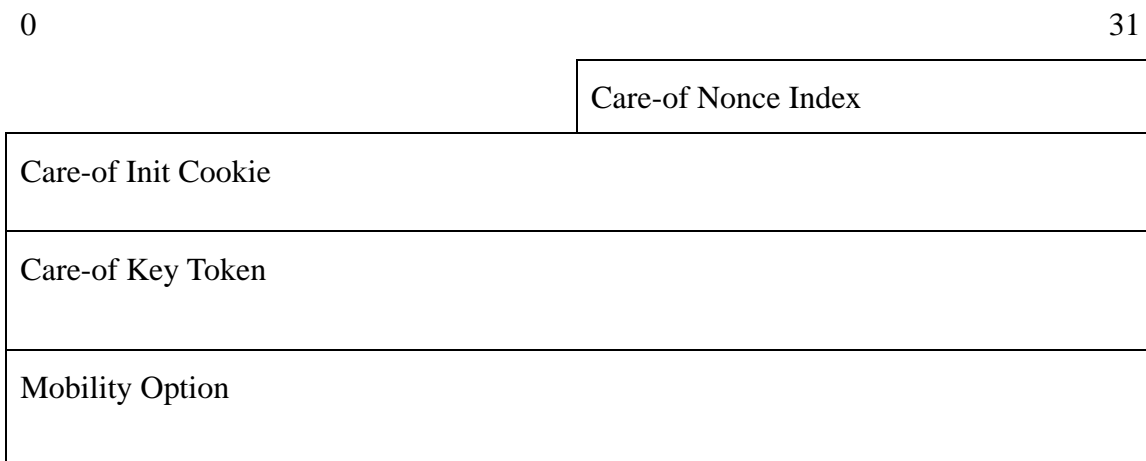


Figure 17 Care of Test message

(Type=4)Care-of Test message

The Care-of Test (CoT) message is a response to the Care-of Test Init from the correspondent node to the mobile node.

(Type=5)Binding Update message

The Binding Update (BU) message is used by a mobile node to notify other nodes of its new CoA.

| | | | | | |
|------------------|--|--|--|----------|------------------|
| | | | | | Sequence |
| | | | | Reserved | Cookie Life Time |
| Mobility Options | | | | | |

Figure 18 Binding Update message

(Type=6)Binding Acknowledgment message

The Binding Acknowledgment (BA) is used to acknowledge receipt of a Binding Update.



(Type=7)Binding Error Message

The Binding Error (BErr) message is used by the correspondent node to signal an error related to mobility, such as an inappropriate attempt, to use the HoAddr destination option without an existing binding.

Type 2 Routing Header

When Mobile Node is away from home, Mobile IPv6-capable correspondent nodes use a new Type 2 Routing header to modify a mobile node of its home address. When there is correspondent registration of CN's binding cache, Correspondent Node is able to perform direct delivery and set the Destination Address field in the IPv6 header to the mobile node's care-of address.

The Mobile Node replaces the Destination Address field with the value in the Home

Address field by processing a packet with a Type 2 Routing header. The actual home address of the Mobile Node will be put into Home Address option in the Destination Options extension header and the Mobile Node will send binding updates with home address to home agents and directly to Correspondent Nodes when Mobile Node is away from home. Besides, about the care-of address stored in the Destination Address field of the IPv6 header is merely an intermediate delivery address.

The different routing types allow a firewall to treat source-routed packets differently and can store address with varied capability for the router to process generalized source routing. Home Address Option

Generally speaking, a mobile node uses Home Test Init (HoTI) and Care-of Test Init packet to initiate the return routability procedure indirectly through MN's home agent and directly with the Correspondent Node. To prevent falsification, Correspondent Node response to HoTI and CoTI by Home Test and Care-of Test Message with home key token and use current nonce index as Home Nonce Index.

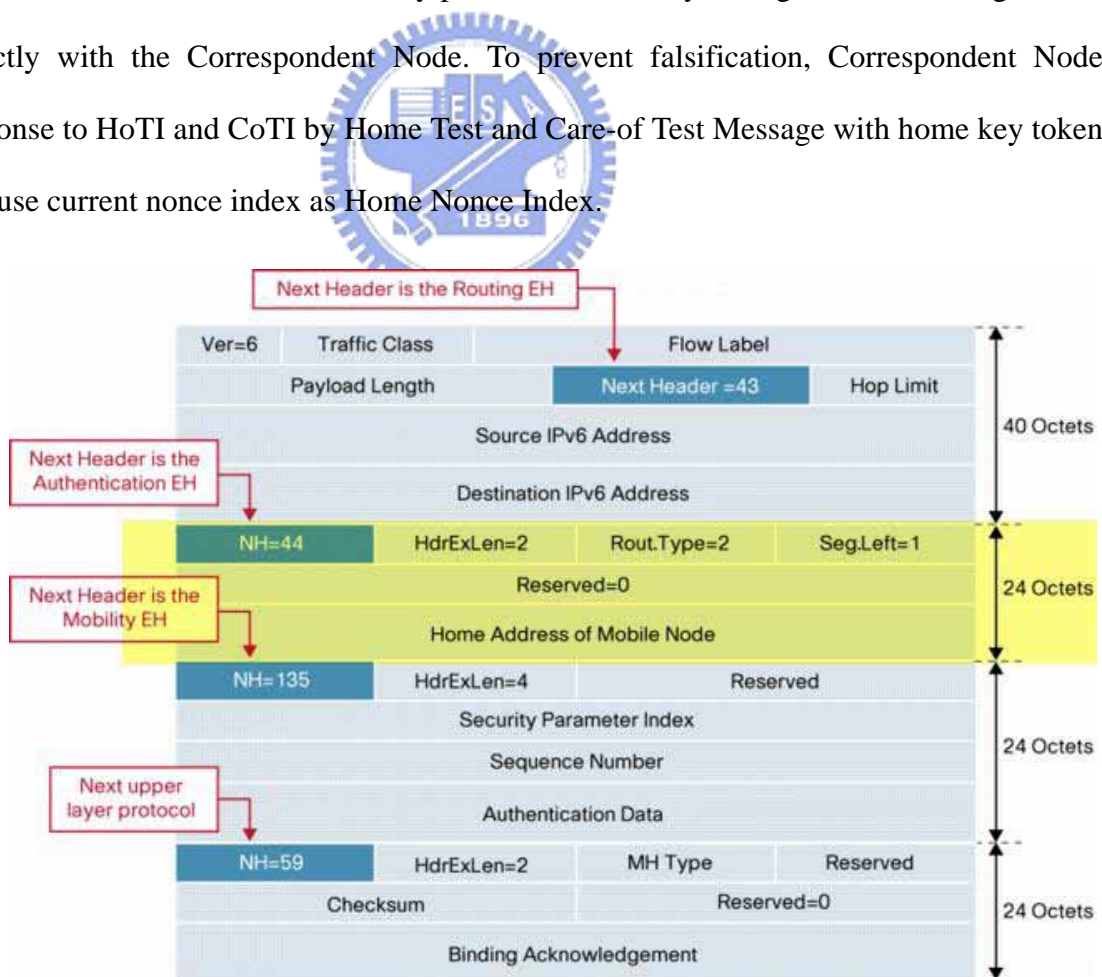


Figure 19 the structure of the new Type 2 Routing header (from cisco)

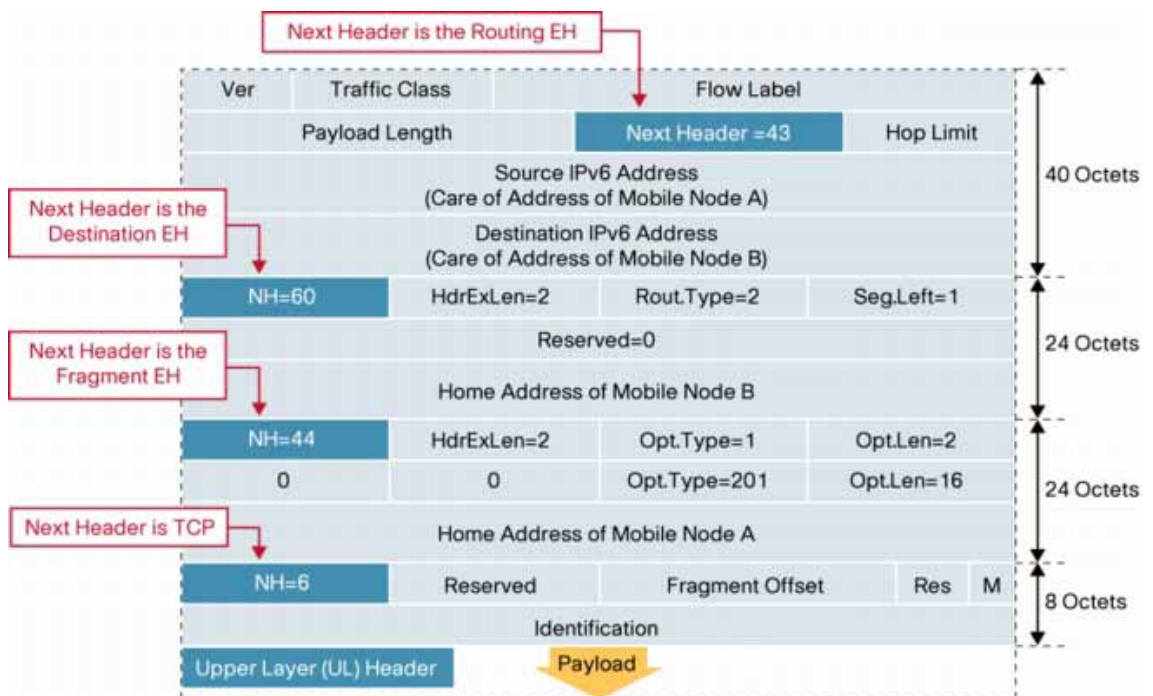


Figure 20 Packet between two Mobile Nodes (from cisco)

Figure 20 shows data traffic between two mobile nodes over the Route Optimized Path. After MN successfully complete RR Test procedure, it then performs Binding Update to CN for correspondent registration. Correspondent Node receives the Binding Update from Mobile Node, writes the update to its binding cache and then replies with Binding Acknowledgement.

4.3 Processing Bindings

Before the correspondent registration, a MIPv6 Correspondent Node will need to send data indirectly through Home Agent. As data traffic flow from MN to CN, packets will be tunneled via a series of Home Agent. After the outer IPv6 header is stripped off, the original packets are delivered to the correspondent node. If the correspondent is Mobile IPv6-capable, and has completed the binding registration for Mobile Node, it can send a

Type 2 routing header directly to Mobile Node's Care-of-Address to indicate Mobile Nodes' home address. On the other hand, Mobile Node can use the Home Address destination option to send its home address directly to the correspondent node.

In our proposal, MN receives multiple source IP addresses through multiple antennas and SCTP multi-homing feature. Users can employ upper layer application to randomly select the source address to process Return Routability Test. However, it is not covered in our paper for source address selection and our paper tends to manipulate source address by ourself. About Home Agent available for routing information, there is a document of DHAAD (Dynamic Home Agent Address Discovery) [9] by which Mobile Node can find the address of available Home Agent when it need to register its care of address and to process RR Test. The Mobile Node sends an ICMPv6 DHAAD request message to the Mobile IPv6 Home-Agents subnet any cast address for its home network. Besides, we also propose an idea of distributed Home Agent which may be applied to global company with overseas branches. The basic concept is that travelers moving to geographical different place (different continent) can use the Home Agent near to him. However, we don't discuss the methodology for how to evaluate the round trip time, how to get the available HA and how to picking the suitable Home Agent in this thesis. Moreover, we can also consider more complexity scenario that correspondent has multiple interfaces which we may use them as a parameter of multiple destination.

After that, enhanced Return Routability initial test begins through multiple source addresses and random routing paths. At following section, we explain the enhanced Return Routability and multiple paths.

Multiple Sources – We use the multihomed feature of SCTP to alter source address so that the mobile node could masquerade as a different source node.

Multiple Paths – MN generates multiple test packets that travel through different paths to CN. MN-> CN or MN-> HA->CN.

As a basic model, there are two paths and source addresses are unpredictable. The source address will be from 2 to n which depend on how we define it. Those packets will go direct or indirect to CN by random manner.

The model could be enhanced by choosing a more capricious path because we can select some other trusted nodes as intermediate routing nodes. So, the routing paths become more complicated. According to the description above, you may find not only the sources but the routing paths are variable which may thwart attacker employing man-in-the-middle attack.

CN then responds to all initial test packets by replying HoT (Home Test) and CoT (Care of Test) through their original path. After Return Routability procedure to respond to HoTI and CoTI, Mobile Node (MN) then send Binding Update message to Correspondent Node (CN). If CN successfully authenticate MN and verify its address ownership, it then commit MN's address to CN's binding cache and send Binding Acknowledgement to Mobile Node.

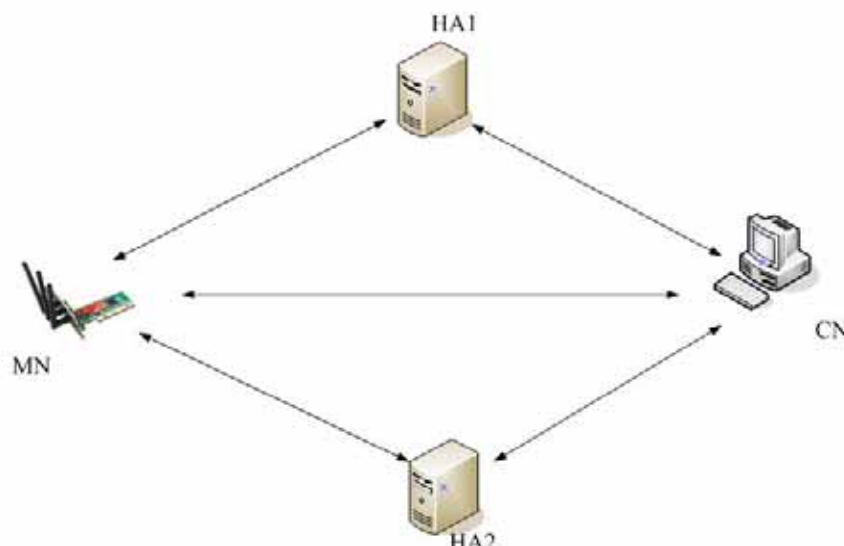


Figure 21 Selective Source address and Routing Path

In Figure 21, we draw a simplified diagram showing the Mobile Node with multiple antennas and two Home Agents which can be selected as Return Routability Test. In the

following section, we derive and compute the probabilities of compromise in different scenarios.

4.4 Reduce probabilities of compromise

In this new mechanism of RR, a successful attacker must compromise more links at the same time. If there are 3 source nodes, the attacker may need to try 63 possible links simultaneously. We compute the probability of compromise like as follows:

$$P(X) = \frac{1}{C_1^n \times (R)^1 + C_r^n \times (R)^r + C_{r+1}^n \times (R)^{r+1} + C_{r+2}^n \times (R)^{r+2} \dots\dots\dots + C_n^n \times (R)^n}$$

Figure 22 Equation

n= all (All nodes)

r = want (Number of source address)

R = numbers of HA



MN can choose how many source addresses are used to perform Return Routability test to CN (Correspondent Node). Picking source addresses dynamically can reduce the probability for attack. Besides, our thesis not only comes up with picking source addresses dynamically but also arranging routing path randomly. These two parameters can be used independently or simultaneously which may reduce the chance for man-in-the middle attack.

In Figures 23, we show the hit rate (probability) versus the number of source IP addresses of MN when attackers attempted to launch attacks. We find that as the number of source IP addresses increases from 1 to 5, nearly 31 guesses are required in average to find the actual link and see the probability drops dramatically after the numbers of source addresses becomes 3. For example, if there are two source addresses, Mobile Node (MN) can pick either one or both to perform Return Routability test. The combination will be as:

$$2C1 + 2C2 = 3$$

And

The probability of being compromised is 1/3 compared to static path in this case.

Table 3 Hit ratios by increasing nodes

| Prob. | Node | HA |
|-------------|------|----|
| 1 | 1 | 1 |
| 0.333 | 2 | 1 |
| 0.142857143 | 3 | 1 |
| 0.066666667 | 4 | 1 |
| 0.032258065 | 5 | 1 |

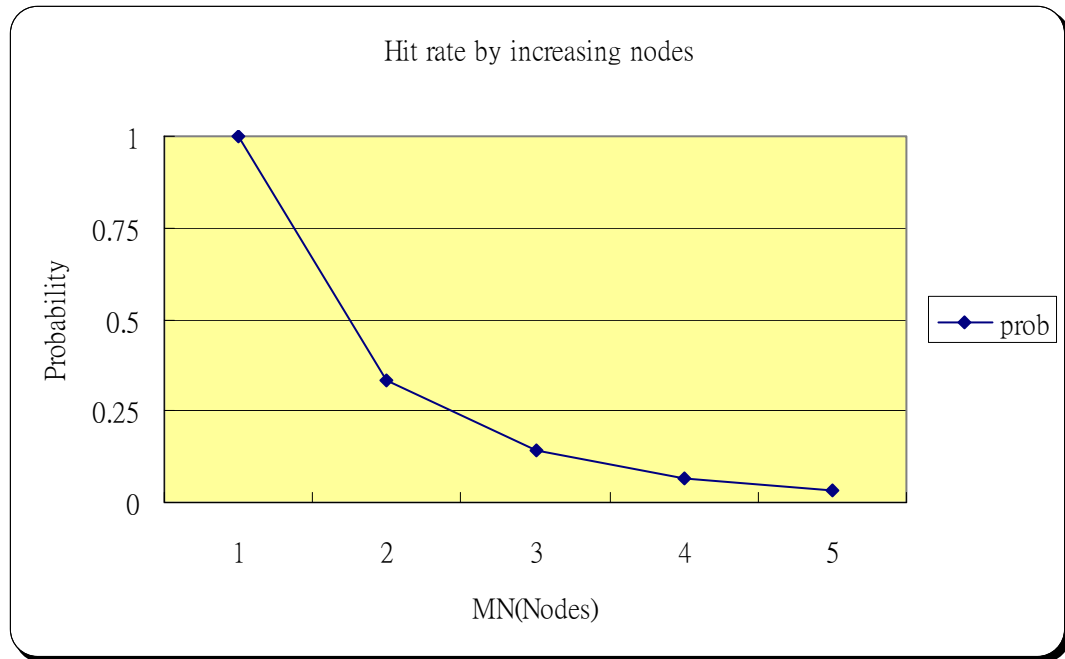


Figure 23 Hit ratios by increasing node

In another scenario, we fix the number of source addresses to 1 and vary the number of HA. That is, we use conventional MN but employ the idea of load balanced HA and distributed HA. In our thesis, HA Node can be increased by setting up load balanced HA, distributed HA or third-party HA which we registered or allied with some trustworthy third-party. Through this way, we put some variation to the routing path allowing MN to

choose many HAs simultaneously or single HA by the situation of network availability.

Table 4 Hit ratios by increasing HA nodes

| Prob. | MN | HA |
|-------|----|----|
| 1.000 | 1 | 1 |
| 0.500 | 1 | 2 |
| 0.333 | 1 | 3 |
| 0.250 | 1 | 4 |
| 0.200 | 1 | 5 |

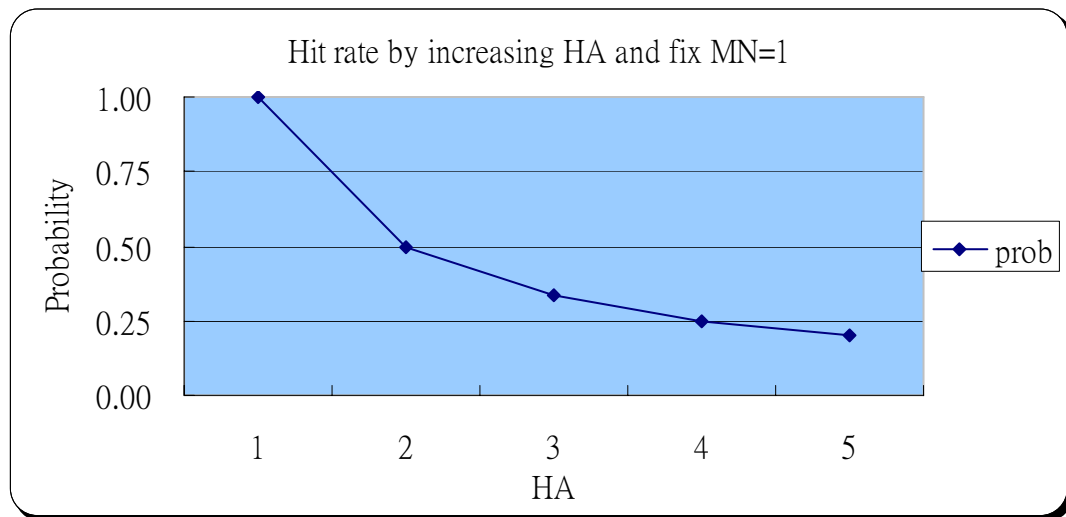


Figure 24 Hit ratios by increasing HA and by fixing MN to 1

In the following scenario, we combine these 2 parameters together but fix the number of MN to 3, because we think for the current MIMO client devices, there are only 3 network interfaces at most. Of course, if implementing SCTP, we can also bind legacy Ethernet interface except wireless interface when communicating with Correspondent Node or Home Agent.

Table 5 Hit ratios by increasing HA nodes but by fixing MN to 3

| Prob. | MN | HA |
|--------------|----|----|
| 0.142857143 | 3 | 1 |
| 0.0384615385 | 3 | 2 |
| 0.015873016 | 3 | 3 |
| 0.008064516 | 3 | 4 |
| 0.0046511628 | 3 | 5 |

From the values above, we can observe the probability is lower than those in Table 3 and Table 4. Once combing these two features, dynamic multiple sources and multiple random paths, the probability for successful attack drop. In other word, we reduce the chance for malicious node to intercept exchanging messages.

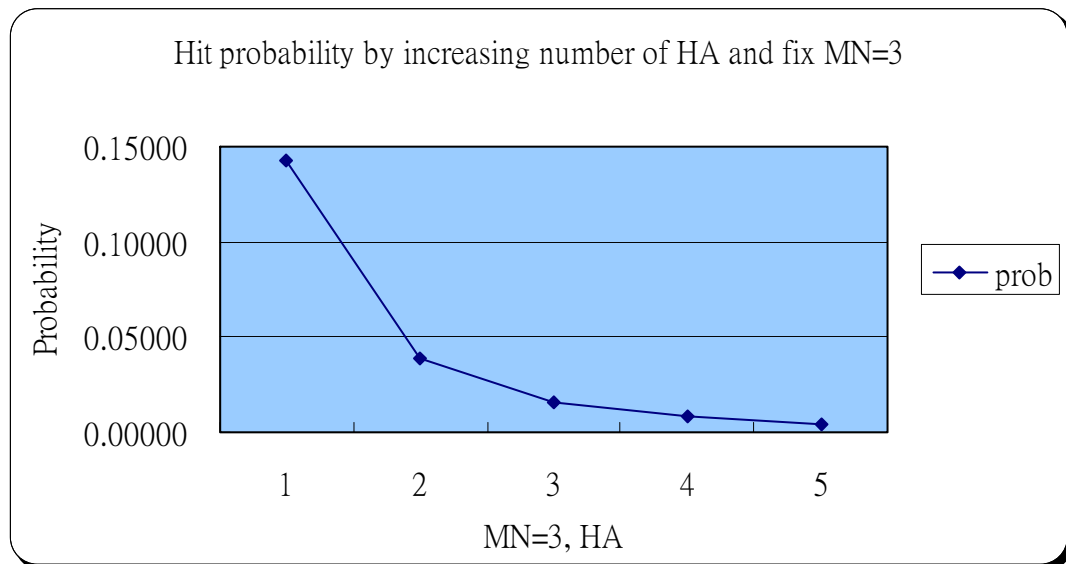


Figure 25 Hit ratios by increasing HA and by fixing MN to 3

In fact, we underestimated some variations such as CoTI when MN try to reach MN directly (Not through HA). The direct path, from MN to CN, depending on conventional routing mechanism varies. It makes attacker harder to intercept path because the routing path may vary or keep the same. Besides, at the above scenario, we have not discussed about multiple destination, like multiple interface CN. If we assume CN as a media server, it can be equipped with multiple interfaces as depicted in chapter of SCTP.

Once CN is equipped with more than one interface, the routing path will become more complicated. Just as the securities escort president's car, there are multiple targets for attacker, if attacker want intercept message between source and destination, he must get all messages between two communicating parties.

The probabilities are calculated under the assumption that the attacker knows the number of MN's source IP address. In the real case, they can't determine the number of source addresses generated by MN. For attacker, by brute-force attack, guessing both the number source and their routing paths make things complicated. They need to use brute force to combine all possible matrixes and then try to crack it.

By spoofing just one of the source addresses, the attacker cannot successfully disguise as a MN. The attacker will need to disguise all source addresses in order to successfully intercept all packets. Otherwise, CN can easily recognize the malicious nodes and refuse the connection.



Chapter 5 Simulation and experimental result

In this Chapter, we would like to use simulation results to show the efficiency of our method as the pseudo nodes grow and the routing path varies. Here, we use network simulator (NS2) with Extension Module for Mobility (Mobiwan).

NS-2 is an object-oriented simulator developed as part of the VINT project at the University of California in Berkeley. The project is funded by DARPA in collaboration with XEROX Palo Alto Research Center (PARC) and Lawrence Berkeley National Laboratory ((LBNL).

Since NS2 is an open- source tool, it is extensively used by the networking research community to help to design and test new protocols. It provides substantial support for simulation of TCP, SCTP (with extended patch), and routing, multicast protocols over wired and wireless networks. With this kind of tool, we can do large scale tests and reproduce the problems again and again. The simulator is event-driven and runs in a non-real-time fashion. It consists of C++ core methods and uses Tcl and Object Tcl shell as interface allowing the input file (simulation script) to describe the model to simulate.

MobiWan is a simulation tool based on NS (version ns-2.1b6) for simulating Mobile IPv6 under large WANs. Additionally, MobiWan has extensions to manipulate and configure large network topologies (TOPOMAN / TOPOGEN). However, it becomes outdated if we would like to simulate both SCTP and MIPv6. So, we upgrade NS2 to version 2.28 and apply the necessary patches to make our script workable for both SCTP and MIPv6.

5.1 Environment and simulation scenario

At first, we would like to evaluate legacy TCP over MIPv6 and carry out Binding Update. Figure 26 shows the scenario for simulation. We setup one domain and 16 Base

Stations and let Mobile Node (MN) move from BS1 -> BS4 -> BS16 -> BS13 -BS1 as to draw a square.

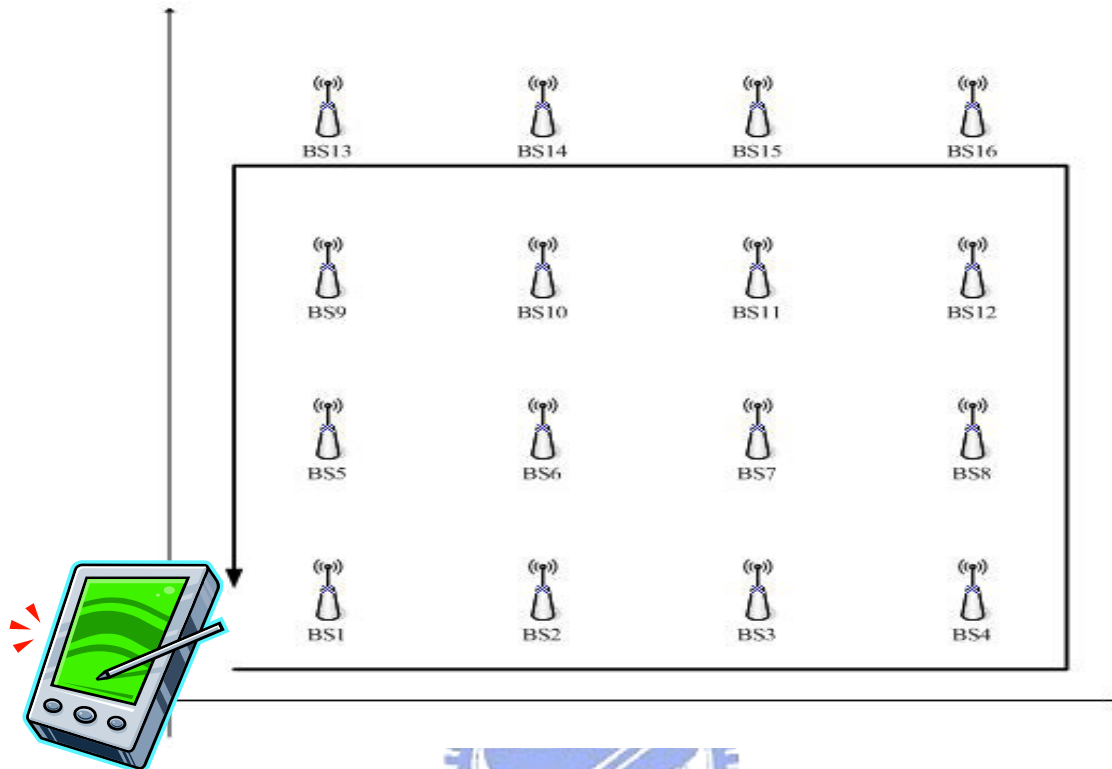


Figure 26 Scenario of MN movement

Mobile nodes with multiple interfaces will soon emerge. You may notice there are differences between appendix 1 and appendix 2. At second scenario, we add another source address and assign same HA (Home Agent) to both source address. The selective source address for Mobile Node(MN) vary by certain random allocation algorithm, so attacker is hard to find exact number of addresses involved for initiating HoTI and CoTI.

Actually, the routing path will be quite different from original static routing path. In this scenario, we don't employ multiple Home Agents. Load balancing Home Agents will synchronize their database, which includes public key information and Home Agent List. Besides, we could vary implementation by putting HA in different place. For example, a global company might have foreign offices or branches all over the world. When a mobile user travels to a foreign site, his/her authentication message does not need to go back to Home Agent (HA) located in geographical divergent places. Certainly, the company can

authorize a trusted third party to manage their Home Agent. This kind of company can deploy their distributed HA in different continents.

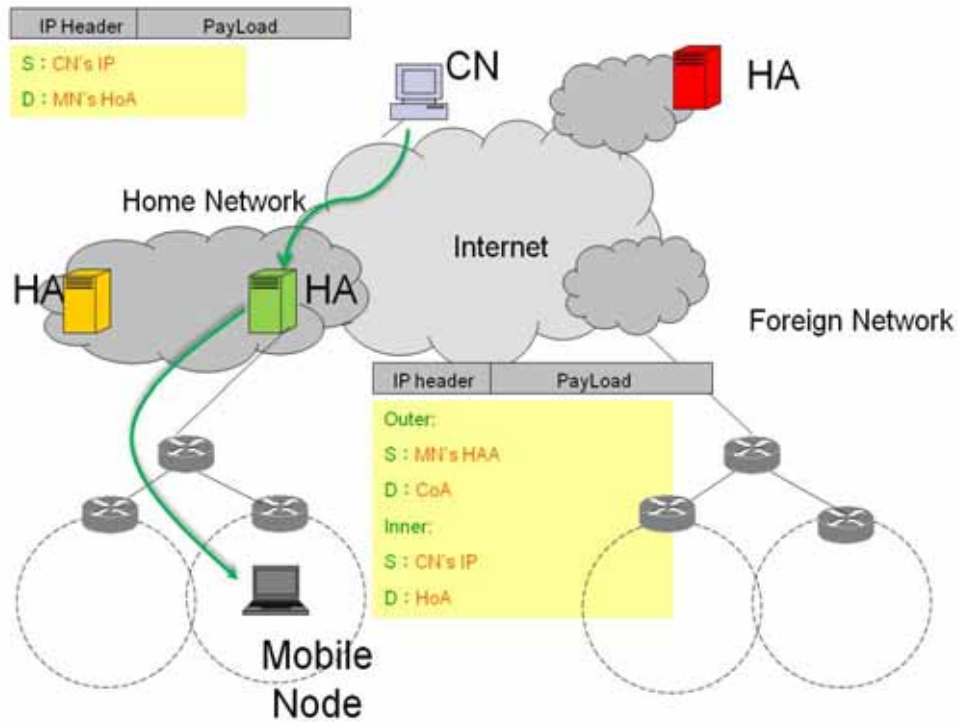


Figure 27 Data packets sent by CN to MN indirectly via HA



5.2 Experimental Result

In the first scenario, we let a mobile node traverse the closed path from BS1 (Base Station1) to BS4, BS4 to BS16, BS16 to BS13 and then BS13 to origin. We can observe the Binding Update and HoTI, CoTI and CoT, HoT between MN, CN and Home Agent. MN will get a Care-of-Address when it moves to a new location and launches Binding Process. In Figure 26, readers can notice the binding cache entries that witness the movement and registration of Mobile Node's information.

By using the following Tcl script, we understand the location of each node and the orientation of their movement at specific time.

```

#>-----<
# Set NS Addressing

  AddrParams set domain_num_ 2

  AddrParams set cluster_num_ {1 17 }

  AddrParams set nodes_num_ {1 1 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1}

# Create Nodes

set cn_ [create-router 0.0.0]

set router_ [create-router 1.0.0]

set bs1_ [create-base-station 1.1.0 1.0.0 200 200 0]

set bs2_ [create-base-station 1.2.0 1.0.0 400 200 0]

set bs3_ [create-base-station 1.3.0 1.0.0 600 200 0]

set bs4_ [create-base-station 1.4.0 1.0.0 800 200 0]

set bs5_ [create-base-station 1.5.0 1.0.0 200 400 0]

set bs6_ [create-base-station 1.6.0 1.0.0 400 400 0]

set bs7_ [create-base-station 1.7.0 1.0.0 600 400 0]

set bs8_ [create-base-station 1.8.0 1.0.0 800 400 0]

set bs9_ [create-base-station 1.9.0 1.0.0 200 600 0]

set bs10_ [create-base-station 1.10.0 1.0.0 400 600 0]

set bs11_ [create-base-station 1.11.0 1.0.0 600 600 0]

set bs12_ [create-base-station 1.12.0 1.0.0 800 600 0]

set bs13_ [create-base-station 1.13.0 1.0.0 200 800 0]

set bs14_ [create-base-station 1.14.0 1.0.0 400 800 0]

set bs15_ [create-base-station 1.15.0 1.0.0 600 800 0]

set bs16_ [create-base-station 1.16.0 1.0.0 800 800 0]

set mobile_ [create-mobile 1.1.1 1.1.0 190 190 0 0 0.01]

#>----- Run Simulation -----<

```

\$ns at \$opt(stop) "finish"

\$ns at 1.00 "\$mobile_ setdest 390 190 5"

\$ns at 50.00 "\$mobile_ setdest 590 190 5"

\$ns at 100.00 "\$mobile_ setdest 790 190 5"

\$ns at 150.00 "\$mobile_ setdest 790 390 5"

\$ns at 200.00 "\$mobile_ setdest 790 590 5"

\$ns at 250.00 "\$mobile_ setdest 790 790 5"

\$ns at 300.00 "\$mobile_ setdest 590 790 5"

\$ns at 350.00 "\$mobile_ setdest 390 790 5"

\$ns at 400.00 "\$mobile_ setdest 190 790 5"

\$ns at 450.00 "\$mobile_ setdest 190 590 5"

\$ns at 500.00 "\$mobile_ setdest 190 390 5"

\$ns at 550.00 "\$mobile_ setdest 190 190 5"

\$ns run



#>-----<

```

----- NS Addressing -----<
  Domain (domain_num) : 2
  Clusters (cluster_num) : 1 5
  Nodes (nodes_num) : 1 1 2 1 1 1
-----<

SORTING LISTS ...DONE!
channel.ccs:sendp - Calc highestAntennaZ_and distCSI_
highestAntennaZ = 1.5, distCSI_ = 550.0
35.0026 get_coa for BS 1.2.0:A190400 Current location: 6.89962, 442.03 Destination: 582.578, 316.599
36 Send BU to HA
37 Send HoI and CoI to CH
38.1129 CoI received
38.1156 HoI received
38.1154 Send BU to CH
316.6 Lost contact with current BS: 1.2.0:A190400 Current location: 353.599, 394.604 Destination: 623.935, 79.8246
316.603 return home 1.1.0:A190352 Current location: 353.604, 394.609 Destination: 623.935, 79.8246
317.6 Send BU to HA
326 Lost contact with current BS: 1.1.0:A190352 Current location: 408.67, 353.06 Destination: 796.745, 130.475
327.003 get_coa for BS 1.3.0:A200440 Current location: 408.332, 351.002 Destination: 796.745, 130.475
328 Send BU to HA
328.014 Send HoI and CoI to CH
328.113 CoI received
328.115 HoI received
328.115 Send BU to CH
404.975 return home 1.1.0:A190352 Current location: 428.486, 269.955 Destination: 190, 190
Simulation finished

Binding Cache for node 1.1.0 at 450
Node CoA Type Info Flag Last Time Life Expire HB|
1.1.1 1.3.6 TT HH 1 161 445.011 10 0 80 |

Binding Cache for node 0.0.0 at 450
Node CoA Type Info Flag Last Time Life Expire HB|
1.1.1 1.3.6 TT HH 1 162 445.053 10 0 78 |

Binding Update List for node 1.1.1 at 450
Node CoA Type Info Flag Last Time Life Expire HB|
0.0.0 1.3.6 9 CH 1 162 445 10 459.957 79 |
1.1.0 1.3.6 2 HH 1 161 445 10 2.68435e+00 82 |

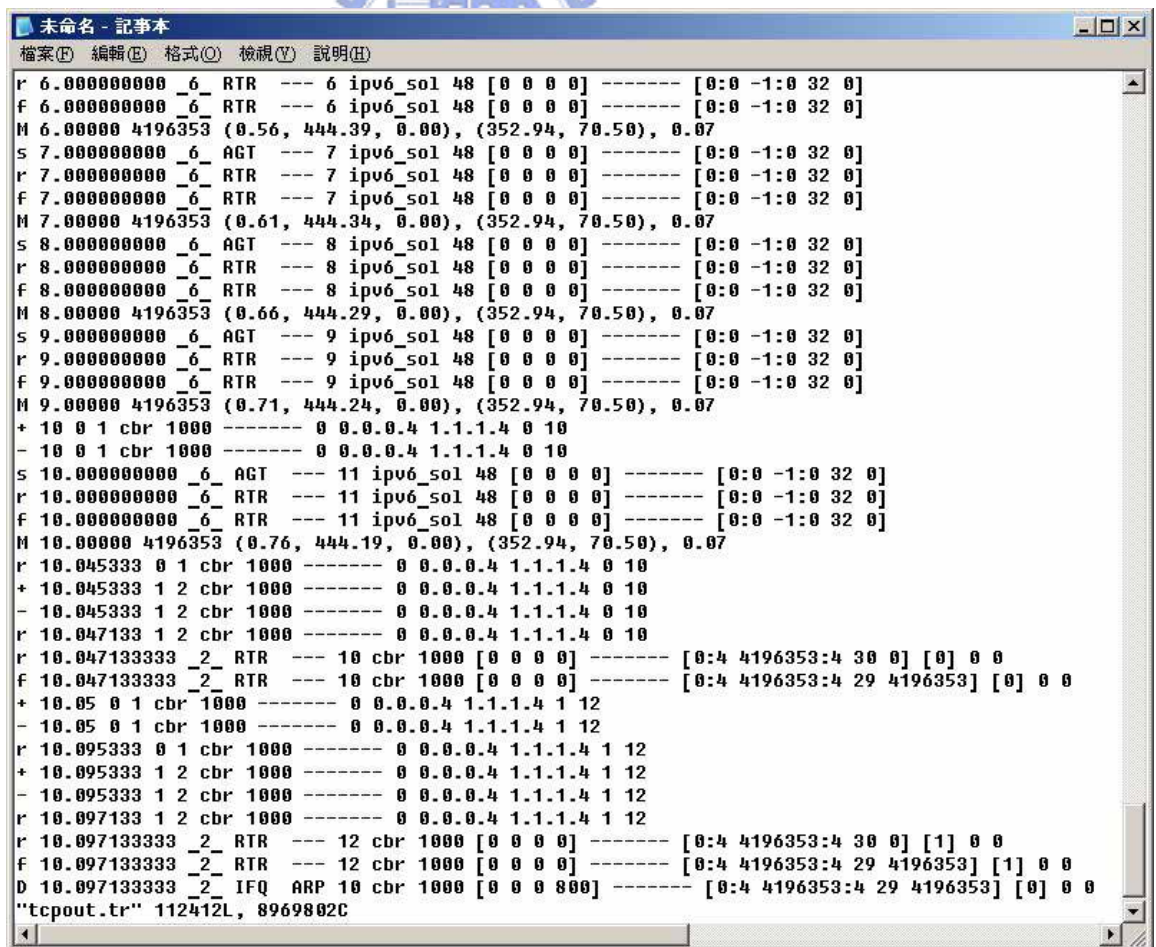
Base Station List for node 1.1.1 at 450
Node CoA Type Info Flag Last Time Life Expire HB|
1.1.0 1.1.1 12 BS 1 -1 449.675 1 0 98 |
1.3.0 1.3.6 12 BS 1 -1 449.689 1 0 234 |

History List for node 1.1.1 at 450
Node CoA Type Info Flag Last Time Life Expire HB|
1.2.0 1.1.1 0 BS 1 -1 317.6 10 327.6 1 |

```

Figure 28 Binding process dump

In Figure 29, we display the generated trace file from our Tcl scripts. Every entries record the cause of event. For example, reader can see Node 6 receiving the reply of solicitation from the first entry and the movement of Mobile Node at third entry. Each digit and abbreviation stands for different meaning. Besides, the format of wired and wireless differs which make it difficult to parse the result of trace file. We decide to use AWK, a general utility of UNIX which can be easily used to match the pattern. AWK has string manipulation functions, so it can search for particular strings and modify the output. For more detail of trace format, we would like to make a simple introduction by interpreting two entries. Through it, we can thus analyze the trace file and get clue from the packet conversation.



```

r 6.000000000 _6_RTR --- 6 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
f 6.000000000 _6_RTR --- 6 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
M 6.00000 4196353 (0.56, 444.39, 0.00), (352.94, 70.50), 0.07
s 7.000000000 _6_AGT --- 7 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
r 7.000000000 _6_RTR --- 7 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
f 7.000000000 _6_RTR --- 7 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
M 7.00000 4196353 (0.61, 444.34, 0.00), (352.94, 70.50), 0.07
s 8.000000000 _6_AGT --- 8 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
r 8.000000000 _6_RTR --- 8 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
f 8.000000000 _6_RTR --- 8 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
M 8.00000 4196353 (0.66, 444.29, 0.00), (352.94, 70.50), 0.07
s 9.000000000 _6_AGT --- 9 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
r 9.000000000 _6_RTR --- 9 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
f 9.000000000 _6_RTR --- 9 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
M 9.00000 4196353 (0.71, 444.24, 0.00), (352.94, 70.50), 0.07
+ 10 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 0 10
- 10 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 0 10
s 10.000000000 _6_AGT --- 11 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
r 10.000000000 _6_RTR --- 11 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
f 10.000000000 _6_RTR --- 11 ipv6_sol 48 [0 0 0 0] ----- [0:0 -1:0 32 0]
M 10.00000 4196353 (0.76, 444.19, 0.00), (352.94, 70.50), 0.07
r 10.045333 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 0 10
+ 10.045333 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 0 10
- 10.045333 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 0 10
r 10.047133 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 0 10
r 10.047133333 _2_RTR --- 10 cbr 1000 [0 0 0 0] ----- [0:4 4196353:4 30 0] [0] 0 0
f 10.047133333 _2_RTR --- 10 cbr 1000 [0 0 0 0] ----- [0:4 4196353:4 29 4196353] [0] 0 0
+ 10.05 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 1 12
- 10.05 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 1 12
r 10.095333 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 1 12
+ 10.095333 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 1 12
- 10.095333 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 1 12
r 10.097133 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 1 12
r 10.097133333 _2_RTR --- 12 cbr 1000 [0 0 0 0] ----- [0:4 4196353:4 30 0] [1] 0 0
f 10.097133333 _2_RTR --- 12 cbr 1000 [0 0 0 0] ----- [0:4 4196353:4 29 4196353] [1] 0 0
D 10.097133333 _2_IFQ ARP 10 cbr 1000 [0 0 0 800] ----- [0:4 4196353:4 29 4196353] [0] 0 0
"tcpout.tr" 112412L, 8969802C

```

Figure 29 raw data of trace file

Let us take a snatch of simulation result.

ACTION: [s|r|D]: s -- sent, r -- received, D -- dropped, f -- Forward

WHEN: the time when the action happened

WHERE: the node where the action happened

LAYER:

AGT -- application (Agent Trace)

RTR -- routing (Router Trace)

LL -- link layer (ARP is done here)

IFQ -- outgoing packet queue (between link and mac layer)

MAC -- mac (MAC Trace)

PHY -- physical

Flags:

SEQNO: the sequence number of the packet

TYPE: the packet type

cbr -- CBR data stream packet

DSR -- DSR routing packet (control packet generated by routing)

RTS -- RTS packet generated by MAC 802.11

ARP -- link layer ARP packet

SIZE: the size of packet at current layer, when packet goes down, size increases,
goes up size decreases

[a b c d]:

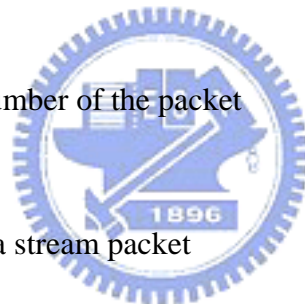
a -- the packet duration in mac layer header

b -- the mac address of destination

c -- the mac address of source

d -- the mac type of the packet body

Flags:



```
[.....]: [
    source node ip : port_number
    destination node ip (-1 means broadcast) : port_number
    ip header ttl
    ip of next hop (0 means node 0 or broadcast)
]
```

So we can interpret the trace below

```
s 76.000000000 _98_ AGT --- 1812 cbr 32 [0 0 0 0] ----- [98:0 0:0 32 0]
```

As Application 0 (port number) on node 98 had sent a 32 bytes CBR packet whose ID is 1812, at time 76.0 second, to application 0 on node 0 with TTL of 32 hops. The next hop is not decided yet.

And we can also interpret the below trace

```
r 0.010176954 _9_ RTR --- 1 ipv6_rads 56 [0 ffffffff 8 800] ----- [8:255 -1:255 32
0]
```

In the same way, as the routing agent on node 9 had received a 56 bytes cbr broadcast routing packet whose ID is 1 and size is 56 bytes, at time 0.010176954 second, from node 8 (both mac and ip addresses are 8), port 255 (routing agent).

Readers can refer to following table to interpret each field in the wired format.

Table 6 Wired format

| Event | Time | From Node | To Node | Pkt Type | Pkt Size | Flags | Fid | Src Addr | Dest Addr | Seq Num | Pkt id |
|-------|------|-----------|---------|----------|----------|-------|-----|----------|-----------|---------|--------|
|-------|------|-----------|---------|----------|----------|-------|-----|----------|-----------|---------|--------|

```
+ 20.45 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 9 30
```

```
- 20.45 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 9 30
```

```

r 20.45188 0 1 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 9 30
+ 20.45188 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 9 30
- 20.45188 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 9 30
r 20.45376 1 2 cbr 1000 ----- 0 0.0.0.4 1.1.1.4 9 30

```

Table 7 Symbol explanation

| | |
|--------------------------|-----------------------|
| r : receive (at to_node) | Src_addr : node.port |
| +: equeue (at queue) | Dest_addr : node.port |
| - : dequeue (at queue) | |
| d: drop (at queue) | |

In the same way, as the wireless format, the first column shows the event of the entry. The symbol 'r' stand for receiving by some node and '+' mean the packet entering queue, '-' 'leaving queue, and 'd' stand for being dropped. The second column show the time of event; column 3 and column 4 indicate the location(from node & to node), column 5 represent packet type, column 6 (size of packet);column 7 show the flag; column 8 is flow id, column 9 (source address),column 10 (destination address),column 11(sequence number) and final column is the packet id.

Table 8 Collection of successful RR Test

| BU2HA | HoTI/CoTI | HoT | CoT | BU2CN |
|-------|-----------|---------|---------|---------|
| 2 | 5 | 5.09434 | 5.09169 | 5.09434 |
| 31.3 | 40 | 40.0941 | 40.0916 | 40.0941 |
| 116.2 | 120 | 120.095 | 120.092 | 120.095 |
| 265.1 | 270 | 270.094 | 270.092 | 270.094 |
| 286.4 | 290 | 290.095 | 290.092 | 290.095 |
| 410.3 | 415 | 415.094 | 415.092 | 415.094 |
| 476.6 | 485 | 485.095 | 485.092 | 485.095 |
| 525.9 | 535 | 535.095 | 535.092 | 535.095 |

The table above is the result of scenario1 using single source address and standalone HA (Home Agent). We screened those successes Binding Update to CN (Correspondent

Node) from dump file and show it on the table above. Those packets being leaved out from the dump files are the packets failure at RR Test. Mobile Node might successfully received either one of HoT or CoT but was not able to receive HoT and CoT in pair.

Table 9 Binding latency of two different interfaces

| | HoT-HoTI(if1) | CoT-CoTI(if1) |
|--------|---------------|---------------|
| BU2CN1 | 0.09434 | 0.09169 |
| BU2CN2 | 0.0941 | 0.0916 |
| BU2CN3 | 0.095 | 0.092 |
| BU2CN4 | 0.094 | 0.092 |
| BU2CN5 | 0.095 | 0.092 |
| BU2CN6 | 0.094 | 0.092 |
| BU2CN7 | 0.095 | 0.092 |
| BU2CN8 | 0.095 | 0.092 |
| Avg | 0.094555 | 0.09191125 |

The table above shows the binding latency between HoTI and HoT and between CoTI and CoT. In general, HoTI and HoT take more time because those packets must go through home agent which caused more delay. However, the average latency is around 0.094555 and 0.09191125 which might be acceptable for a simple way authentication.

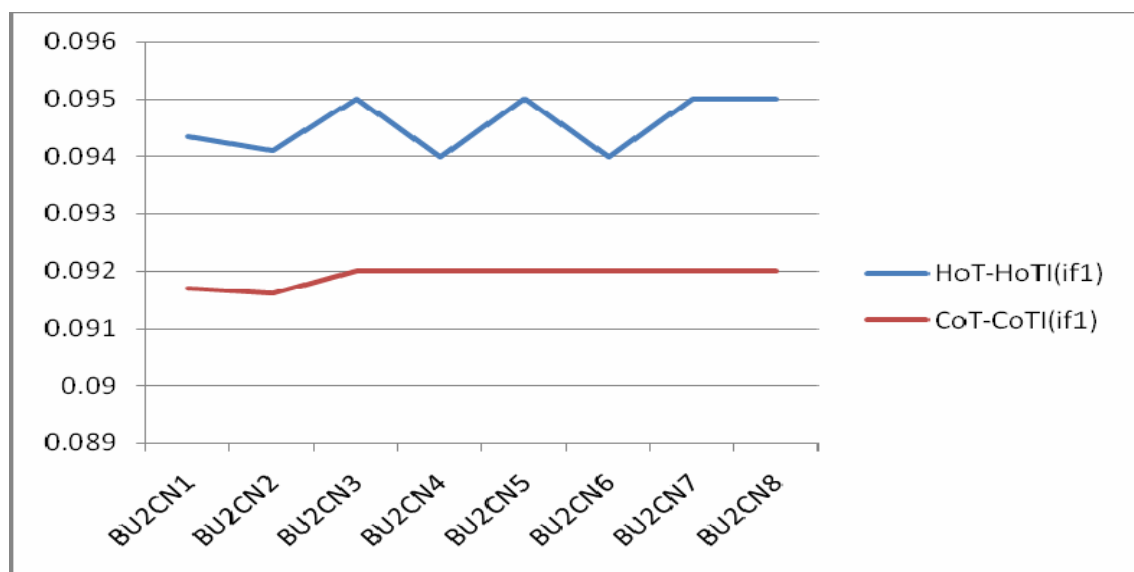


Figure 30 Latency of HoTI-HoT and CoTI-CoT

Figure 31 shows the latency from the start to the end of RR test. That is, the time MN send Binding Update to change current location to CN(Correspondent Node) and flush the registration in binding cache of CN. The latency will between 0.094 and 0.095 to complete RR Test process.

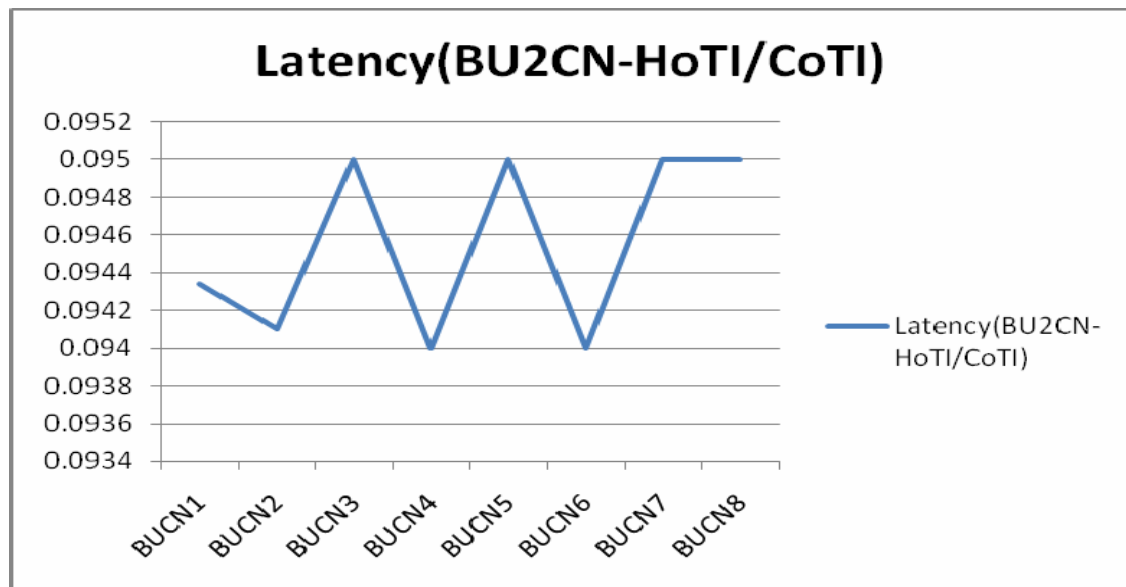


Figure 31 Latency of RR Test

From Figure 32, we can see that the average delay between BU to HA and BU to CN is 5.869555. The process start from Mobile Node changing its location information and trying to update its registration in Home Agent and then finish at updating its location to Correspondent Node in order to launch the route optimization after that. As we know, the process should be completed to both Home Agent and Correspondent Node. Only after Home Agent update the Care of Address of Mobile Node, the requested packet(ex. HoT, CoT) targeting Mobile Node can be reached.

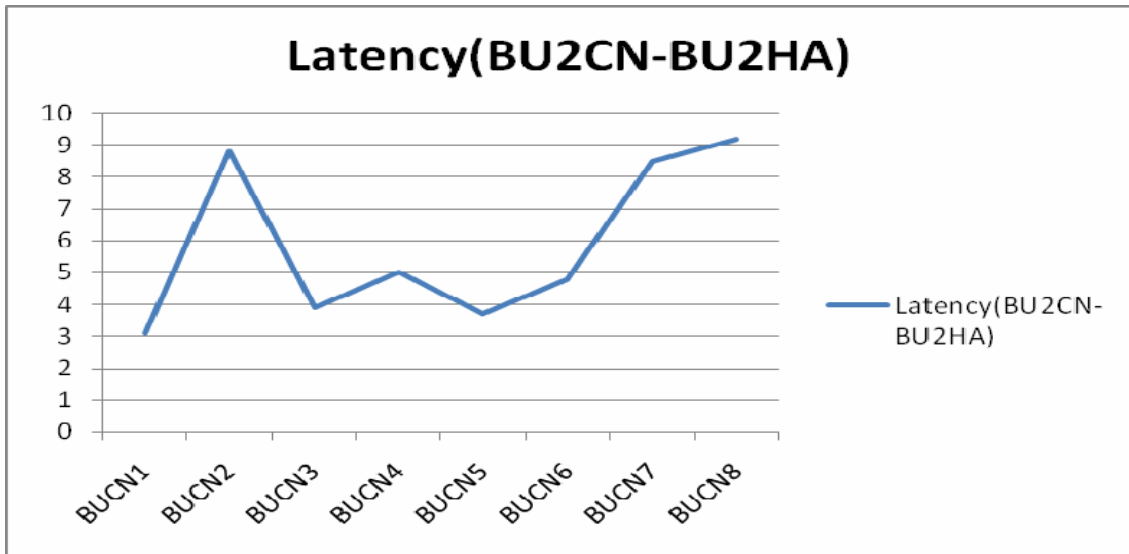


Figure 32 Latency between RR Test and movement registration to HA

Table 10 and 11 show the successful RR Test of different interface (different source address) between single HA (Home Agent) and CN (Correspondent Node).

Table 10 Collection of multi-homed interface- interface 1

| | BU2HA | HoTI/CoTI | HoT | CoT | BU2CN |
|-----|-------|-----------|---------|---------|---------|
| If1 | 2 | 5 | 5.42393 | 5.42159 | 5.42393 |
| If1 | 115.9 | 120 | 120.453 | 120.451 | 120.453 |
| If1 | 186.2 | 195 | 195.424 | 195.421 | 195.424 |
| If1 | 235.5 | 240 | 240.419 | 240.416 | 240.419 |
| If1 | 264.1 | 275 | 275.426 | 275.45 | 275.45 |
| If1 | 359.4 | 365 | 365.424 | 365.439 | 365.439 |
| If1 | 381.7 | 390 | 390.455 | 390.452 | 390.455 |
| If1 | 410.3 | 415 | 415.446 | 415.444 | 415.446 |

Table 11 Collection of multi-homed interface- interface 2

| | BU2HA | HoTI/CoTI | HoT | CoT | BU2CN |
|-----|-------|-----------|---------|---------|---------|
| if2 | 2 | 5 | 5.41829 | 5.42627 | 5.42627 |
| if2 | 115.9 | 125 | 125.424 | 125.426 | 125.426 |
| if2 | 186.2 | 190 | 190.426 | 190.423 | 190.426 |
| if2 | 235.5 | 240 | 240.45 | 240.447 | 240.45 |
| if2 | 264.1 | 270 | 270.419 | 270.416 | 270.419 |
| if2 | 359.4 | 370 | 370.423 | 370.42 | 370.423 |
| if2 | 381.7 | 395 | 395.418 | 395.42 | 395.42 |
| if2 | 410.3 | 420 | 420.42 | 420.422 | 420.422 |

In table 12, we can observe the latency between HoTI/CoTI and HoT/CoT of Mobile Node's multiple interfaces (sources address).

Table 12 Latency of HoTI-HoT/CoTI-CoT for interface 1 and interface 2

| | HoT-HoTI(if1) | CoT-CoTI(if1) | HoT-HoTI(if2) | CoT-CoTI(if2) |
|-------|---------------|---------------|---------------|---------------|
| 2 | 0.42393 | 0.42159 | 0.41829 | 0.42627 |
| 115.9 | 0.453 | 0.451 | 0.424 | 0.426 |
| 186.2 | 0.424 | 0.421 | 0.426 | 0.423 |
| 235.5 | 0.419 | 0.416 | 0.45 | 0.447 |
| 264.1 | 0.426 | 0.45 | 0.419 | 0.416 |
| 359.4 | 0.424 | 0.439 | 0.423 | 0.42 |
| 381.7 | 0.455 | 0.452 | 0.418 | 0.42 |
| 410.3 | 0.446 | 0.444 | 0.42 | 0.422 |

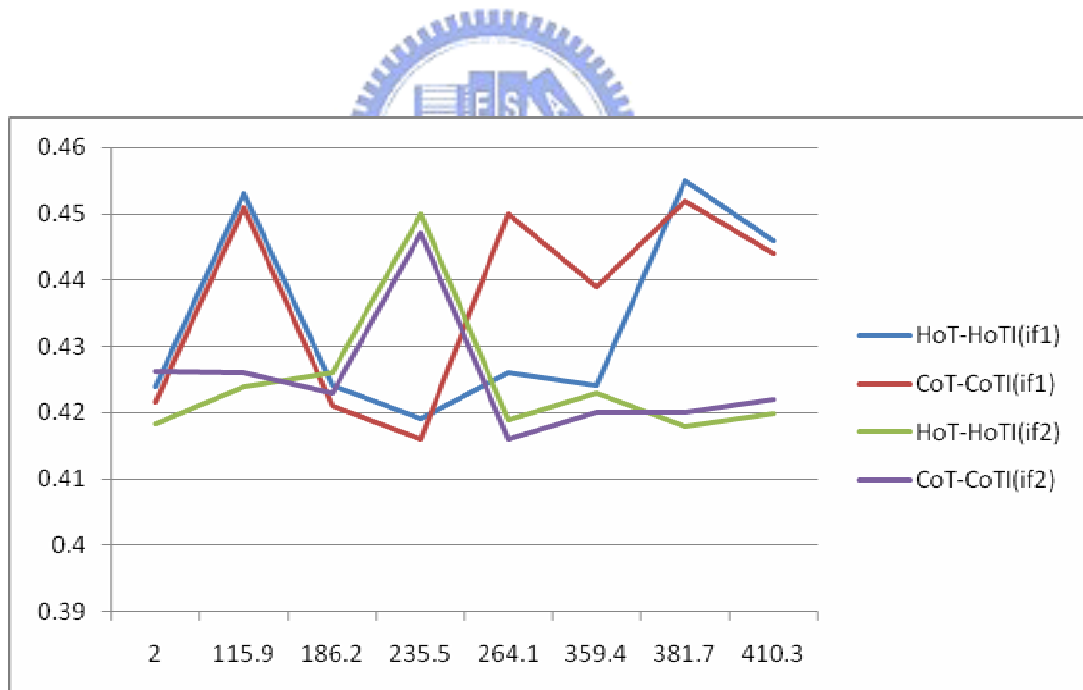


Figure 33 Latency of HoTI-HoT/CoTI-CoT for interface 1 and interface 2

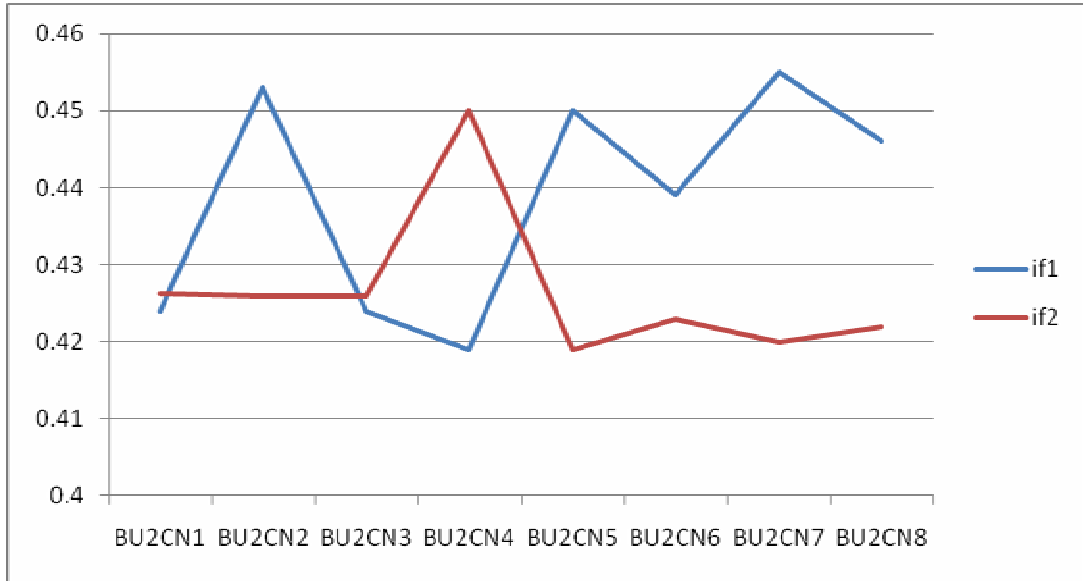


Figure 34 BU variance of interface 1 and interface 2

In our approach of RR Test, the binding update completes its process once the two separate RR tests receive responses from CN. Thus, we have to consider the latency between two interfaces. From figure xx, we can observe when the dot close to X axis, it means the latency will be low. However, if the value away from X axis either high or low, it means the variance of latency.

We have to consider this variance when applying our method to RR Test (Return Routability Test). Anyway, it's a kind of return routability authentication. We don't want users take too much time waiting for the authentication.

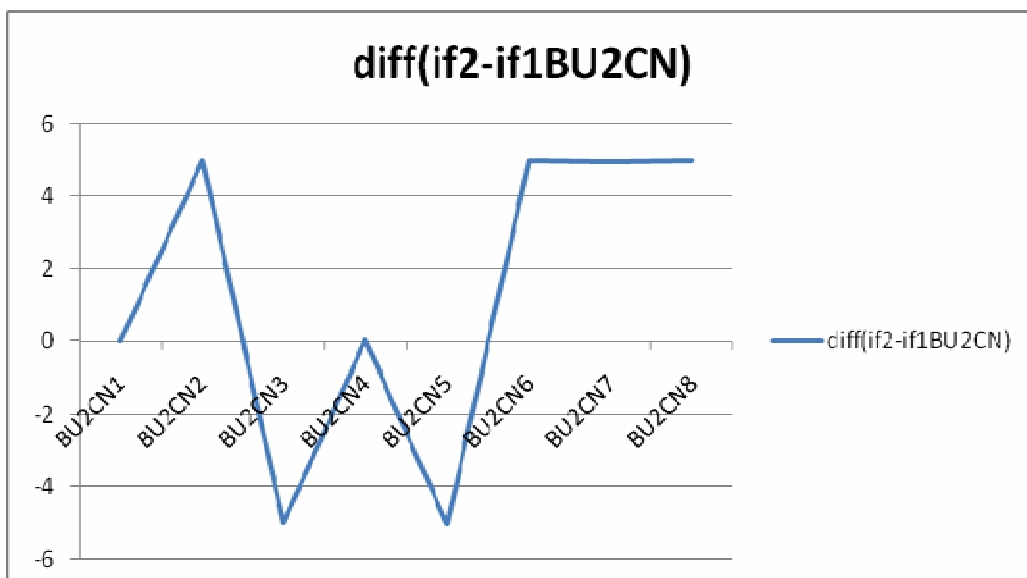


Figure 35 Latency between interface1 and interface 2

At last, by comparing the successful Binding Update to CN(Correspondent Node) in the cases of single-homed and multi-homed interface,we can observe the Binding Line in specific time period(600 sec.) through different approach.

Table 13 Comparison of successful BU to CN between single-homed and multi-homed interface

| BU2CN (Single-homed) | BU2CN (Multi-homed) |
|----------------------|---------------------|
| 5.09434 | 5.42627 |
| 40.0941 | 125.426 |
| 120.095 | 195.424 |
| 270.094 | 240.45 |
| 290.095 | 275.45 |
| 415.094 | 370.423 |
| 485.095 | 395.42 |
| 535.095 | 420.422 |

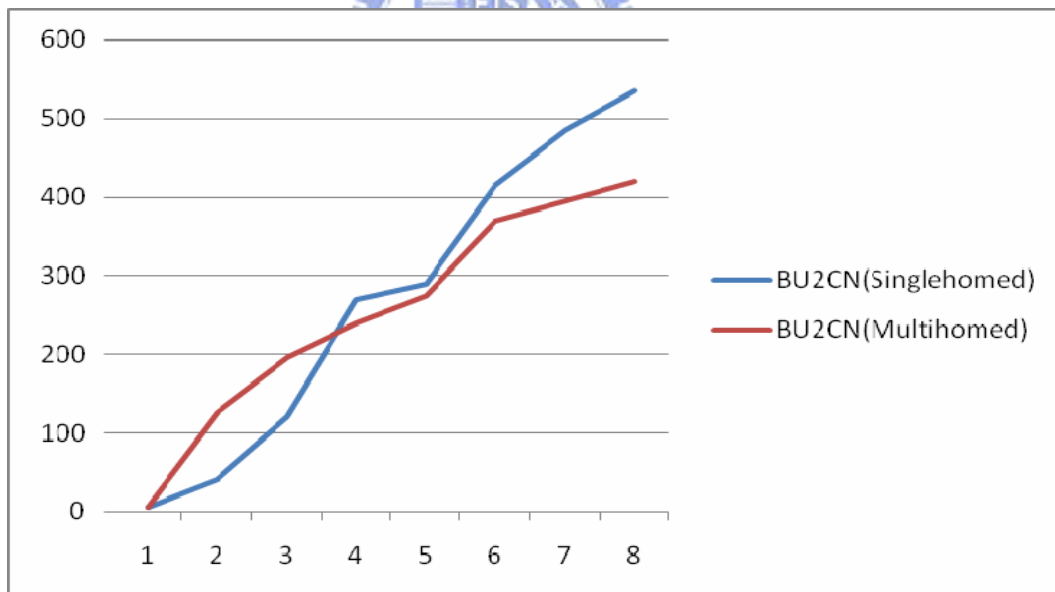


Figure 36 Comparing complete BU during specific time period of single and multi-homed interface

5.3 Discussion and Limitation

In the experiments, we assume the two interfaces are independent but we recognize the successful binding by adopting successful RR Test of both interfaces during specific time

frame. However, according to the description of SCTP features, different kinds of interfaces can have more cooperation. At the present time, several SCTP functions are incomplete in NS2. This is a motivation to extend our experiments in the future once these functions are ready.

Readers may notice that Home Agent's allocation is not the same as we described in former chapters. Actually, we assume the Home Agents should be redundant, load-balanced, distributed, or even alliance with trustworthy third parties. That is, to improve Home Agent's availability and to speed up the response time from different geographical location, the multiple intermediate Home Agents are needed. Through that way, routing paths can be more capricious which may confuse malicious attacker. The attacker will pay more cost even we don't apply complicated encryption mechanism. However, with the technique of multi-homing support, not only the source node but also the destination node can be equipped with so many interfaces which greatly increase the difficulty for man-in-the-middle attack.

Actually, in the above scenario, we did not simulate CN with multiple interfaces. If CN (Correspondent Node) is a media server with the capability of expanding interfaces, it can provide higher throughput and more complicated mix of sources address, routing path and destination address. By combining above factors definitely make up variability of communicating paths. Consequently, we would like to have more parameters in our simulation at next phase.

Mobile devices are limited by their computing capability which might substantially reduce the complexity of public key design and let alone the PKI infrastructure. Due to overwhelming demands of high bandwidth and fast transferring, it emphasizes the need of multi-path, multi-streaming, and multi-homing. Thus, we would like to provide this thesis as a light-weight authentication mechanism, selective source address and routing path, to avoid intensive computing requirement.

While implementing the simulations, we encountered lots of difficulties, such as the incompleteness of the Mobian module for MIPv6 and SCTP functions. Therefore, several protocol features are not simulated at this time. If time permit, we might have more experiments on this topic.



Chapter 6 Conclusion and Future Work

We have described attacks against Mobile IPv6 Route Optimization and mechanisms for protecting the protocol participants and third parties. Some of the attacks may be new in the sense that they have not been considered in earlier BU authentication requirements and protocol drafts. It is our hope that this paper will help in designing BU authentication protocols and in the process of choosing the protocol.

6.1 Conclusion

Our approaches, selective source address and routing path, leverage the RR Test of MIPv6 and the new transport layer protocol, SCTP, which provides a multi-homing solution.

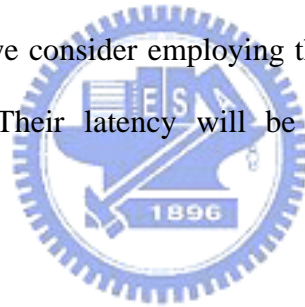
From categorized threats of MIPv6 in section 2.3, we understand most of the threats can be solved by a sound authentication methodology. Besides, from the perspective of IPv6, IPSec is bound to be the likely way for authentication and encryption in the future. However, current status of PKI was suffered as there is no pervasive MIPv6 implementation. Thus, many approaches have been raised and researches are now undertaking in this transition period.

Return routability test is one of promising approach among many other solutions and has been adopted in MIPv6 as the standard for basic authentication. Two independent paths to complete authentication is a good way but static routing paths can only prevent attacks to certain extent. That is why we would like to improve it with minimum change and yet achieve maximum effect. With the multi-homing support of SCTP and distributed Home Agents, the routing paths vary. Because of multi-homing feature, carriers can be very different, such as 802.3, 802.11, and 802.16. For each fix attachment or radio link, their access technology and network router are distinct. Attackers should have capability

to intercept signals or messages from different carrier at same time. Thus, our approach greatly reduced the probability to be compromised.

With the formula provided in section 4.4, we can compute the probability of our approach comparing to conventional RR. Our approach enhances the security during authentication and can reduce the chance of being compromised especially when CN is also a multi-homing host.

However, from the experimental result in last chapter, we also observe some issues when the Binding Update process associated to multiple interfaces. If separating the binding process to several individual sub-processes, we should consider the cooperation between them. Once the binding fail in one of process but success in the rest of binding, we should assume it as failure binding. Accordingly, this kind of waiting will inevitably increase the latency when we consider employing this mechanism to radio links, such as WiFi, 3G, and WiMAX. Their latency will be different compared to fix network attachment.



6.2 Future work

The new paradigm of the Mobile IPv6 networks presents new challenges on security due to its salient characteristics that are totally different from the conventional wired and wireless networks.

In this paper, we studied the security issues in the MIPv6 networks and analyzed the problems in order to come up a workable solution. The existing solutions, like Return Routability (RR), cannot solve the security issues for the MIPv6 networks well. Therefore, we propose the use of multiple source addresses. It may be quite a luxury in IPv4 but considerably more addresses in IPv6 gives us a chance to do that. Our mechanisms, selective source and routing paths, not only showed the ability to authenticate Binding

Update against many attacks effectively but also gained the benefit of SCTP features to increase the throughput for multimedia applications.

In the future, we intend to undertake more experiments to study feasibility of distributed HA (Home Agent), multi-homing CN (Correspondent Node) and multi-stream feature of SCTP. How distributed Home Agents synchronize data and how to find Home Agents that are near to Mobile Node in order to reduce the authentication latency? Besides, the experiment of RR latency to different carriers whether wired or wireless, 3G or 4G, can be another topic for research.



References

- [1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", RFC3775, June 2004
- [2] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.
- [3] W Fritsche, F Heissenhuber, "Mobile IPv6-Mobility Support for the Next Generation Internet", IPv6 Forum, white paper, 2000.
- [4] T. Aura and J. Arkko, "MIPv6 BU Attacks and Defenses", Internet Draft draft-aura-mipv6-bu-attacks-01, expired, March 2002.
- [5] M. Roe, T. Aura, G. O'Shea, and J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgments", draft-roe-mobileipupdateauth-02 , expired, March 2002.
- [6] P. Nikander, T. Aura, J. Arkko, G. Montenegro, and E. Nordmark, "Mobile IP version 6 Route Optimization Security Design Background" , Internet Draft draft-nikander-mobileip-v6-ro-sec-00.txt, work in progress, April 7, 2003.
- [7] R. Bush, and D. Meyer, "Some Internet Architectural Guidelines and Philosophy", RFC3439, Internet Engineering Task Force, December 2002.
- [8] E. Nordmark, "Securing MIPv6 BUs using return routability (BU3WAY)", Internet Draft draft-nordmark-mobileip-bu3way-00.txt, expired, November 2001
- [9] M. Kulkarni,A. Patel , K. Leung, " Mobile IPv4 Dynamic Home Agent (HA) Assignment", RFC 4433 ,March 2006
- [10] M Ratola, " Which Layer for Mobility?-Comparing Mobile IPv6, HIP and SCTP", Helsinki Institute for Information Technology, 2004
- [11] Feng BAO,Robert DENG,Ying QIU,Jianying ZHOU, "Improvement of Return Routability Protocol", August 30, 2004
- [12] J. Arkko,V. Devarapalli,F. Dupont,"Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents",RFC 3776,June 2004
- [13] Shaojian Fu , Mohammed Atiquzzaman, "SCTP : State of Art in Research ,Products , and Technical Challenges ", IEEE Communication Magazine, April 2004

- [14] S. Deering, S. and Hinden, R. Internet Protocol, Version 6 (IPv6) Specification. Internet Engineering Task Force (IETF) RFC2460. December 1998.
- [15] Greg O'Shea, Michael Roe, "Child-proof authentication for MIPv6 (CAM)", pp. 4-8, ACM SIGCOMM Computer Communication Review, 2001
- [16] Tuomas Aura, "Cryptographically Generated Addresses (CGA)", Volume 2851/2003, pp. 29-43, Springer Berlin/Heidelberg, Dec. 2003
- [17] Matthew Emery Neal Whitehead, Sirisha R. Medidi, "Buddy enhanced return routability for authentication in mobile IPv6", In proceedings of Defense and Security Conference on Digital Wireless Communication, vol. 5400, pages 347-358, April 12-13, 2004
- [18] Seok Joo Koh, Moon Jeong Chang, Meejeong Lee, "mSCTP for soft handover in transport layer", Communications Letters, IEEE, Volume 8, Issue 3, pp. 189-191, March 2004
- [19] Microsoft Corporation, "Understanding Mobile IPv6", April 2004
- [20] W. Haddad, L. Madour, J. Arkko, "Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)", IETF, draft-haddad-mip6-cga-omip6-04, May 3, 2005

