Metode Pengamanan Jaringan LTE/SAE dari Serangan Berbasis Protokol IP

Makalah Akhir

EL6115 Secure Operations and Incident Response

Harashta Tatimma Larasati
23216117

Abstrak

Pada jaringan Long Term Evolution/System Architecture Evolution (LTE/SAE), keseluruhan sistemnya telah berbasis Internet Protocol (IP). Hal ini menimbulkan kerentanan baru yang tidak terjadi pada teknologi jaringan seluler sebelumnya. Pada makalah ini, dilakukan pemetaan serangan berbasis IP yang dapat terjadi pada jaringan LTE/SAE beserta *entry point*-nya, kemudian dibuat solusi generik untuk mengamankan jaringan LTE/SAE. Hasil yang diperoleh adalah bahwa serangan berbasis IP yang dapat terjadi pada jaringan LTE/SAE adalah berbagai serangan terhadap backhaul, VoLTE-based Attack, GTP-based Attack, dan Diameter-based Attack. *Entry point* serangan adalah dari UE, eNB, EPC, dan jaringan eksternal. Solusi keamanan generik yang sebaiknya diterapkan adalah adanya sistem yang melakukan proses *capturing*, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), sistem monitoring, dan pengamanan trafik dengan metode pada *framework* IPSec.

Kata Kunci: *LTE, SAE,* Attack, Enforcement Points

Daftar Isi

1 Pendahuluan **1**

2 Jaringan LTE/SAE **1**
2.1 *Overview* Jaringan LTE/SAE 1
2.2 Arsitektur Jaringan LTE/SAE 2
2.3 Perbedaan LTE/SAE dengan UMTS 3
2.4 Arsitektur Keamanan Jaringan LTE/SAE 5

3 Ancaman Keamanan pada Jaringan LTE/SAE **6**
3.1 Serangan pada jaringan LTE/SAE 6
3.2 Pemetaan serangan pada jaringan LTE/SAE 12

4 Metode Pengamanan pada Jaringan LTE/SAE **13**
4.1 Solusi Pengamanan Per Kasus 13
4.2 *Security Enforcement Points* 15
4.3 Resume Metode Pengamanan Jaringan LTE/SAE dari Serangan Berbasis IP 17

5 Kesimpulan **18**

Daftar Gambar

1 Arsitektur Jaringan LTE/SAE [7]. 3
2 Perbedaan Arsitektur UMTS/3G dan LTE/4G [3]. 4
3 Posisi TCP/IP pada *Cellular Stack* [9]. 5
4 Arsitektur Keamanan Jaringan LTE/SAE [10]. 6
5 Kategorisasi Serangan pada Jaringan LTE/SAE 7
6 Model *Threat Space* pada [11]. 13
7 *Security Enforcement Points* pada Jaringan LTE/SAE [21]. . . . 15

Daftar Tabel

1 Pemetaan Serangan Berbasis IP pada Jaringan LTE/SAE (diolah oleh penulis dari [7, 11] 14

1 Pendahuluan

Long Term Evolution (LTE) atau 4G adalah teknologi jaringan akses seluler yang distandarkan oleh 3GPP. Bersama dengan System Architecture Evolution (SAE) sebagai arsitektur *core network*, keduanya membentuk sistem Evolved Packet System (EPS) seperti yang digunakan saat ini. Keseluruhan sistemnya telah berbasis IP, membentuk koneksi IP *end-to-end*. Teknologi berbasis *packet-switching* ini memungkinkan LTE/SAE memiliki *data rate* yang jauh lebih tinggi dibandingkan pendahulunya, UMTS/3G.

Namun, sistem berbasis *all*-IP ini juga mengandung ancaman keamanan tersendiri. Sistem ini otomatis rentan terhadap serangan yang menyerang jaringan berbasis protokol IP lainnya seperti serangan *man-in-the-middle, spoofing, data tampering*, dan lain-lain. Operator telekomunikasi (Telco) sebagai pihak penyedia layanan dan infrastruktur perlu mengupayakan jaringan yang aman dengan membentengi jaringan dari berbagai ancaman keamanan yang muncul pada jaringan LTE/SAE.

Makalah ini memiliki tujuan sebagai berikut:

1. memberikan gambaran serangan berbasis IP pada jaringan LTE/SAE
2. mengidentifikasi *entry point* pada jaringan LTE/SAE
3. memberikan solusi keamanan generik pada jaringan LTE/SAE

Pada makalah ini, dijelaskan berbagai ancaman keamanan yang ada pada jaringan LTE. Dibahas titik-titik masuknya serangan (*entry point*) pada jaringan: dari *user equipment* (UE) atau *mobile station*, jaringan akses, *backhaul* dan *core*, serta jaringan eksternal atau pihak ketiga. Dilakukan pemetaan serangan yang mungkin terjadi pada jaringan LTE, kemudian dibahas metode penanganannya (*countermeasure*) secara garis besar. Terakhir, dibuat (berdasarkan referensi) solusi keamanan yang bersifat generik untuk mencegah dan menanggulangi timbulnya ancaman-ancaman keamanan yang telah dirumuskan sebelumnya.

2 Jaringan LTE/SAE

2.1 *Overview* Jaringan LTE/SAE

Long Term Evolution (LTE) atau 4G adalah teknologi jaringan akses seluler yang distandarkan oleh 3GPP Release 8. Teknologi ini merupakan suksesor teknologi UMTS atau 3G. LTE menawarkan *data rate* yang lebih tinggi dan *bandwidth* yang lebih lebar [1] dengan mengaplikasikan teknologi *multiplexing* pada lapisan fisik yang lebih efisien, yaitu Orthogonal Frequency Division Multiple Access (OFDMA). LTE menawarkan kecepatan hingga 300 Mbps bila menggunakan konfigurasi antenna *Multiple Input Multiple Output* (MIMO) [1]. LTE Release 8 adalah fase pertama teknologi LTE, yang kemudian dilanjutkan dengan LTE Advanced (LTE-A) dengan *throughput* yang lebih besar. System Architecture Evolution (SAE) adalah arsitektur *core network* untuk jaringan LTE.

Jaringan LTE/SAE, dirancang untuk mendukung konektivitas berbasis Internet Protocol (IP) dan kompatibel sepenuhnya dengan berbagai jenis teknologi akses *wireless* seperti WiFi dan WLAN [2]. Konektivitas berbasis IP

menerapkan konsep *flat architecture*. Konsep *flat architecture* bertujuan untuk mengurangi jumlah *node*, mendistribusikan *processing load* dengan lebih baik sehingga mengurangi latensi di jaringan [3, 4]. Hal ini berbeda dengan UMTS atau 3G di mana arsitekturnya bersifat hirarkis.

Fitur atau teknologi yang baru diperkenalkan di LTE adalah sebagai berikut [2]:

- mendukung konektivitas IP secara flat *(flat IP connectivity)*
- memiliki kompatibilitas penuh dengan teknologi *wireless* lainnya dan berbagai tipe *base station*, misalnya berbagai jenis *small cell (picocell, femtocell)*.

2.2 Arsitektur Jaringan LTE/SAE

LTE/SAE, yang disebut juga dengan Evolved Packet System (EPS), memiliki arsitektur seperti yang ditunjukkan pada Gambar 1. Fungsi LTE sebagai bagian jaringan akses direpresentasikan dengan Evolved Universal Terrestrial Radio Access Network (E-UTRAN). Fungsi SAE sebagai bagian *core network* direpresentasikan dengan Evolved Packet Core (EPC). Di antara keduanya adalah yang disebut dengan *backhaul*, yaitu hubugan antara E-UTRAN dengan EPC.

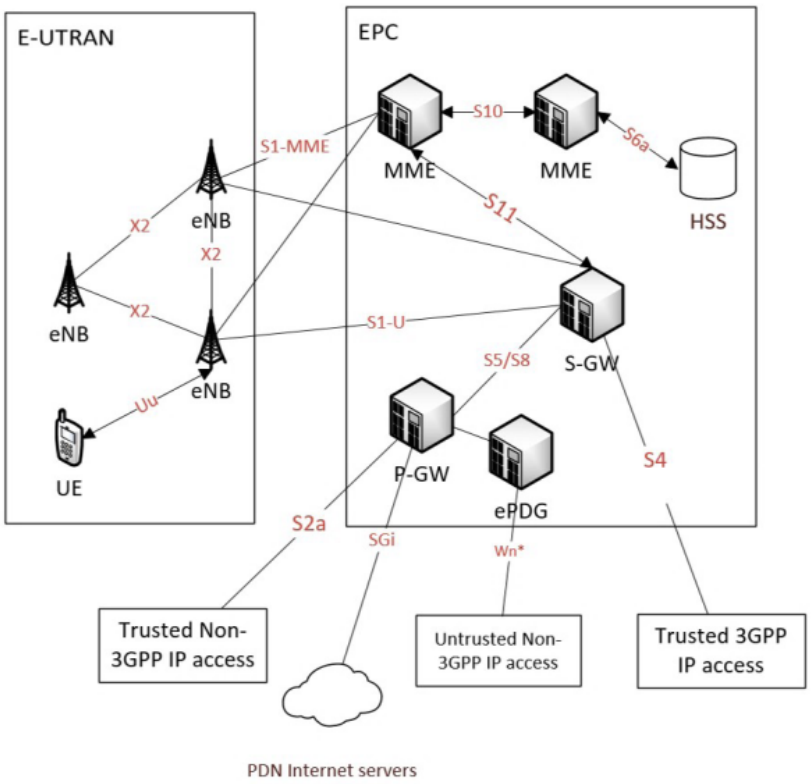
E-UTRAN terdiri dari sekumpulan *base station* yang disebut e-NodeB (selanjutnya disebut eNB saja). eNB bertanggungjawab dalam melakukan proses *signaling*, menerima dan meneruskan data *user*, dan mengatur *radio resource* [5]. Pada *control plane*, eNB terhubung ke satu atau lebih Mobility Management Entity (MME) yang berada di *core network* melalui *interface* S1-MME (disebut juga interface S1-C). Pada *user plane*, eNB terhubung ke Serving Gateway (S-GW) di *core network* melalui *interface* S1-U. eNB juga berkomunikasi dengan eNB lain melalui *interface* X2. Untuk melayani *mobile station* (untuk seterusnya disebut dengan *user equipment*, UE), eNB menggunakan *interface* Uu.

EPC memiliki entitas yang lebih banyak dibandingkan E-UTRAN, dengan setiap entitas memiliki tugasnya masing-masing. Entitas tersebut adalah sebagai berikut [6]:

1. Mobility Management Entity (MME): merupakan *node* kontrol utama pada LTE/SAE. MME berperan untuk melayani dan mengatur mobilitas UE pada mode *idle*. Suatu UE yang bergerak akan mengalami perpindahan *attachment* eNB (disebut dengan handover). Data mobilitas UE tersebut nantinya akan dicatat di MME. MME juga melakukan fungsi-fungsi yang berhubungan dengan *security*.

2. Packet Data Network Gateway (P-GW): merupakan titik bertemu antara EPC dengan jaringan berbasis paket *(packet-based network)* lainnya (misalnya internet) untuk mengalirkan informasi dari dan ke UE.

3. Serving Gateway (S-GW): berperan sebagai *local mobility anchor*, yaitu yang melayani mobilitas UE saat UE melakukan *handover*. S-GW juga bertugas melakukan *buffering* trafik pengguna saat *handover* sehingga data tersebut tidak perlu lagi diminta dari entitas luar EPC. Fungsi S-GW mirip dengan *data plane* SGSN pada jaringan 3G.



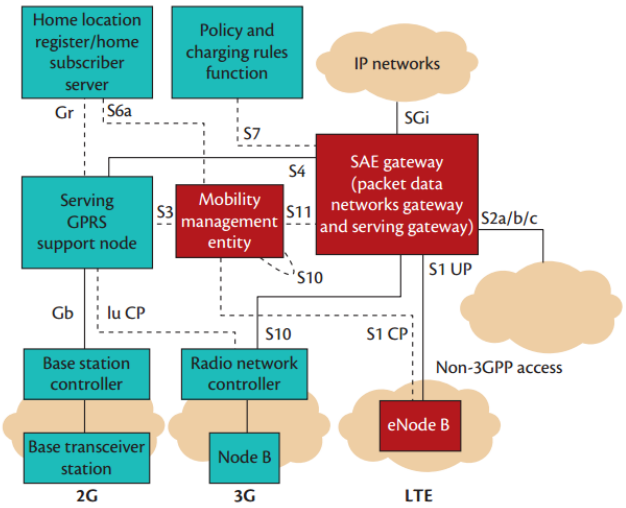
Gambar 1: Arsitektur Jaringan LTE/SAE [7].

4. Home Subscriber Server (HSS): merupakan *database* yang berisikan informasi *subscription user*, *home location* setiap user, dan parameter-parameter yang digunakan untuk proses otentikasi. *Home location* yang dimaksud bukanlah lokasi tempat tinggal, tetapi lokasi dicatatnya suatu user pertama kali. Bila *user* tidak sedang berada di home location, keadaan ini disebut dengan keadaan *roaming*.

5. Policy and Charging Rules Function (PCRF): berperan dalam hal kebijakan dan *billing* setiap *flow* yang masuk.

2.3 Perbedaan LTE/SAE dengan UMTS

Telah disebutkan bahwa jaringan LTE/SAE berbeda dengan UMTS salah satunya adalah dalam arsitektur jaringan yang lebih *flat*. Maksud *flat* di sini adalah bahwa pada jaringan LTE, komunikasi ditangani oleh lebih sedikit entitas bila dilihat secara vertikal. Pada Gambar 2, dapat dilihat bahwa pada UMTS / 3G, NodeB secara hirarkis berada di bawah Radio Network Controller (RNC). Bila UE bergerak, melakukan komunikasi dengan internet, dan sebagainya, langkah yang harus dilalui oleh UE adalah melalui NodeB, kemudian RNC, baru kemudian ke *core network*. Hal ini menyebabkan adanya tambahan latensi. Pada jaringan LTE di mana diharapkan *throughput* yang lebih tinggi dan latensi



Gambar 2: Perbedaan Arsitektur UMTS/3G dan LTE/4G [3].

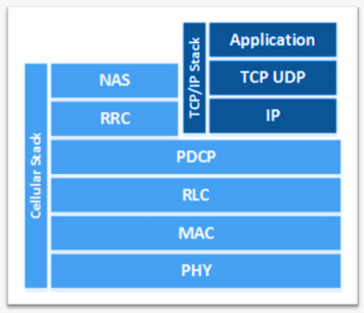
yang lebih rendah, fungsionalitas RNC banyak dipindahkan ke NodeB, menjadi eNB sehingga proses yang ditempuh UE dapat berjalan lebih cepat.

Pada dasarnya, arsitektur jaringan berbasis TCP/IP tidak sama dengan jaringan seluler. Keduanya memiliki lapisan *(layer)* yang berbeda. Sejak adanya layanan internet pada jaringan seluler, otomatis jaringan seluler menyediakan interkoneksi dengan jaringan berbasis TCP/IP. Pada jaringan LTE/SAE, sudah didukung *full IP connectivity*. Protocol stack TCP/IP di stack jaringan seluler ditunjukkan pada Gambar 3. Di lapisan bawah, terdapat *layer* Physical, MAC, RLC, dan PDCP. Lapisan IP berada di atas lapisan PDCP, yaitu "ditumpangkan" di lapisan RRC pada lapisan jaringan seluler.

Selain arsitektur, terdapat beberapa perbedaan antara UMTS dan LTE. Dalam hal mekanisme dan prosedur di jaringan, terdapat minimal dua hal yang patut diperhatikan, yaitu sebagai berikut:

1. Otentikasi
   Otentikasi pada jaringan LTE menggunakan EPS-*Authentication and Key Agreement* (EPS-AKA), sedangkan jaringan UMTS menggunakan UMTS-AKA. EPS-AKA memiliki fungsi serupa dengan UMTS-AKA, dengan beberapa perubahan, salah satunya mengganti mekanisme *cipher key* dan *integrity key* dengan sebuah *master key* [6].

2. Proses signaling
   Proses *signaling* pada 3G dan 2G menggunakan protokol yang disebut dengan SS7. Pada 4G, digunakan *Diameter signaling*. SS7 dianggap sangat sulit ditembus [8]. Sebaliknya, *diameter signaling* jauh lebih rentan disebabkan jaringan yang sepenuhnya berbasis IP.



Gambar 3: Posisi TCP/IP pada *Cellular Stack* [9].

2.4 Arsitektur Keamanan Jaringan LTE/SAE

3GPP pada dasarnya telah memberikan spesifikasi teknis tentang keamanan untuk jaringan LTE/SAE yaitu 3GPP TS 33.401 [9]. Di dalam TS33401 telah diatur mekanisme dan hal lain untuk mengamankan 4G, misalnya, akses ke E-UTRAN menggunakan SIM 2G tidak diperbolehkan, otentikasi yang lebih aman dibandingkan UMTS-AKA, dan lain-lain. Arsitektur keamanan tersebut, ditunjukkan pada Gambar 4, diantaranya membahas *security feature groups* [6] sebagai berikut:

1. *Network Access Security* (I): kumpulan fitur keamanan *(security features)* untuk membuat UE terlindungi dari serangan saat mengakses layanan di jaringan akses *(radio access link)*;

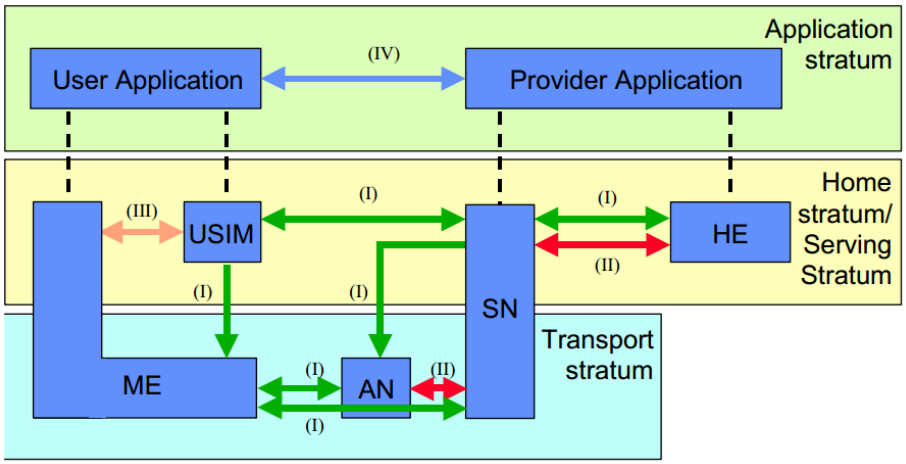
2. *Network Domain Security* (II): kumpulan fitur keamanan untuk membuat jaringan dengan kabel sebagai medium transmisi (pada backhaul, misalnya) dapat bertukar informasi *signaling* dan data pengguna dengan aman;

3. *User Domain Security* (III): kumpulan fitur keamanan untuk mengamankan akses ke UE;

4. *Application Domain Security* (IV): kumpulan fitur keamanan untuk membuat aplikasi di pengguna dan di penyedia layanan dapat bertukar informasi dengan aman. Prinsipnya mirip dengan *network access security*, namun untuk lapisan aplikasi;

5. *Visibility and Configurability of Security* (V): kumpulan fitur keamanan yang membuat UE dapat memberitahu dirinya sendiri tentang apakah sebuah fitur keamanan sedang beroperasi dan apakah *provisioning* layanan harus bergantung pada fitur keamanan.

Terdapat pula standar-standar lain yang menggunakan arsitektur keamanan jaringan yang berlapis *(layered network security architecture)* seperti Y-Comm dan X.805 *recommendations* [3]. Meskipun telah dilengkapi mekanisme keamanan yang lebih tinggi dibandingkan 3G, *nature* dari jaringan LTE yang telah memiliki fitur-fitur baru yang tidak ada sebelumnya tentu membuka peluang terjadinya berbagai jenis serangan yang dulunya tidak terjadi di bidang seluler.



Gambar 4: Arsitektur Keamanan Jaringan LTE/SAE [10].

3 Ancaman Keamanan pada Jaringan LTE/SAE

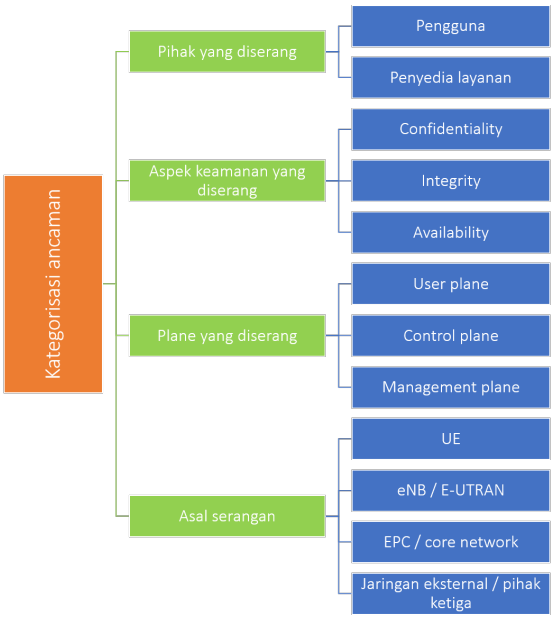
3.1 Serangan pada jaringan LTE/SAE

Menurut [7], kelemahan (*vulnerability*) pada *mobile network* dapat diartikan sebagai kelemahan yang melekat pada arsitektur dan komponen jaringan, yang dapat dimanfaatkan untuk melakukan serangan (*attack*). Ancaman *threat*, masih menurut [7], diartikan sebagai kemampuan sesuatu atau seseorang untuk dengan sengaja melakukan hal-hal yang berakibat pada satu atau lebih hasil berikut ini:

1. mengakses informasi secara tidak sah;
2. memanipulasi informasi;
3. menyebabkan suatu sistem tidak dapat diandalkan atau tidak dapat digunakan.

Terdapat berbagai macam ancaman keamanan yang dapat terjadi pada suatu sistem, termasuk pada jaringan LTE/SAE. Untuk mempermudah melihat persoalan, dilakukan kategorisasi atau pengelompokan jenis-jenis ancaman. Tidak ada aturan khusus tentang tata cara pengelompokan. Penulis menemukan perbedaan cara pengelompokan pada [7, 11, 2, 12] dan lain-lain sehingga dibuat kategorisasi ancaman dengan mengombinasikan kategori pada *paper-paper* referensi tersebut. Kategorisasi ancaman yang digunakan pada makalah ini ditunjukkan pada Gambar 5.

1. Pihak yang diserang
   Dilihat dari pihak yang diserang, ancaman keamanan dapat dikelompokkan sebagai berikut:
   (a) Ancaman terhadap pengguna
   Serangan terhadap pengguna umumnya adalah bertujuan untuk mengetahui informasi pribadi seseorang. Contoh serangan ini dapat dila-



Gambar 5: Kategorisasi Serangan pada Jaringan LTE/SAE

.

kukan melalui penyadapan saat pengguna sedang berselancar di internet. Untuk melakukan serangan ini, biasanya tidak diperlukan kemampuan yang terlalu "canggih". Dengan menggunakan *network sniffer* biasa seperti Wireshark dan Cain and Abel, data pelanggan sudah bisa diperoleh.

Pada jaringan LTE/SAE, terdapat enkripsi dan pertukaran kunci *(key exchange)* antara UE dengan eNB sehingga komunikasi relatif lebih aman. Namun, serangan tetap dapat terjadi. Jaringan akses pada sistem LTE/SAE, tidak seperti UMTS, tidak hanya terdiri dari *base station* "besar", tetapi juga memiliki *base station* kecil yang dikenal dengan nama *small cell* (berupa *picocell* atau *femtocell*) yang dapat dipasang di dalam ruangan, misalnya di mal dan gedung perkantoran. Hal ini disebabkan penerimaan sinyal LTE jauh lebih kecil dibandingkan UMTS (*coverage* lebih kecil karena mengedepankan *throughput*). Serangan dapat dilakukan dengan berpura-pura menjadi *small cell* (disebut *rogue base station*) dengan sinyal yang kuat sehingga memaksa UE untuk terkoneksi kepadanya [11]. Meskipun terdapat proses otentikasi antara UE dan eNB, menurut [13], otentikasi tersebut tidak bersifat *mutual*, melainkan hanya eNB yang mengotentikasi UE. Hal ini menyebabkan *rogue base station* dapat mengambil informasi seperti daftar panggilan yang dilakukan UE, dan lain-lain.

(b) Ancaman terhadap penyedia layanan
Serangan terhadap operator telekomunikasi (Telco) sebagai penyedia layanan umumnya memiliki tujuan dengan dampak yang lebih luas

dengan artian lebih banyak pihak yang dirugikan, misalnya dengan menurunnya performansi jaringan di suatu region, atau untuk menjatuhkan operator itu sendiri. Tujuan kedua dapat dilakukan tanpa memasuki sistem seluler operator tersebut, seperti yang terjadi baru-baru ini di mana penyerang melakukan *deface* website Telkomsel yang terjadi pada 28 April 2018 [14].

Pada jaringan LTE/SAE sendiri, serangan juga dapat dilakukan dari UE maupun *rogue base station*. DDoS Attack dapat dilakukan menggunakan sejumlah besar UE yang terkontaminasi sehingga berperan sebagai *botnet*, seperti yang disimulasikan pada [15]. Penyerang juga dapat menggunakan *rogue base station*. Setelah mendapatkan identitas pengguna melalui *rogue base station*, penyerang dapat berpura-pura menjadi UE yang valid [11], kemudian melakukan serangan lebih lanjut untuk dapat masuk ke dalam EPC.

2. Aspek keamanan yang diserang
   Dilihat dari aspek keamanan yang diserang, secara umum ancaman keamanan dapat dikelompokkan sebagai berikut:

   (a) Ancaman terhadap kerahasiaan (confidentiality)
   Kerahasiaan (confidentiality) adalah mempertahankan kerahasiaan informasi pengguna dengan mencegah diaksesnya informasi oleh pihak yang tidak berwenang [11]. Serangan pada aspek ini biasanya tidak sampai mengganggu operasional, dalam artian tidak akan terlihat penurunan performansi di jaringan. Serangan terhadap kerahasiaan dapat ditargetkan kepada pengguna maupun operator telekomunikasi (Telco) sebagai penyedia layanan. Serangan terhadap pengguna biasanya tidak berdampak secara luas dalam artian tidak banyak pihak yang dirugikan, contohnya adalah dengan melakukan penyadapan *(eavesdropping)*. Meskipun begitu, operator memiliki kewajiban untuk melindungi data pribadi pelanggannya sehingga serangan semacam ini juga harus dilakukan pencegahan dan penanganannya oleh pihak operator. Serangan terhadap operator dapat terjadi, misalnya, dengan melakukan infiltrasi ke dalam HSS *(Home Subscriber Server)* yang berisi data pelanggan, kemudian membocorkannya sehingga menjatuhkan kredibilitas operator. Salah satu cara mencegah serangan terhadap aspek *confidentiality* pada jaringan LTE/SAE adalah dengan menggunakan algoritma kriptografi seperti SNOW 3G, AES, dan ZUC [9].

   (b) Ancaman terhadap availabilitas (availability)
   Availabilitas *(availability)* dalam jaringan LTE/SAE mengacu pada artian bahwa komunikasi seluler menggunakan jaringan LTE harus selalu tersedia untuk *legitimate user* di setiap saat [11]. Serangan pada aspek ini bertujuan menyebabkan *service disruption* dan sudah pasti mengganggu operasional jaringan, bahkan dapat menjadikan sistem *down*. Serangan ini dikenal dengan sebutan Denial of Service Attack (DoS Attack). Bila target serangan adalah pengguna secara spesifik, *rogue base station* dapat digunakan untuk mengambil alih koneksi UE untuk kemudian memutusnya dari jaringan. Bila targetnya adalah operator, Distributed Denial of Service Attack (DoS

Attack) dapat dilakukan melalui UE yang telah di-*compromise*. UE dapat mengirimkan *request* terus-menerus ke jaringan untuk menghabiskan *resource* pada eNB, menghasilkan penurunan performansi dan lebih sedikit *legitimate* UE yang dapat dilayani.

(c) Ancaman terhadap integritas data (integrity)
Integritas *(integrity)* adalah melindungi data pengguna dari modifikasi, penghapusan, dan/atau injeksi [11]. Serangan pada aspek ini dilakukan dengan mengintersepsi trafik tanpa sepengetahuan pengirim maupun penerima, melakukan sesuatu terhadap data (modifikasi, menghapus, dan lain-lain) sesuai kepentingan penyerang, kemudian dikirim ke tujuan sebenarnya. Pengirim dan penerima tidak menyadari hal ini dan mengira bahwa komunikasi memang dilakukan antara dua pihak yang sah. Serangan seperti ini dikenal dengan istilah *Man-in-the-Middle Attack* (MitM Attack). Jenis serangan ini pada jaringan LTE/SAE kurang populer dibandingkan dengan kedua serangan lainnya.

Selain ketiga aspek yang telah dijelaskan, terdapat 2 kategori aspek lain yang dijabarkan pada [7], yaitu ancaman terhadap kontrol dan pencurian layanan *(theft of service)*. Ancaman terhadap kontrol meliputi dua hal: komponen jaringan yang berhasil diretas *(compromised network element)* dan orang dalam yang memiliki niat jahat *(malicious insider)*. Pencurian layanan adalah adalah menggunakan layanan tanpa membayar sesuai dengan ketentuan, misalnya dengan membeli kuota internet dari orang dalam tanpa seizin atau tidak sesuai dengan ketentuan operator.

3. *Plane* yang diserang
Komunikasi pada jaringan LTE dapat dikelompokkan ke dalam 3 buah *plane*: *user plane, control plane,* dan *management plane* [10]. Ketiga *plane* merupakan pemisahan secara *logical*. Pada kenyataannya, jalur komunikasi ketiga plane tersebut bisa jadi melewati komponen-komponen yang sama. Masing-masing plane pun memiliki ancaman keamanan, sehingga dapat dikelompokkan ancaman keamanan menurut *plane* yang diserang sebagai berikut:

   (a) *User Plane*
   User plane adalah bidang atau jalur mengalirnya data yang memang di-*request* oleh *user*. Dalam dunia *computer networking*, *user plane* juga sering disebut dengan *data plane*.

   (b) *Control Plane*
   Control plane adalah bidang atau jalur tempat mengalirnya proses-proses *signaling* yang bertujuan mengatur dan menjamin terbentuknya jalur komunikasi di *user plane*.

   (c) *Management Plane*
   Management plane adalah *plane* tertinggi dibandingkan dua *plane* lainnya. *Plane* ini melihat jaringan secara *high level* untuk memastikan dapat terjadinya komunikasi pada *plane* di bawahnya. Contoh proses pada *management plane* adalah trafik *setup* dan konfigurasi eNB.

4. Asal serangan
   Pada umumnya, serangan dapat terjadi atau masuk melalui titik-titik terluar dari sebuah sistem. Setelah berhasil masuk melalui titik-titik terluar tersebut, serangan dapat ditujukan ke berbagai entitas di dalam sistem dengan lebih mudah. Selain itu, serangan juga dapat terjadi dari dalam sistem itu sendiri, misalnya oleh orang dalam (sering disebut dengan *insider* atau *disgruntled employee*) dengan memanfaatkan hak akses yang ia miliki. Titik-titik tempat masuknya serangan tersebut dikenal dengan istilah *entry point*. Secara lebih spesifik, dilakukan perincian *entry point* pada [7] dan [11] pada jaringan LTE/SAE menjadi 4 titik, yaitu sebagai berikut:

   (a) UE
   UE adalah salah satu *entry point* termudah untuk melakukan penyerangan. Tidak seperti operator sebagai perusahaan yang umumnya menerapkan standar minimal keamanan, UE yang dimiliki pengguna dapat bersentuhan dengan berbagai jenis lingkungan tanpa perlindungan yang cukup. UE dapat dengan mudah terkena *malware* seperti Trojan [15] pada sangat mengunduh file atau aplikasi dari internet, kemudian dapat dikontrol agar bertindak sebagai *botnet* yang dapat menghabiskan *resource* di jaringan.

   (b) Jaringan akses (E-UTRAN)
   eNB sebagai komponen terluar dari pihak operator menjadi yang bersentuhan langsung dengan UE di pengguna. Seperti yang ditunjukkan pada Gambar 1, eNB terhubung ke *core network* melalui *interface* S1-MME untuk fungsi kontrol dan S1-U untuk *user plane*. Terdapat kelemahan dalam hal interoperasi antara LTE dengan teknologi di bawahnya, yaitu UMTS dan GSM. Kelemahan ini dapat digunakan untuk masuk ke jaringan akses, kemudian mengincar MME di *core network*.

   (c) *Backhaul* dan *core* (EPC)
   Berbeda dengan jaringan akses yang memiliki medium transmisi berupa radio, *backhaul* dan *core network* umumnya menggunakan kabel untuk koneksinya. *Entry point* ini lebih sulit ditembus, namun tetap memiliki kelemahan yang dapat dieksploitasi [2]. Menurut [11], *femtocell* yang gagal melakukan otentikasi setelah beberapa kali, akan mengontak OAM server yang ada di *core network* tanpa menggunakan otentikasi.

   (d) Jaringan eksternal / pihak ketiga
   Jaringan eksternal / pihak ketiga yang dimaksud adalah jaringan di bawah LTE, yaitu UMTS dan GSM (3GPP), jaringan akses non-3GPP seperti WiFi, dan IMS seperti internet. Interkoneksi antara ketiganya mengutamakan kompatibilitas sehingga beberapa fungsi pengamanan yang ada di jaringan *full* LTE tidak digunakan di sini.

Jaringan LTE/SAE tidak lepas dari kelemahan yang dapat dimanfaatkan untuk melancarkan serangan. Serangan yang dapat terjadi secara spesifik pada jaringan LTE/SAE, disebabkan oleh sifatnya yang berbasis IP, di antaranya adalah sebagai berikut [7]:

1. *IP-based attack* pada *backhaul*
   Serangan pada *backhaul* dapat terjadi karena backhaul terdiri dari elemen kontrol dan *interface* berbasis IP. *Interface* pada *backhaul* yaitu S1 dan X2 menjadi tempat yang rawan terjadi serangan [11]. Serangan berbasis IP yang mungkin terjadi, disebutkan pada [7], adalah sebagai berikut:

   - *spoofing attack* di eNB;
   - *eavesdropping* terhadap trafik pengguna;
   - *unauthorized access attack*;
   - *flooding attack*, misalnya dengan TCP-SYN atau TCP-reset attack

2. *GTP-based attack*
   GPRS Tunneling Protocol (GTP) adalah protokol untuk melakukan transfer data, melakukan *assign* IP *address*, dan mengatur *resource* jaringan. GTP adalah protokol yang berbasis UDP, yaitu bersifat *connectionless* sehingga tidak membutuhkan *acknowledgement* dari penerima. Serangan-serangan yang dapat terjadi terkait GTP adalah sebagai berikut:

   - *GTP scanning attack*: serangan dengan mengirimkan paket *echo* secara terus menerus untuk melakukan scanning pada komponen-komponen yang ada di jaringan, mirip seperti melakukan *port scanning* pada suatu jaringan. Serangan ini dapat mengungkap identitas komponen jaringan.
   - *Create Session Request attack*: serangan dengan mengirimkan message *create session request* secara terus menerus. Seperti halnya *flooding attack*, serangan ini menyebabkan eNB harus mengalokasikan banyak *resource* untuk penyerang, baik dari sisi komputasi maupun resource lain seperti IP address. *Exhaustion* akan menyebabkan pengguna valid tidak terlayani.
   - *Abnormal GTP packet attack*: serangan dari jaringan 3G maupun jaringan non-3GPP (WiFi, WLAN, WiMAX) dengan mengirimkan paket yang tidak normal. Serangan ini dapat menyebabkan malfungsi pada komponen yang berkaitan dengan GTP.
   - *Voice phishing attack*: serangan ini dapat dilakukan dengan melakukan modifikasi alias *tampering* pada protokol SIP.

3. *VoLTE-based attack*
   VoLTE adalah layanan Voice-over-IP (VoIP) pada jaringan LTE/SAE [16]. VoLTE menggunakan protokol Session Initiation Protocol (SIP) pada *control plane*. Menurut [16], VoLTE memiliki celah keamanan pada bagian *access* dan *session control*. Kelemahan ini dapat di-*abuse* untuk membawa paket berupa data, tidak hanya paket *voice signaling*. Hal ini dapat dimanfaatkan untuk melakukan serangan berikut:

   - *information exposure*: *access control* masih memiliki kelemahan. *Interface* VoLTE yang diimplementasikan saat ini belum di-*harden* terhadap akses *non-authorized*. Penyerang dapat memperoleh informasi pengguna dari interface VoLTE.

- *message forgery*, *message tampering*: setelah masuk ke jaringan, penyerang dapat mengubah, memodifikasi, dan menginjeksi data sesuai kebutuhan.
- *SIP flooding* untuk DoS Attack: protokol SIP yang digunakan untuk proses *signaling* juga dapat dimanfaatkan untuk melakukan DoS Attack.

4. Diameter-based attack
   Diameter adalah protokol *Authorization, Authentication* dan *Accounting* (AAA) untuk bertukar informasi pelanggan untuk keperluan *billing*, QoS, dan lain-lain antara entitas di dalam EPC [8]. Diameter *signaling* menggunakan TCP atau SCTP sebagai protokol pada lapisan transport. Kelemahannya adalah ketiadaan mekanisme proteksi *end-to-end* bila terjadi *congestion* di jaringan. Hal ini dapat dilakukan penyerang untuk melakukan serangan, di antaranya sebagai berikut:

   - *diameter-injected signaling flood*
   - *message forgery*

   Masih terdapat berbagai serangan yang dapat terjadi pada jaringan LTE/SAE, namun pada [7] tidak dikategorikan sebagai serangan berbasis IP.

Daftar serangan berbasis IP yang dibahas pada [7] adalah sebagai berikut:

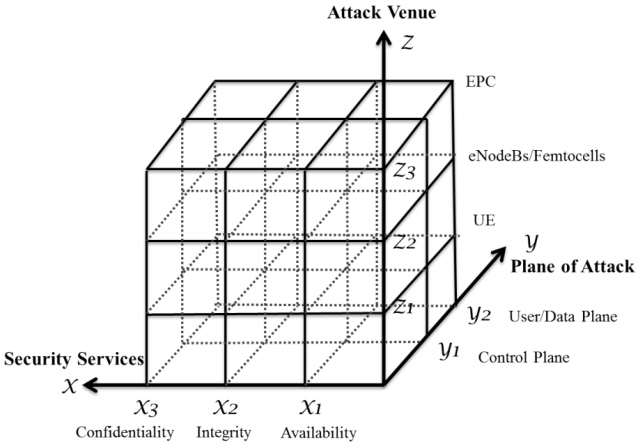
3.2 Pemetaan serangan pada jaringan LTE/SAE

Pada [11], dijelaskan salah satu model pemetaan serangan yang dinamakan *threat space*. *Threat space*, ditunjukkan pada Gambar 6, mengategorisasikan serangan-serangan dalam bentuk 3 dimensi. Ketiga dimensi yang diajukan pada paper tersebut adalah sebagai berikut:

- *Communication security services*, yaitu layanan keamanan apa yang diserang. Dimensi ini memiliki tiga buah komponen: *confidentiality, integrity,* dan *availability*.
- *Plane of attack*, yaitu di *plane* mana serangan dapat terjadi. Dimensi ini memiliki dua buah komponen: *user plane* dan *control plane*.
- *Attack venue*, yaitu di entitas mana serangan dapat terjadi. Dimensi ini memiliki tiga buah komponen: EPC, eNB atau *femtocell*, dan UE.

Model *threat space* yang diajukan tersebut sebenarnya tidak jauh berbeda dengan kategorisasi ancaman keamanan yang telah dibahas pada Bab 3.2. *Communication security services* berpadanan dengan aspek keamanan yang diserang, *plane of attack* berpadanan dengan *entry point*. *Plane of attack* sama dengan yang dibahas pada Bab 3.2, namun *management plane* tidak dibahas pada model *threat space*.

Kelebihan model *threat space* adalah ancaman-ancaman yang ada dapat divisualisasikan dengan lebih baik dan dapat diambil kesimpulan serta mitigasi secara generik atau *high level* dari berbagai serangan yang ada. Model ini juga dapat diperluas sesuai dengan kebutuhan, misalnya ditambahkan *management*



Gambar 6: Model *Threat Space* pada [11].

plane pada sumbu *plane of attack* dan *theft of service* pada sumbu *security services*.

Kekurangan model ini adalah bila ingin menambah dimensi, misalnya menjadi 4 dimensi, akan menjadi sulit untuk divisualisasikan. Oleh karena itu, model *threat space* hanya dijadikan acuan untuk melakukan pengelompokan, namun tidak ditunjukkan pada makalah ini dikarenakan keterbatasan visualisasi. Serangan-serangan berbasis IP pada jaringan LTE yang dibahas sebelumnya dapat dikelompokkan menjadi seperti yang ditunjukkan pada tabel 1.

4 Metode Pengamanan pada Jaringan LTE/SAE

4.1 Solusi Pengamanan Per Kasus

Terdapat berbagai *paper* yang membahas kelemahan dan serangan yang masih mungkin terjadi pada jaringan LTE. Beberapa memberikan solusi spesifik per kasus. Berikut *overview* solusi yang ditawarkan terhadap serangan pada Bab 3.1:

1. *IP-based attack* pada *backhaul*
   Solusi yang ditawarkan oleh [17] untuk menanggulangi serangan berbasis IP pada *backhaul* adalah dengan menggunakan IPSec, yaitu framework keamanan di lapisan 3 model OSI. Komunikasi pada *backhaul* diajukan melalui tunnel VPN untuk melindungi dari serangan. Diajukan 2 buah solusi berbasis IPSec: menggunakan L3 VPN dengan protokol IKEv2 yang telah dimodifikasi untuk memberi pengamanan dari DoS Attack; dan menggunakan L3 VPN dengan protokol HIP yang telah dimodifikasi untuk memberi pengamanan dari *spoofing attack*.

2. *GTP-based attack*
   Solusi yang ditawarkan oleh [18] adalah lebih kepada melakukan deteksi dengan monitoring. Dilakukan proses *capture* trafik pada jaringan 4G, baik trafik kontrol maupun data. Bila telah dimiliki data trafik *baseline*,

Tabel 1: Pemetaan Serangan Berbasis IP pada Jaringan LTE/SAE (diolah oleh penulis dari [7, 11]

No		Serangan	Aspek	Plane	Asal Serangan	Target
1	Backhaul	TCP SYN/RESET Packet Flooding Attack	Availability	CP	eNB	operator
2		TCP RESET Attack	Availability	CP	eNB	operator
3	GTP Attack	Packet Tampering	Integrity	UP	eNB, EPC	pengguna
4		GTP Scanning Attack	Confidentiality	CP, UP	eNB, EPC	pengguna
5		Abnormal GTP Message	Availability	CP	eNB, EPC	pengguna, operator
6	VoLTE Attack	Network Scanning	Confidentiality	CP	UE, eNB	operator
7		Resource Exhaustion Attacks	Availability	UP	UE, eNB	operator
8		Packet Forgery	Integrity	UP	eNB, EPC	pengguna
9		Packet Tampering	Integrity	UP	eNB, EPC	pengguna
10		SIP Flooding	Availability	CP	eNB	operator
11		VoLTE Signaling Bearer Data Injection Attacks	Availability	CP, UP	eNB, EPC	operator
12		VoLTE Signaling Bearer Qos Abuse Attacks	Theft of Service	CP, UP	eNB, EPC	operator
13		Call Spoofing	Integrity	CP, UP	eNB	pengguna
14		Sending Data Over A VoLTE Bearer	Theft of Service	CP	eNB, EPC	operator
15		eNB Spoofing	Integrity	CP	eNB	pengguna, operator
16		Eavesdropping User Traffic	Confidentiality	UP	eNB, EPC	pengguna
17		Unauthorized Access To Network Equipment	Confidentiality	UP	eNB, EPC	operator
18	Diameter Attack	Diameter Interface Congestion Attack	Availability	CP	UE, eNB	operator
19		Diameter Dos Attack	Availability	CP	UE	operator

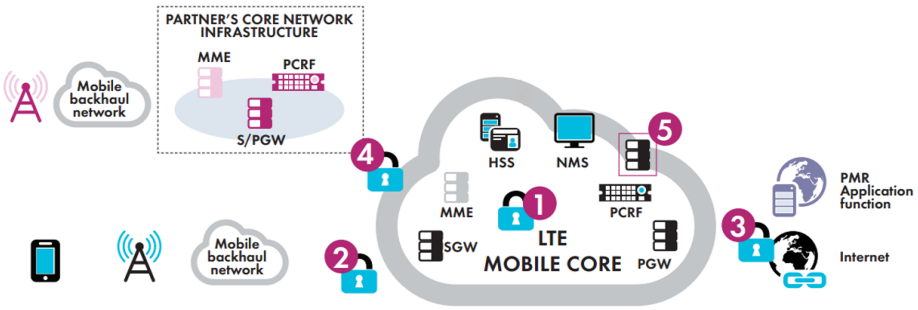
yaitu pola umum trafik pada jaringan (dengan mengambil data hasil *monitoring* sehari-hari), dapat dilakukan deteksi pola trafik yang abnormal sehingga dapat segera ditindaklanjuti sesuai dengan kebutuhan, misalnya men-*drop* paket abnormal, atau meneruskannya untuk diteliti lebih lanjut. Selain itu, sistem pendeteksi intrusi (Intrusion Prevention System, IPS) juga dapat digunakan untuk mencegah paket GTP yang abnormal untuk ikut dirutekan.

3. *VoLTE-based attack*
   Solusi yang ditawarkan pada [12] adalah dengan melakukan *session control management* dan menggunakan sistem deteksi untuk trafik VoLTE dengan pendekatan *flow-based*. Selain itu, diajukan pemanfaatan penggunaan *digital certificate* untuk melakukan pencegahan trafik yang tidak sesuai atau *malicious*. IPS kemudian digunakan dengan mengacu pada *signature* di *digital certificate*. Penggunaan mekanisme *deep packet inspection* (DPI) juga disarankan oleh [19] di P-GW karena P-GW adalah *entry point* yang bersentuhan dengan jaringan non-LTE. Mirip dengan [12], diajukan pula *session management* dengan aturan yang lebih ketat.

4. *Diameter-based attack*
   Solusi yang ditawarkan pada [20] adalah dengan menambahkan enkripsi untuk trafik diameter signaling dan melakukan deteksi anomali. *Explicit COngestion Notification* (ECN) juga diajukan pada [8] untuk mitigasi pada DoS Attack yang membuat terjadi *congestion* pada *interface* yang digunakan untuk *diameter signaling*.

Berdasarkan *overview* solusi yang ditawarkan pada beberapa *paper*, dapat diamati beberapa mekanisme atau solusi generik sebagai berikut:

- mekanisme deteksi paket dengan IDS dan lain-lain;



Gambar 7: *Security Enforcement Points* pada Jaringan LTE/SAE [21].

- mekanisme pencegahan lewatnya paket abnormal atau *malicious* dengan IPS dan lain-lain;
- penggunaan tunnel dan /atau enkripsi pada jaringan komunikasi.

4.2 *Security Enforcement Points*

Menurut [21], metode pengamanan yang paling tepat adalah dengan menerapkan *security by design*. Desain haruslah *secure* sedari awal, bukan hanya dengan menambal atau mencari *countermeasure* untuk setiap masalah yang ditemukan. Hal ini dilakukan dengan mengidentifikasi kemungkinan-kemungkinan tempat serangan berasal, kemudian membuat solusi generik untuk mengurangi kemungkinan timbulnya masalah tersebut atau dapat mendeteksi masalah dengan cepat sehingga penanggulangan masalah dapat dilakukan dengan cepat pula.

Entry point, sesuai yang dikemukakan pada 3, adalah tempat masuknya serangan ke dalam sistem. Oleh karena itu, *entry point* tersebut-lah yang harus diperkuat. *Security enforcement points* sebagaimana yang ditunjukkan pada Gambar 7 menunjukkan titik-titik atau *entry point* yang harus diperkuat. Selain itu, termasuk di dalam *security enforcement point* adalah proses *monitoring* dan *logging*. Kemudian, dibuat objektif yang harus dapat dipenuhi di setiap titik. Tujuan tersebut dapat digunakan untuk merinci fungsi-fungsi yang dibutuhkan, yang kemudian akan dilaksanakan oleh perangkat jaringan. Terdapat 4 buah *security enforcement point* yang didefinisikan pada [21], yaitu:

1. *secured hosting platform*
2. *secured interface to external networks*
3. *secured interfaces to roaming partners*
4. *security mediation (log management and monitoring)*

Penjelasan tiap-tiap *enforcement point* adalah sebagai berikut:

1. *Secured hosting platform LTE hosting platform* adalah tempat terletak elemen-elemen inti yang menangani layanan LTE [21], yaitu EPC itu sendiri. Elemen-elemen tersebut terlibat dalam *logical plane* yang berbeda-beda, sesuai pada Bab 3. Objektif yang perlu dilakukan dipenuhi untuk menjadikan sistem aman adalah sebagai berikut:

- meminimasi paparan dengan jaringan eksternal;
- mengimplementasikan prinsip *defence-in-depth*, yaitu segmentasi antara trafik control plane dan management plane;
- melindungi informasi sensitif
- segregasi yang jelas antarplane dengan menggunakan perangkat jaringan yang *dedicated* (boleh secara fisik atau logical), harus dibedakan jaringan untuk ketiga *plane* tersebut.

2. *Secured interface to external networks*

   - meminimasi paparan dengan jaringan eksternal
     Interkoneksi ke jaringan 3GPP maupun non-3GPP lain haruslah dibatasi, misalnya hanya dari beberapa interface tertentu yang bersifat sebagai *trunk*. Control plane dihubungkan ke jaringan luar melalui interface S6a/S9 dengan protokol SCTP. User plane dihubungkan ke jaringan luar melalui interface S8 dengan protokol GPRS Tunneling Protocol (GTP-U). Karena merupakan "warisan" dari teknologi sebelumnya, memiliki celah keamanan karena memang tidak didesain dengan fungsi keamanan, mirip dengan GRE Tunnel yang juga tidak dilengkapi dengan fitur keamanan. Harus dilakukan inspeksi terhadap paket GTP yang malformed atau forged sebelum diproses oleh gateway.
   - melakukan stateful filtering untuk session control dan untuk mencegah masuknya trafik malicious.

3. *Secured interfaces to roaming partners*
   Roaming partner adalah jaringan milik operator lain. Hal yang dapat dilakukan untuk mengamankan salah satunya dengan melakukan inspeksi SCTP stream untuk mengamati trafik mencurigakan.

4. *Security mediation (log management* dan *monitoring)*
   Security mediation yaitu melakukan *log management* dan *monitoring* pada jaringan. Dari hasil *monitoring*, dapat diperoleh informasi berharga terkait trafik normal pada umumnya dan trafik abnormal sehingga dapat dilakukan deteksi dini serangan maupun evaluasi terhadap serangan yang pernah terjadi.

Penguatan yang perlu diberikan di *security enforcement point* dijelaskan pada [12], disebut sebagai *framework* untuk *4G Mobile Network Threats Countermeasure* sebagai berikut:

- Sistem 4G *Mobile Network Control/Data Traffic Capturing*
  Sistem ini bertugas melakukan *traffic capturing*, baik untuk trafik data maupun trafik kontrol. Proses *capture* dilakukan di interface S11 dan S1-U sebagai *interface* yang terhubung dengan jaringan luar. Data ini lah yang kemudian akan digunakan untuk menganalisis dan menjadi patokan perbedaan trafik normal dan abnormal untuk setiap *user session*.

- Sistem 4G *Mobile Network Attack/Abnormal Traffic Detection System*
  Sistem ini berfungsi mendeteksi trafik abnormal. Input sistem ini adalah hasil *capture* pada poin sebelumnya.

- Sistem 4G *Mobile Network Intrusion Prevention System*
  Sistem ini berfungsi mem-*block* trafik *malicious* berdasarkan *output* dari sistem pada poin sebelumnya.

- Sistem 4G *Mobile Network Security Monitoring and Control System*
  Sistem ini berfungsi seperti *logger* pada umumnya. Data hasil deteksi, pencegahan, dan sebagainya dikumpulkan dan diolah sedemikian rupa sehingga diperoleh gambaran trafik yang ada pada jaringan.

4.3 Resume Metode Pengamanan Jaringan LTE/SAE dari Serangan Berbasis IP

Berdasarkan solusi generik yang dirangkum dan *framework* yang dibahas pada [12], dapat diamati bahwa penangan yang diajukan cukup bersesuaian. Seperti laiknya sistem berbasis IP lainnya, metode pengamanan yang diajukan juga serupa dengan jaringan berbasis IP pada umumnya. Sistem atau *Tools* yang diperlukan adalah sebagai berikut:

- Adanya sistem yang melakukan proses *capturing*
- Adanya sistem Intrusion Detection System (IDS)
- Adanya sistem Intrusion Prevention System (IPS)
- Adanya sistem *log* dan *monitoring*
- Melakukan pengamanan trafik dengan berbagai metode pada *framework* IPSec.

Fungsi-fungsi yang dilakukan oleh sistem tersebut, bila *cost* tidak menjadi masalah, sebaiknya ditempatkan di setiap *entry point*, kecuali di UE karena tidak memungkinkan. Bila *cost* menjadi kendala, fungsi tersebut dapat ditempatkan di *interface* S1,S11, dan X2 karena ketiga *interface* lah yang paling terpapar dengan jaringan eksternal dari *core network*.

5 Kesimpulan

Berdasarkan bahasan pada bab sebelumnya, diperoleh kesimpulan sebagai berikut:

1. Serangan berbasis IP pada jaringan LTE/SAE diantaranya adalah:
   - Serangan terhadap Backhaul
   - VoLTE-based Attack
   - GTP-based Attack
   - Diameter-based Attack
2. Entry point pada jaringan LTE/SAE adalah *interface* pada:
   - *User Equipment* (UE)
   - *evolved Node-B* (eNB), yaitu *interface* X2
   - *Evolved Packet Core* (EPC), yaitu S1 dan S11
   - Jaringan eksternal (3GPP dan non-3GPP)
3. Solusi keamanan generik pada jaringan LTE/SAE adalah:
   - Adanya sistem yang melakukan proses *capturing*
   - Adanya sistem Intrusion Detection System (IDS)
   - Adanya sistem Intrusion Prevention System (IPS)
   - Adanya sistem *log* dan *monitoring*
   - Melakukan pengamanan trafik dengan metode pada *framework* IPSec.

Pustaka

[1] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of lte networks against jamming attacks," *EURASIP Journal on Information Security*, vol. 2014, no. 1, p. 7, 2014.

[2] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for lte and lte-a networks," *IEEE Communications Surveys Tutorials*, vol. 16, pp. 283–302, First 2014.

[3] A. N. Bikos and N. Sklavos, "Lte/sae security issues on 4g wireless networks," *IEEE Security & Privacy*, vol. 11, no. 2, pp. 55–62, 2013.

[4] C. K. Han and H. K. Choi, "Security analysis of handover key management in 4g lte/sae networks," *IEEE Transactions on Mobile Computing*, vol. 13, pp. 457–468, Feb 2014.

[5] Q. Xiao, W. Zhou, B. Cui, and L. Li, "An enhancement for key management in lte/sae x2 handover based on ciphering key parameters," in *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, pp. 256–261, Nov 2014.

[6] M. Abdeljebbar and R. Elkouch, "Security analysis of lte/sae networks over e-utran," in *2016 International Conference on Information Technology for Organizations Development (IT4OD)*, pp. 1–5, March 2016.

[7] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, 2016.

[8] J. Henrydoss and T. Boult, "Critical security review and study of ddos attacks on lte mobile network," in *Wireless and Mobile, 2014 IEEE Asia Pacific Conference on*, pp. 194–200, IEEE, 2014.

[9] NIST, "LTE Security – How Good Is It?." `http://csrc.nist.gov/news_events/cif_2015/research/day2_research_200-250.pdf`. [Online; retrieved 4-March-2017].

[10] D. Zhang, "3gpp ts 33.401 v12. 5.0 3gpp system architecture evolution (sae); security architecture," 2012.

[11] S. Bhattarai, S. Rook, L. Ge, S. Wei, W. Yu, and X. Fu, "On simulation studies of cyber attacks against lte networks," in *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, pp. 1–8, Aug 2014.

[12] S. Park, S. Kim, J. Oh, M. Noh, and C. Im, "Threats and countermeasures on a 4g mobile network," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2014 Eighth International Conference on*, pp. 538–541, IEEE, 2014.

[13] T. Wu and G. Gong, "The weakness of integrity protection for lte," in *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pp. 79–88, ACM, 2013.

[14] T. Firmansyah, "Laman Telkomsel Dibajak, Ini Kata Menkominfo." http://www.republika.co.id/berita/ekonomi/korporasi/17/04/28/op4frp377-peretas-diyakini-berhasil-menguasai-server-situs-telkomsel. [Online; retrieved 10-May-2017].

[15] M. Khosroshahy, D. Qiu, and M. K. M. Ali, "Botnets in 4g cellular networks: Platforms to launch ddos attacks against the air interface," in *Selected Topics in Mobile and Wireless Networking (MoWNeT), 2013 International Conference on*, pp. 30–35, IEEE, 2013.

[16] C.-Y. Li, G.-H. Tu, C. Peng, Z. Yuan, Y. Li, S. Lu, and X. Wang, "Insecurity of voice solution volte in lte mobile networks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 316–327, ACM, 2015.

[17] M. Liyanage and A. Gurtov, "Secured vpn models for lte backhaul networks," in *Vehicular Technology Conference (VTC Fall), 2012 IEEE*, pp. 1–5, IEEE, 2012.

[18] S. Park, S. Kim, J. Oh, M. Noh, and C. Im, "Threats and countermeasures on a 4g mobile network," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2014 Eighth International Conference on*, pp. 538–541, IEEE, 2014.

[19] H. Kim, D. Kim, M. Kwon, H. Han, Y. Jang, D. Han, T. Kim, and Y. Kim, "Breaking and fixing volte: Exploiting hidden data channels and misimplementations," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 328–339, ACM, 2015.

[20] T. Q. Thanh, Y. Rebahi, and T. Magedanz, "A diameter based security framework for mobile networks," in *Telecommunications and Multimedia (TEMU), 2014 International Conference on*, pp. 7–12, IEEE, 2014.

[21] Thales, "Cyber-secured 4G/LTE PMR Networks: Guaranteeing Mission Success with Always Available and Operational Network." https://www.thalesgroup.com/sites/default/files/asset/document/whitepaper_securing-lte-pmr-corenetwork_ok_0.pdf. [Online; retrieved 4-March-2017].