

**SISTEM KEAMANAN OPTIMISASI ROUTE  
PADA MOBILE IPv6**

**Tugas Akhir**

Tugas Akhir ini disusun untuk memenuhi tugas mata kuliah  
Keamanan Sistem Lanjut EC 7010

Oleh  
**MOHAMMAD FARID**  
NIM : 23203120



**DEPARTEMEN TEKNIK ELEKTRO  
PROGRAM MAGISTER TEKNOLOGI INFORMASI – DIKMENJUR  
INSTITUT TEKNOLOGI BANDUNG  
2004**

## ABSTRAKSI

Mobile IPv6 ( MIPv6) mengizinkan *Mobile Node (MN)* untuk berkomunikasi langsung dengan pasangannya yaitu *Correspondent Node (CN)* dengan kemampuannya merubah arah dengan menggunakan alamat IP. Cara ini dinamakan Optimisasi Route. Optimisasi Route mengizinkan paket untuk menyilang rute yang lebih pendek dibanding melalui *Home Agent*. Pada Optimisasi Route, pasangan titik antara *Home Address* sebagai titik tetap dari MN dan *Care-of-Address* sebagai titik temporer. Bila mengirimkan semua paket yang di tujukan kepada suatu tujuan dengan menunjukan *Care-Of-Address* , dapat berpotensi terhadap berbahaya, dengan cara pemalsuan alamat agar tidak sampai tujuan, serangan dengan pengalihan jalur dan membanjiri isi jalur yang tidak diperlukan

Pada paper ini akan dijelaskan Sistem Keamanan Optimisasi Route pada Mobile IP versi 6.

## DAFTAR ISI

Halaman	
<b>ABSTRAKSI</b> .....	i
<b>DAFTAR ISI</b> .....	ii
<b>DAFTAR GAMBAR</b> .....	iii
<b>Sistem Keamanan Optimisasi Route pada Mobile IPv6</b>	
1. Pendahuluan .....	1
2. Gangguan Keamanan MIPv6 .....	2
2.1 Serangan <i>False Binding Update</i> .....	3
2.2 Serangan <i>Man-in-the-Middle</i> .....	4
2.3 Serangan <i>Denial-of-Service</i> .....	4
2.4 Pencurian Jalur .....	5
2.5 Serangan <i>Reflection</i> dan <i>Flooding</i> .....	6
2.6 Serangan <i>MITM</i> pada <i>MPS/MPA</i> .....	7
3. Keamanan Optimisasi Route Mobile IPv6.....	7
3.1 <i>Return Routability</i> .....	9
3.2 Pembuatan Keadaan Aman .....	14
3.3 Ketepatan Waktu Binding .....	15
4. Kesimpulan .....	16
Daftar Pustaka .....	16

## DAFTAR GAMBAR

	<b>Halaman</b>
Gambar 1 Skenario komunikasi dengan dan tanpa Optimisasi Route .....	2
Gambar 2 Serangan False Binding Update.....	3
Gambar 3 Serangan man-in-the-Middle .....	4
Gambar 4 Bad Guy mencuri jalur Mobile Node (MN) .....	6
Gambar 5 Serangan Refleksi .....	7
Gambar 6 Return Routability .....	12
Gambar 7 Prosedur Return Routability .....	13

# SISTEM KEAMANAN OPTIMISASI ROUTE PADA MOBILE IPv6

## 1. Pendahuluan

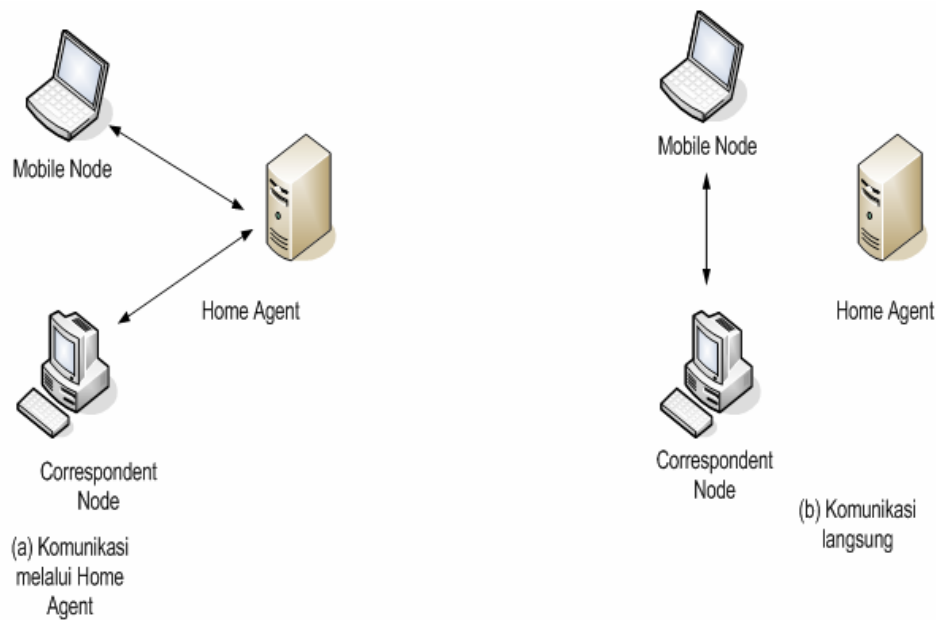
Semakin cepatnya perkembangan teknologi wireless mengakibatkan *Internet Protocol* (IP) versi 4 tidak mampu seiring dengan tuntutan peningkatan dan pengembangan kebutuhan *Internet Protocol*, sehingga untuk memenuhinya diperlukan versi yang baru, maka muncullah versi 6. Mobile IP versi 6 merupakan suatu *routing protocol* yang menyediakan connectivitas tanpa persyaratan untuk peralatan mobile yang menjelajahi antar jaringan IP generasi yang berikutnya. Pada tahun lalu, telah ada pengembang yang terus meningkat pelayanan pengguna dibidang telekomunikasi dengan menggunakan Mobile IPv6 untuk membantu pelayanan publik masa yang akan datang dengan mengakses jaringan yang tanpa kawat, terutama didaerah perkotaan dan pelabuhan udara.

Masalah yang paling besar pada *Internet Protocol* saat ini adalah perputaran kecepatan untuk mencapai suatu titik alamat jaringan yang tersedia. IPv4 mempertimbangkan sekitar  $2^{32}$  atau 4.294.967.296 alamat, sebagian besar kesalahan pada alokasi awal, tanpa meninggalkan ruang untuk pengembangan. IP versi baru yaitu IPv6 menawarkan suatu pemecahan yang lebih permanen, yaitu sekitar  $2^{128}$  atau 340.282.366.920.938.463.463.374.607.431.768.211.456 alamat.

Pada Mobile IPv6 menyediakan tambahan yang mendukung untuk mobilitas berupa Optimisasi Route. Pada Optimisasi Route, *Corresponden Node* (CN) berpasangan dengan *Mobile Node* (MN). Bingkai antara *Home Address* pada *Mobile Node* dan *Care-of-Address* digunakan untuk memodifikasi penanganan suatu paket keluaran yang mendorong masalah keamanan. Batasan keamanan ini berdasarkan penyelidikan terhadap sifat alami infrastruktur IP yang ada dan prinsip desain yang diterapkan. Ada 2 perbedaan skenario komunikasi yang dimungkinkan ketika Mobile IPv6 digunakan. Perbedaan ini dapat dilihat pada Gambar 1.

MN boleh membuat terowongan untuk mengirimkan paketnya kepada Home Agent yang didalamnya didecapsulasi dan dilanjutkan ke CN. Jika

optimisasi route digunakan (misalnya *MN* mengirim *Binding Updates (BUs)* kepada *CN*), *MN* akan mengirim langsung kepada *CN* setelah penambahan *Home Address*. *CN* juga akan mengirim paket-paketnya langsung kepada *MN* dengan menggunakan *routing header type 2* yang mengandung *Home Address* pada *MN*. Ada dua jenis penyerangan yaitu *Bad Guy* meluncurkan pada jalur dan diluar jalur. Penyerangan pada jalur merupakan salah satu yang dapat dilihat paket melalui jalur tertentu antara 2 titik. Penyerang pada jalur antara *MN* dan *CN* atau rangkaian antara keduanya dimana paket berada pada dua titik rutenya. Kebalikannya penyerangan pada luar jalur penyerang tidak dapat melihat paket yang dikirim antara 2 titik dan dia berusaha untuk menyerangnya.



Gambar 1. Skenario komunikasi dengan dan tanpa Optimisasi Route

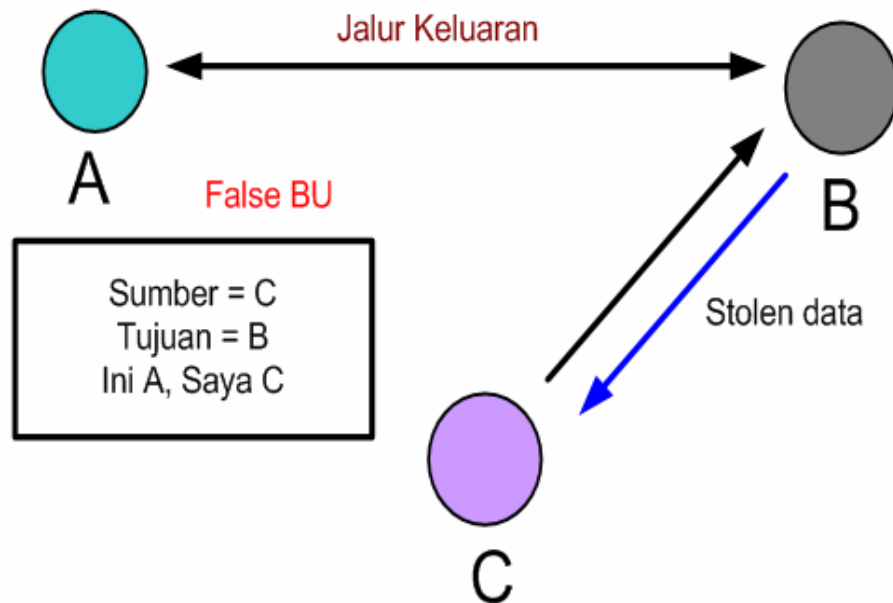
## 2. Gangguan Keamanan MIPv6

Maksud dari penyerangan atau ancaman gangguan yang dapat merusak *CN* dan menyebabkan paket-paket yang dikirimkan salah alamat. *Binding Updates (BUs)* digunakan untuk mengalihkan jalur dari satu alamat ke alamat yang lain. Jika tidak hati-hati dapat membawa dampak merugikan komunikasi antara *MN* dan *CN*.

## 2.1 Serangan False Binding Update

*Spoofed binding update* mungkin dikirim ke *Home Agent (HA)* dan *CN*. Sebagai tiap titik IPv6 diharapkan untuk menyebarkan seperti titik MIPv6 juga, dan tiap titik MIPv6 diharapkan untuk *CN*, ancaman keamanan *Binding Update* dapat dilihat seperti yang digunakan untuk keseluruhan Internet.

Dengan *spoofing binding update*, penyerang dapat mengalihkan jalurnya sendiri atau titik yang lain dan mencegah titik yang asli dari jalur tujuan penerimanya. Seperti contoh, A dan B sedang berkomunikasi satu sama lain, kemudian penyerang pada titik C mengirimkan paket *spoofing binding update* ke B, pengakuan A dengan *care-of-address (CoA)* dari C. Ini akan menyebabkan B menciptakan bungkus untuk CoA titik A dan berikut lalu lintas lebih lanjut ke C, hal ini diakui sebagai *CoA* baru pada titik A. Titik A tidak akan menerima data yang dimaksud jika data di paket tidaklah dilindungi dengan *cryptografi*, C akan mampu lihat semua informasi di titik A.

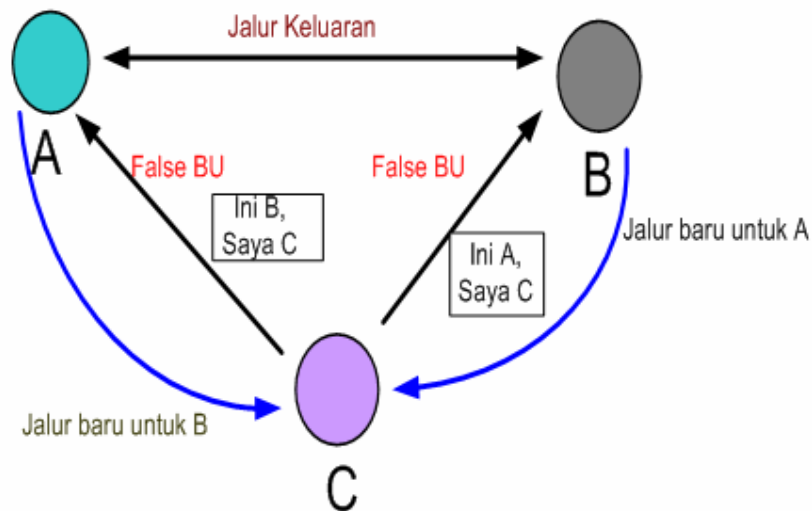


Gambar 2. Serangan False Binding Update

## 2.2 Serangan Man-in-the-Middle

Penyerang boleh juga mengirim *spoof BUs* untuk dua CN dalam rangka menetapkan dirinya sebagai *Man-in-the-Middle* antara MN dan CN. Seperti contoh, jika A dan B sedang berkomunikasi, penyerang bisa mengirimkan keduanya *Spoofed Binding Update* dengan CoA dari alamatnya sendiri. Ini akan menyebabkan keduanya A dan B mengirimkan semua paket ke C antara satu sama lain.

Tanpa Optimisasi Route MIPv6, suatu penyerang mempunyai jalur diantaranya dan dapat menangkap dan membaca paket antara A dan B.



Gambar 3 Serangan Man-in-the-Middle

## 2.3 Serangan Denial-of-Service

Serangan *Denial of Service (DoS)* merupakan suatu usaha (dalam bentuk serangan) untuk melumpuhkan sistem yang menjadi target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya (*denial-of service*) atau tingkat servis menurun dengan. Cara melumpuhkan dapat bermacam-macam dan akibatnya pun dapat beragam. Sistem yang diserang dapat menjadi “bengong” (*hang, crash*), tidak berfungsi atau kinerjanya menjadi turun (beban CPU tinggi).

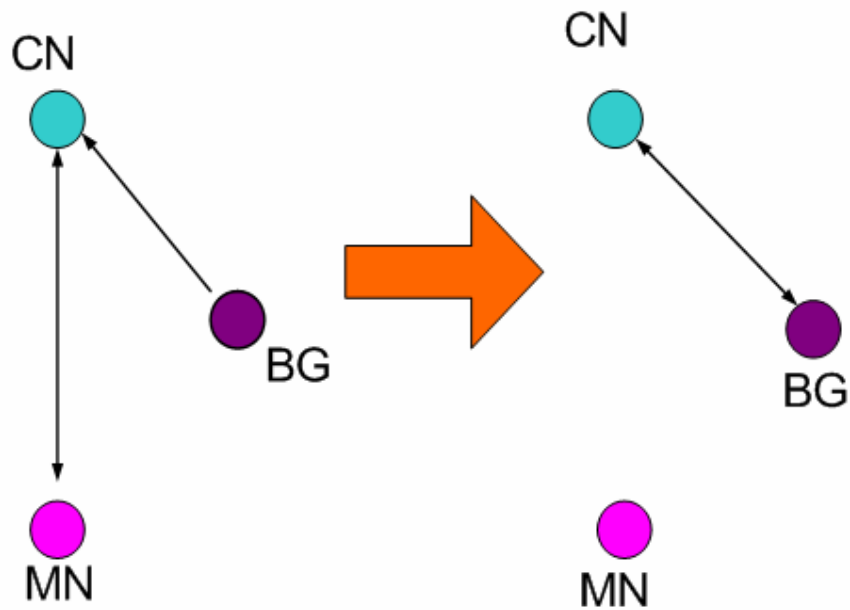
Serangan *DoS* berbeda dengan kejahatan pencurian data atau kejahatan memonitor informasi yang lalu lalang. Dalam serangan *DoS* tidak ada yang dicuri. Selain itu serangan *DoS* sering digunakan sebagai bagian dari serangan lainnya yaitu dalam serangan *IPspoofing* ( seolah serangan dari tempat lain dengan nomor *IP* milik orang lain), seringkali *DoS* digunakan untuk membungkam server yang akan *dispoof*.

Dasar penyerangan ini diantaranya adalah :

1. dengan pengiriman *spoofed BU*, penyerang dapat mengalihkan jalur semua paket pengiriman antara dua titik *IP* pada alamat yang kosong. Serangan ini dapat mengganggu jalur komunikasi antar titik. Serangan beberapa titik internet dapat ditargetkan dan ditetapkan titiknya sepanjang infratraktur yang peka.
2. dengan pengiriman *spoofed BU*, penyerang dapat mengalihkan jalur lalu lintas alamat *IP*. Hal ini digunakan untuk megebom alamat internet dengan sejumlah paket yang berlebihan. Penyerang dapat juga mengalihkan jalur data kepada satu atau lebih alamat *IP* pada jaringan. Serangan *flooding* yang sederhana, penyerang mengetahui bahwa suatu arus data yang besar dari titik A ke B dan pengalihan jalur ke tujuan alamat C. Namun A segera menghentikan pengiriman data sebat tidak mau menerima pengakuan dari B. Titik A lebih canggih dan bertindak sendiri seperti B. Pada awalnya seperti arus data dan kemudian mengalihkan jalur ke alamat C. Penyerang akan dapat menjadi *spoof*.

#### **2.4 Pencurian Jalur**

Bila *Bad Guy* (seseorang yang tidak dikehendaki pada suatu bagian tertentu) mengetahui home address pada *MN* ( tdaka sulit karena semua orang dapat mengetahui dan dapat disimpan pada *DNS*), dia dapat mengirim *BUs* kepada *CN* untuk mengalihkan jalur *MN* kepadanya. Pada contoh ini *Bad Guy* mencuri jalur asli *MN* dan kemungkinan dapat membajak hubungan *MN* dengan *CN* dan menganggap dirinya *MN* sehingga *MN* dapat berhenti untuk berkomunikasi. Dengan catatan dalam kasus ini *Bad Guy* bukan bagian diantara *MN* dan *CN*.

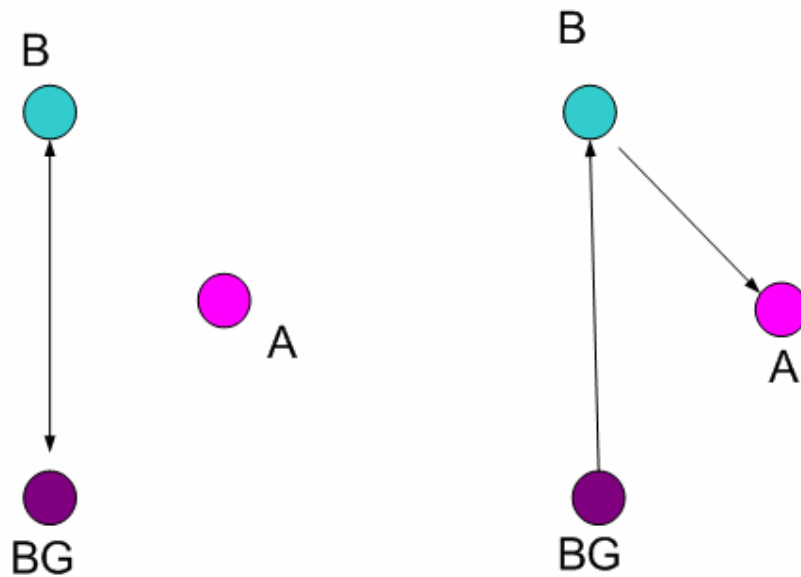


Gambar 4. Bad Guy mencuri jalur Mobile Node (MN)

### 2.5 Serangan Reflektion dan Flooding

A dan B dapat berkomunikasi dengan sempurna bila A mengirim pesan kepada B dan B menjawabnya. Namun jika A mengirim pesan kepada B dan B menjawabnya kepada C. Ini dinamakan serangan refleksi. Sedangkan kesempurnaan komunikasi antara satu dengan yang lain melalui agent penyiaran. Pengiriman paket dari A ke B. B tidak boleh menjawab kepada C. Hal ini dapat diterima bila B mengirim paket yang sama kepada C dan C menjawab kepada A, tetapi hal ini tidak diterima untuk B yang menjawab untuk semua titik. *Bad Guy* boleh melancarkan serangan refleksi. Lihat gambar dibawah ini.

Dalam kasus ini *Bad Guy* dapat mulai hubungan dengan B. Setelah hubungan dimulai, *Bad Guy* dapat mengirim *BU*s kepada B dan B meminta langsung jalurnya untuk alamat yang lain, yang mana ditugaskan kepada A. Hal ini menyebabkan B mengirim semua paket kepada A. Jika B adalah *server streaming video* sebagai contoh *Bad Guy* sedang mendownload file yang besar dari B, hal ini menyebabkan B membanjiri (*flooding*) jalur A dengan informasi yang tidak ia kehendaki. Serangan *Flooding* sering disebut serangan pengeboman.



Gambar 5. Serangan Refleksi

### 2.6 Serangan MITM pada MPS/MPA

Pesan *Mobile Prefix Solicitation (MPS)* dan *Mobile Prefix Advertisement (MPA)* digunakan MN untuk memperhatikan awaln rangkaian home. MPS mengirim dengan MN dan menyebabkan *Home agent* mengirim MPA. MN menggunakan informasi pada MPA untuk mengikat *home addressnya* kepada *care-of-addressnya*. *Bad Guy* dapat meluncurkan serangan MITM pada pesan ini jika terjadi pada jalur antara MN dan *Home Agent*. *Bad Guy* dapat menginterupsi dan merubah isinya.

### 3. Keamanan Optimisasi Route Mobile Ipv6

Keamanan optimisasi route pada Mobile IPv6 dirancang secara hati-hati guna mencegah atau mengurangi jumlah ancaman seperti yang diuraikan diatas. Ada beberapa hal yang diperhatikan tentang keamanan *BUs* yang dikirimkan kepada *CN* dari MN pada lingkungan MIPv6. Kelompok kerja Mobile IP telah mengenali keamanan ini dan sudah memperkenalkannya sebagai model ancaman dan persyaratan untuk keamanan. Percobaan untuk memiliki suatu keamanan *BUs*

tentu saja sebuah proses tantangan. *BU*s dikirim untuk mencapai optimisasi route arus paket dari *CN* ke *MN*.

Ancaman keamanan dapat muncul ketika penyerang menyamar sebagai *MN* yang mengirim *BU*s gadungan kepada *CN*. Sekarang *CN* salah berasumsi bahwa *MN* telah bergerak ke *CoA* baru dan memperbaharui masukannya. Komunikasi berikutnya dari *CN* ke *MN* akan dialihkan penyerang. *MN* kemudian dapat menyadari setelah suatu waktu tidak menerima komunikasi dan dapat mencoba untuk mengirim binding yang baru kepada *CN*, namun penyerang kemudian dapat mengalihkan jalur paket ini ke beberapa tempat lain, mengirimkan *BU*s gadungan kepada *MN* (menurut dugaan *CN*) dan menyisipkan diri sendiri sebagai orang ditengah-tengah. Serangan semacam ini dinamakan sebagai serangan tempat persembunyian *BU*s yang aktif.

Persyaratan dasar untuk mencegah ancaman ini adalah *CN* harus membuktikan keaslian titik yang mengirimkan *BU*s. *CN* hanya memperbaharuinya tempat persembunyian *binding* setelah memverifikasi bahwa pengirim diberi hak untuk membuat tempat persembunyian masukan. Namun dapat diperhatikan bila mekanisme pengesahan yang lemah menyebabkan asosiasi keamanan yang kuat diantara kedua titik yang sebelumnya tidak dikenal (dalam hal ini *CN* dan *MN*) akan memerlukan pembangunan infrastruktur kunci publik secara global yang tidak satupun pilihan dimungkinkan. Beberapa draft internet untuk pengesahan *BU*s sebagai berikut :

1. *Protokol Penetapan Kunci Pengesahan Binding untuk MIPv6 (Binding Authentication Key Establishment (BAKE))*

*BAKE* mengusulkan suatu metoda untuk menyediakan informasi kunci untuk digunakan antara *MN* dan *CN*. Informasi kunci ini telah digunakan untuk membuktikan keaslian dari *BU*s. Pada asosiasi keamanan *BAKE* diciptakan antara *MN* dan *CN* pengolahan *BU*. *CN* menyediakan beberapa data yang acak yang mana *MN* menggunakan sebagai masukan suatu algoritma dan menciptakan suatu asosiasi keamanan. Setelah itu digunakan untuk menciptakan data pengesahan. Data pengesahan diperlukan karena disediakan salah satu pilihan keamanan *BU*s.

Ada tiga jenis pesan yang dibentuk disini yaitu *MN* mengirim kepada *CN* , ini dibutuhkan *Binding Security Assosiasi (BSA)* yaitu suatu assosiasi keamanan antara *CN* dan *MN* yang dibentuk untuk memproduksi dan membuktikan data pengesahan yang dilewati tujuan kemudian *CN* mengirim suatu kunci *BU* kepada *MN* melalui terowongan sampai *Home Agent (HA)*. *MN* kemudian mengirim *Binding Key Establishment Destination* kepada *CN* untuk menetapkan *BSA*. Protokol *BAKE* tidak memastikan bahwa pesan apapun yang berisi muatan keseluruhan dari suatu kunci.dengan demikian diperlukan keamanan tambahan. Protokol ini bekerja baik untuk semua kasus kecuali titik kejahatan diposisikan pada bagian antara *CN* dan *HA* sepanjang *BUs*.

2. *Pengamanan MIPv6 BUs yang menggunakan Return Routability (BUS3WAY)*  
*BUS3WAY* menggunakan *return routability* untuk membuktikan keaslian dari pengirim *BUs* yang digunakan pada tiap-tiap pesan *BUs*. Protokol ini menggunakan mekanisme *three-way-handshake* (cara tiga jabat tangan) yang menjamin *BUs*. Pesan yang pertama adalah *BUs* meminta dikirimkan dari *MN* kepada *CN*. Pesan berikutnya *BUs challenge* dikirimkan dari *CN* kepada *MN*. *CN* dapat menggunakan untuk memverifikasi dengan memberi pesan isyarat kepada seseorang seperti cara jabat tangan tiga orang. Pesan yang ketiga dari jabat tangan tiga orang adalah pesan *BUs* dikirimkan oleh *MN* kepada *CN*. Pesan ini mengulangi informasi dari *BUs challenge* dan meliputi jumlah acak yang digemakan oleh *CN* dalam pesan pengakuan . Demikian mekanisme *three-way handshake* telah lengkap dan *BUs* telah dibuat aman.

### **3.1 Return Routability (RR)**

*Return Routability (RR)* adalah nama dari mekanisme dasar keamanan optimisasi route pada Mobil IPv6. Pada dasarnya hal ini artikan bahwa suatu titik memverifikasi suatu titik yang dapat beraksi terhadap paket yang dikirim kepada alamat pemberi. Hasil pemeriksaan positif jika infrastruktur route dikompromikan atau jika ada penyerang diantara pemeriksa dan alamat yang dibuktikan,kecuali diperkirakan sebagai jawaban yang baik yang menunjukkan bahwa suatu titik

diberi alamat dan titik menjawab pemeriksaan yang dikirim. Dasar mekanismenya *return routability* terdiri dari dua pengecekan yaitu pengecekan *Home Address* dan pengecekan *Care-of-Address (CoA)*. (lihat Gambar 6 )

Kenyataannya *return routability* memeriksa pasangan pesan (*Home Test, Binding Update*) dan (*Care-of-Test, Binding Update*). Pesan *Home Test Init (HoTI)* dan *Care-of-Test Init (CoTI)* hanya dibutuhkan untuk mentrigger paket test dan *Binding Update* bekerja mengkombinasikan routabilitas respon kedua test.

Inti dari prosedur *return routability* adalah bahwa *MN* meminta bahwa *CN* untuk mengetes kepemilikan dari *home address* dan *care-of-address*. Hal ini dilakukan dengan mengirim 2 pesan yang independen yaitu *Home Address Test Init (HoTI)* dan *Care-of-Address Test Init (CoTI)*. *CN* membuat dan mengirim 2 token, masing-masing alamat (*home address dan care-of-address*) dalam 2 bagian pesan yaitu *Home Test (HoT)* dan *Care-of-Test (CoT)*. *MN* menggunakan keduanya untuk membuat kunci ( $K_{bm}$ ) yang dapat digunakan untuk autentikasi pesan *BUs* kepada *CN*. Karena *CN* mengetahui semua informasi yang dibutuhkan untuk menghasilkan kunci, ia dapat mereproduksinya ketika *BUs* dikirim dan juga keaslian pesan. Kunci yang sama digunakan untuk autentikasi pengakuan binding (*binding acknowledgment*).

Dari gambar yang ditunjukkan pada Gambar 7 ada beberapa pesan kiriman yaitu :

1. Pesan *HoTI* yang dikirimkan dari *MN* kepada Home Agent

Isi dari pesan ini adalah :

```
IPv6 header
src = care-of address
dst = home agent
ESP header
IPv6 header
src = home address
dst = correspondent node
Mobility Header type 1
Home init cookie
```

2. Pesan *CoTI* yang dikirim dari *MN* kepada *CN*

Isi dari pesan ini adalah :

```
IPv6 header
src = care-of address
dst = correspondent node
Mobility Header type 2
```

Care-of init cookie

3. Pesan *CoT* yang dikirim dari *CN* kepada *MN*

Isi dari pesan ini adalah :

IPv6 header  
src = correspondent node  
dst = care-of address  
Mobility Header type 4  
Care-of nonce index  
Care-of init cookie  
Care-of keygen token

4. Pesan *HoT* yang dikirim dari *CN* kepada *Home Agent*

Isi dari pesan ini adalah :

IPv6 header  
src = correspondent node  
dst = home address  
Mobility Header type 3  
Home nonce index  
Home init cookie  
Home keygen token

5. Pesan *Binding Update* dari *MN* kepada *CN*

Isi dari pesan ini adalah :

IPv6 header  
src = care-of address  
dst = correspondent node  
DST-options header  
Home address option  
Mobility header type 5  
Binding update  
Nonce indices option  
[optional alternate-care-of address option]  
Authorization data option

Pesan Alternatif jika masukan tempat persembunyian, isi pesannya adalah:

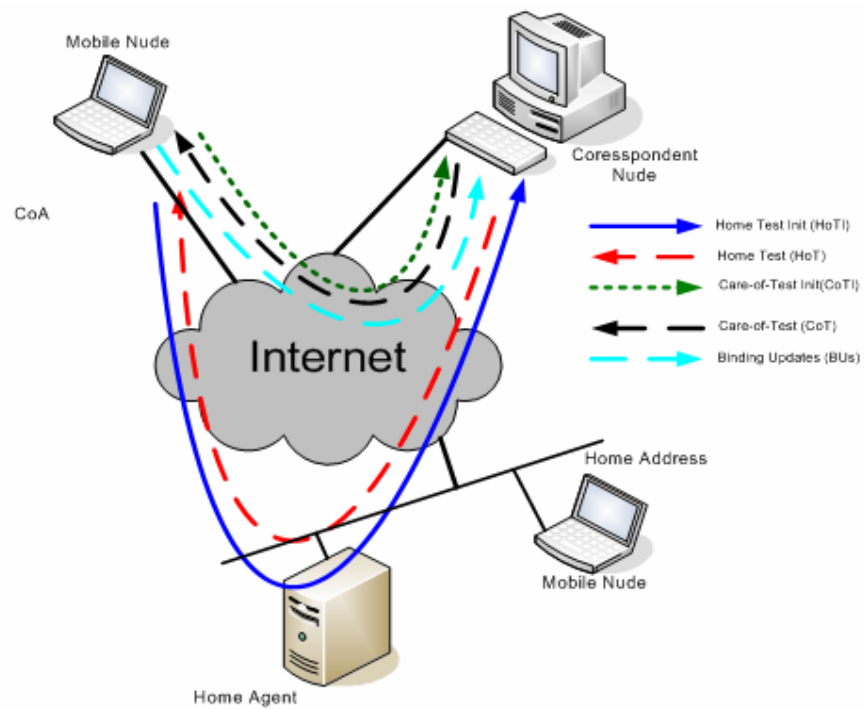
IPv6 header  
src = care-of address  
dst = correspondent node  
Routing header type 2  
Home address\_cn  
DST-options header  
Home address option  
Mobility header type 5  
Binding update  
Nonce indices option  
[optional alternate-care-of address option]  
Authorization data option

6. Pesan *Binding ack* dari *CN* kepada *MN*

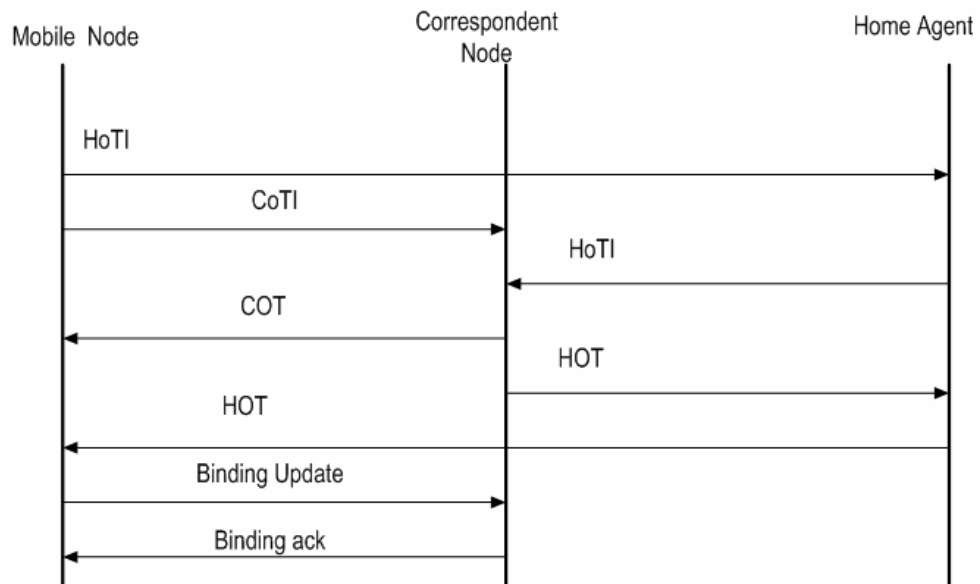
Isi dari pesan ini adalah :

IPv6 header

src: correspondent node  
 dst: care-of address  
 Routing header type 2  
 mobile node's home address  
 DST-options header  
 Home address option (if the correspondent node were also a mobile node)  
 Mobility header type 6  
 Binding acknowledgment  
 [optional binding refresh advice option]  
 Authorization data option



Gambar 6 Return Routability



Gambar 7. Operasi Prosedur Return Routability

### 1. Pengecekan Home Address

Pengecekan *Home Address* terdiri dari paket *Home Test (HoT)* dan *Binding Update (BUs)*. *HoT* diasumsikan seperti terowongan antara *Home Agent* dengan *MN*. *HoT* terdiri dari token yang menghasilkan cryptografi, token kunci rahasia yang dibentuk dari hasil perhitungan fungsi hash atas panggabungan dari kunci  $K_{cn}$  yang dikenal oleh *CN*, alamat sumber paket *HoTI* dan waktu sekarang. Waktu sekarang mengandung paket *HoTI* yang membiarkan *CN* mudah menemukan waktu yang sesuai.

$$\text{Token home} = \text{hash} ( K_{cn} \mid \text{alamat sumber} \mid \text{waktu} \mid 0 )$$

Dalam banyak hal paket *HoT* menyampaikan 2 segmen yang berbeda dari internet. Pertama garis menyilang dari *CN* ke *Home Agent*. Pada perjalanan ini tidak dilindungi dan secara diam-diam mendengarkan isi pada bagian ini. *Home Agent* kemudian mengandung *IPsec* dan terowongan perlindungan ESP, pembuatan ini tidak mungkin untuk diluar isi paket.

## 2. *Pengecekan Care-of-Address*

Dari segi pandangan *CN*, pengecekan keamanan sangat simple untuk Home Address. Perbedaannya hanya paketnya sekarang dikirim langsung kepada *CoA* dari *MN*. Lagi pula token dibuat dengan cara sedikit berbeda untuk membuat hal ini tidak mungkin digunakan *home token* untuk keamanan token atau sebaliknya.

Keamanan token = hash ( $K_{cn}$  | alamat sumber | waktu sekarang | 1)

*CoT* menyilang hanya 1 kaki langsung dari *CN* ke *MN*, sisanya tidak dilindungi sepanjang jalan ini. Pembuatan mendekati *CN*, pada bagian *CN* ke *MN* atau dekat dengan *MN*.

## 3. *Pembentukan Binding Update pertama*

Jika *MN* menerima kedua pesan *HoT* dan *CoT*, pembuatan *binding key*  $K_{bm}$  oleh fungsi *hash* terhadap penggabungan dari token penerima.

$K_{bm} = \text{hash}(\text{home token} | \text{keamanan token})$

Kunci ini digunakan untuk perlindungan awal dan *BU*s berikutnya sepanjang kunci itu benar. Kunci  $K_{bm}$  menyediakan untuk semua orang yang dapat menerima kedua pesan *CoT* dan *HoT*.

Namun route biasanya berbeda dengan route pada jaringan dan *HoT* mengirimkan terowongan enkripsi dan *Home Agent* ke *MN*.

### 3.2 Pembuatan Keadaan Aman

*CN* dapat tidak berstatus sampai menerima *BU*s yang pertama. Keadaan seperti ini tidak diperlukan untuk menerima atau menjawab pesan *HoTI* atau *CoTI*. Pertolongan dalam keadaan seperti ini *Denial-of-Service* tidak memiliki memori yang dipesan ketika pemrosesan pesan *HoTI* dan *CoTI*. Lagi pula pemrosesan *HoTI* dan *CoTI* dirancang lebih ringan dan dapat dibatasi bila diperlukan.

Ketika menerima *BU* yang pertama, *CN* melewati prosedur yang agak rumit. Tujuan prosedur ini memastikan bahwa tentu saja *MN* telah menerima *HoT* dan *CoT* yang dikirim untuk tuntutan *home* dan *care-of-address*, berturut-turut

untuk meyakinkan *CN* untuk membelanjakan CPU atau mencari sumber untuk pengecekan ini.

Karena *CN* tidak memiliki status ketika *BU* tiba, *BU* itu sendiri harus berisi sejumlah informasi yang cukup lalu status yang relevan dapat diciptakan. Pemberian alamat *IP*, tanda waktu sekarang dan kunci  $K_{cn}$ , *CN* dapat membuat lagi *token home* dan *care-of-token* dengan sedikit memory lookup dan dua aplikasi fungsi hash. Secepatnya *CN* membuat lagi token yang lain, pemberian kunci  $K_{bm}$ . Kunci itu kemudian digunakan untuk memverifikasi *MAC* yang melindungi integritas dan keaslian *BUs*.  $K_{bm}$  yang sama dapat digunakan untuk sementara sampai *MN* pindah dan mendapat *care-of-address* yang baru dengan *token address* terakhir atau *token home* terakhir.

### 3.3 Kecepatan Waktu Binding

Masukan tempat persembunyian sepanjang kunci  $K_{bm}$  menghadirkan status return routability jaringan ketika pesan *HoT* dan *CoT* dikirimkan. Sekarang penyerang khusus dapat secara diam-diam mendengarkan pesan *HoT* pada waktu yang tepat. Jika *HoT* memiliki batasan atau waktu yang lama, penyerang diijinkan untuk membuat serangan perubahan waktu. Dalam hal ini, pada arsitektur IPv4, penyerang yang berada diantara *CN* dan *Home Agent* dapat membuat serangan hanya selama penyerang dapat secara diam-diam mendengar komunikasi. Selama perjalanan *HoT* dan konsekuensi untuk mengirim *BU* yang benar sepanjang waktu, penyerang diijinkan melanjutkan serangan sampai penyerang tidak dapat secara diam-diam mendengarkan pada suatu bagian.

Batasan kesungguhan dan ancaman perubahan waktu, kebenaran token dibatasi beberapa menit. Batas efektif kunci  $K_{bm}$  dan waktu yang dihasilkan *BU* dan masukan tempat persembunyian. Waktu yang singkat merupakan aspek kebutuhan yang diberikan pada design keamanan. Mereka membersihkan kerusakan untuk efisiensi dan kekuatan. Dalam hal ini pasangan pesan *HoTI/HoT* boleh diubah melalui *Home Agent* setiap beberapa menit.

#### 4. Kesimpulan

Pada keamanan MIPv6 melibatkan 3 komponen yaitu *Mobile Node*, *Coresspondent Node* dan *Home Agent*. Dari 3 komponen ini muncul perbedaan pandangan tentang hubungan keamanan Mobile IPv6 yaitu hubungan keamanan antara *Mobile Node* dengan *Correspondent Node* dan hubungan keamanan antara *Mobile Node* dengan *Home Agent*. Sistem Keamanan Optimisasi Route pada MIPv6 berkerja menggunakan prosedur *return routability* . Prosedur *return routability* menggunakan dasar mekanisme pengecekan *Home Address* dan pengecekan *Care-of-Address* dari alamat pemberi paket .

#### Daftar pustaka

- [1] Al-Ekram, Raihan. "Mobility Support in IPv6". Waterloo University. 15 Nov 2001.  
[URL:http://www.swen.uwaterloo.ca/~regram/presentations/mobility\\_support\\_in\\_ipv6.pdf](http://www.swen.uwaterloo.ca/~regram/presentations/mobility_support_in_ipv6.pdf) (17 Des 2004).
- [2] Aura, Thomas. "Mobile IPv6 Security". Microsoft Research. 18 Sept 2002.  
[URL:http://research.microsoft.com/users/tuomaura/MobileIPv6/Mobile-IPv6-Security-18Sep2002.pdf](http://research.microsoft.com/users/tuomaura/MobileIPv6/Mobile-IPv6-Security-18Sep2002.pdf) (17 Des 2004).
- [3] Deering, S., Hinden, R. "Internet Protocol Version 6". IETF RFC 2460. Dec. 1998.  
[URL:ftp://ftp.rfc-editor.org/in-notes/rfc2460.txt](ftp://ftp.rfc-editor.org/in-notes/rfc2460.txt). (17 Des 2004).
- [4] Finney, Joe, McCaffrey. "Mobile IPv6: A Home In Every City?" DMRG, Computer Department, Lancaster University.  
[URL:http://www.newcastle.research.ec.org/cabernet/workshops/radicals/2002/Papers/Finney.pdf](http://www.newcastle.research.ec.org/cabernet/workshops/radicals/2002/Papers/Finney.pdf) (17 Des 2004).
- [5] "Introducing Mobile IPv6 in 2G and 3G Networks". Nokia White Paper. 2001.  
[URL:http://www.nokia.com/downloads/solutions/operators/intro\\_to\\_mipv6.pdf](http://www.nokia.com/downloads/solutions/operators/intro_to_mipv6.pdf) (17 Des 2004).
- [6] Irava, Venkata S. "Ensuring security of the Binding updates". IETF Draft.  
[URL:http://www.eecs.wsu.edu/~smedidi/Venkata.txt](http://www.eecs.wsu.edu/~smedidi/Venkata.txt) (17 Des 2004).
- [7] Johnson, David B, Perkins, Charles E., Arkko, Jari. "Mobility Support in IPv6". 29 October 2002.  
[URL:http://ntrg.cs.tcd.ie/htewari/papers/mobicom96.pdf](http://ntrg.cs.tcd.ie/htewari/papers/mobicom96.pdf) (27 Des 2004).

- [8] Kato, Tsuguo, Takechi, Ryuichi, Ono, Hideaki. "A Study of Mobile IPv6 Based Mobility Management Architecture". Fujitsu. Sci Tech. J. 37 1 June 2001  
URL:<http://magazine.fujitsu.com/us/vol37-1/paper09.pdf> ( 17 Des 2004).
- [9] Sudanthi,Sudha. "Mobile IPv6". SANS Institut.17 Januari 2003.  
URL: [http://www.giac.org/practical/GSEC/Sudha\\_Sudanthi\\_GSEC.pdf](http://www.giac.org/practical/GSEC/Sudha_Sudanthi_GSEC.pdf) (27 Des 2004).
- [10] \_\_\_\_\_ "Security Mobile IPv6 Signaling",  
URL:[http://searchsecurity.techtarget.com/searchSecurity/downloads/Mobile IPv6\\_ch05.pdf](http://searchsecurity.techtarget.com/searchSecurity/downloads/Mobile_IPv6_ch05.pdf) (20 Sept 2004)
- [11] P. Nikander, T. Aura, J. Arkko, G. Montenegro, and E. Nordmark, "Mobile IP version 6 Route (MIPv6) Optimization Security Design". URL :  
<http://research.microsoft.com/users/tuomaura/Publications/nikander+-vtc2003f.pdf> (20 Sept 2004)