AN NINH TRONG MẠNG LTE

KS. Bùi Trung Thành

Phòng NCPT Mạng và Hệ thống

Tóm tắt: *LTE là mạng truy nhập di động sẽ đóng vai trò quan trọng trong tổng thể hạ tầng cung cấp các dịch vụ tương lai. Với sự kế thừa các đặc trưng trong lĩnh vực di động cộng với đặc tính mạng all-IP dẫn đến nhiều yêu cầu cũng như giải pháp cho vấn đề an ninh trong miền mạng LTE. Bài báo này sẽ cung cấp thông tin tổng quan về an ninh trong mạng LTE giúp cho các nhà cung cấp dịch vụ di động tại Việt Nam có thêm thông tin cần thiết trong việc triển khai cho mạng LTE thời gian tới. Phần đầu bài báo nêu ra các yêu cầu về an ninh của mạng LTE, tiếp theo bài báo giới thiệu về kiến trúc an ninh được đưa ra bởi tổ chức 3GPP và phần cuối bài báo giới thiệu một số cơ chế an ninh cụ thể được áp dụng trên LTE để đáp ứng các yêu cầu đã nêu ra.*

1. GIỚI THIỆU

Với bất kỳ mạng IP nào việc đảm bảo an ninh là tối quan trọng, điều này đúng với mạng LTE, là một mạng di động all-IP với kiến trúc phẳng (eNodeB được kết nối với nhau thông qua giao diện X2, và kết nối trực tiếp với EPC thông qua giao diện S1, không có thành phần điều khiển tập trung cho các trạm vô tuyến).Bên cạnh các nguy cơ an ninh rõ ràng trêngiao diệnvô tuyến truyền đến và đi khỏi thiết bị người dùng (User Equipment - UE) còn là các nguy cơ an ninh truyền thống liên quan đến các liên kết IP của các nhà cung cấp mạng LTE. Việc xây dựng kiến trúc an ninh để đối phó với các nguy cơ là khởi đầu quan trọng cho các nhà cung cấp di động.

2. YÊU CẦU AN NINH CỦA MẠNG LTE

Tiêu chuẩn 3GPP TS 33.401 đưa ra các yêu cầu về các tính năng an ninh cần có trong mạng LTE như sau:

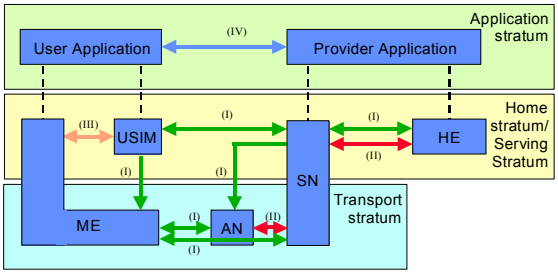
- Đảm bảo an ninh giữa người dùng và mạng, gồm:
  - Nhận dạng người dùng và bảo mật thiết bị,
  - Nhận thực các thực thể,
  - Bảo mật dữ liệu người dùng và dữ liệu báo hiệu,
  - Toàn vẹn dữ liệu người dùng và dữ liệu báo hiệu.
- Có khả năng cấu hình và hiển thị an ninh.
- Đáp ứng các yêu cầu an ninh trên eNodeB.

Ngoài ra, có một số yêu cầu khác đối với an ninh trên mạng LTE có thể dễ dàng nhận ra như:

- Các tính năng an ninh không được ảnh hưởng tới sự tiện dụng của người dùng.
- Các tính năngan ninh không được ảnh hưởng tới quá trình chuyển dịch từ 3G lên LTE.

3. KIẾN TRÚC AN NINH TỔNG QUÁT CỦA LTE

3GPP đã đưa ra kiến trúc an ninh tổng quát của LTE trong tiêu chuẩn 3GPP TS33.401 gồm 5 nhóm tính năngan ninh khác nhau:



Hình 1. Kiến trúc an ninh tổng quát của LTE

- **Network access security (I):** tập hợp các tính năngan ninh cung cấp khả năng bảo vệ truy nhập người dùng tới các dịch vụ, và cũng bảo vệ chống lại các cuộc tấn công trên liên kết truy nhập vô tuyến. Ví dụ: sử dụng USIM cung cấp truy nhập được đảm bảo cho người dùng tới EPC, bao gồm nhận thực tương hỗ và các tính năng riêng khác.

- **Network domain security (II):** tập hợp các tính năngan ninh cho phép các node trao đổi an toàn dữ liệu báo hiệu và dữ liệu người dùng (giữa AN và SN, và trong AN), và cũng bảo vệ chống lại các cuộc tấn công trên mạnghữu tuyến. Ví dụ: AS Security, NAS Security, IPsec EPS.
- **User domain security (III):**tập hợp các tính năngan ninh bảo vệ truy nhập tới các MS (Mobile Station). Ví dụ: khóa màn hình, mã PIN để sử dụng SIM.
- **Application domain security (IV):** tập hợp các tính năngan ninh cho phépbảo vệ các bản tin trao đổi của các ứng dụng tại miền người dùng và miền nhà cung cấp. Ví dụ: https.
- **Visibility and configurability of security (V):** tập hợp các tính năngan ninh cho phép thông báo tới người dùng một tính năng an ninh có đang hoạt động hay không, và các dịch vụ đang sử dụng và được cung cấp nên phụ thuộc vào tính năng an ninh không.

Dưới đây chúng ta sẽ xem xét một số tính năng an ninh áp dụng cho mạng LTE thuộc về các nhóm tính năng an ninh (I) và (II), là những nhóm tính năng an ninh đặc trưng và liên quan trực tiếp đến các thực thể trong mạng LTE.

4. MỘT SỐ CHỨC NĂNG VÀ CƠ CHẾ AN NINH ÁP DỤNG CHO MẠNG LTE

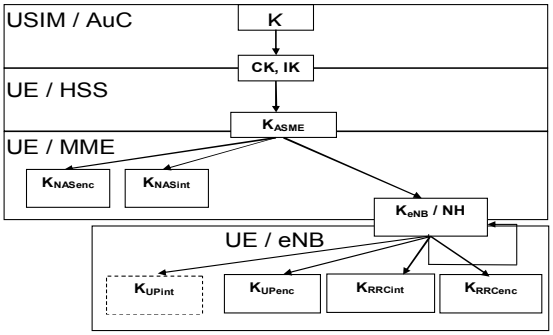
4.1. Cơ chế EPS AKA

Là cơ chế thuộc về nhóm tính năngan ninh(I) và (II), giúp nhận thực thuê bao trên mạng LTE/EPS, làm cơ sở cho việc tạo ra các khóa CK cơ bản cho U-Plane, RRC và NAS, cũng như tạo khóa IK cho RRC và AS. Cơ chế này được thực hiện như sau:

1) MME gửi các thông tin của thuê bao như IMSI, SN ID (Serving Network ID) tới HSS để tạo ra EPS AV (Authentication Vector). Sau đó HSS gửi trả MME các thông số nhận thực gồm: RAND, XRES, AUTN, K_{ASME}.
2) MME gửi tới USIM thông qua ME hai thông số RAND và AUTN cho việc nhận thực mạng từ vertor nhận thực được lựa chọn. MME cũng gửi một KSI_{ASME} cho ME để sử dụng cho việc nhận dạng khóa K_{ASME}được tạo ra bởi thủ tục EPS AKA.
3) Sau khi nhận được thông số từ MME, USIM kiểm tra xem AV mới hay không, bằng việc kiểm tra việc chấp nhận AUTN. Nếu thỏa mãn, USIM sẽ tính toán RES để phản hồi, đồng thời cũng tính toán CK và IK gửi tới ME. ME cũng kiểm tra bit 0 của AUTN được thiết lập bằng 1 hay không.
4) ME phản hồi bản tin chứ thông số RES tới MME trong trường hợp kiểm tra thành công. Sau đó ME tính toán K_{ASME} thông qua CK, IK và SN ID sử dụng thuật toán KDF. SN ID dùng để nhận dạng ngầm mạng phục vụ khi khóa K_{ASME} được sử dụng.
5) MME só sánh RES và XRES, nếu giống nhau thì nhận thực thành công.

Việc thực thi AKA có thể mất vài trăm ms cho việc tính toán khóa trên USIM và cho việc kết nối tới HSS, do đó có thể áp dụng một chức năng cho phép khóa được cập nhật không có AKA để đạt được tốc độ cao hơn trong LTE.

4.2. Hệ thống phân cấp khóa



Hình 2. Hệ thống phân cấp khóa trong LTE

Đối với việc mã hóa dữ liệu, LTE sử dụng một phương thức mã hóa luồng, trong đó dữ liệu được mã hóa bằng cách lấy một loại trừ OR (XOR) của dữ liệu và luồng khóa theo cùng cách như 3G. Các khóa được sử dụng để tạo ra luồng khóa được thay đổi thường xuyên để tránh lặp lại luồng khóa.Các khóa cũng cần không được sử dụng tại nhiều

điểm để tối thiểu hóa tổn hại do một trong các khóa mã hóa và bảo vệ toàn vẹn bị tổn thương. Để giải quyết vấn đề này trên LTE, hệ thống phân cấp khóa được sử dụng.Việc sử dụng hệ thống phân cấp khóa thuộc về nhóm tính năng an ninh(I) và (II).

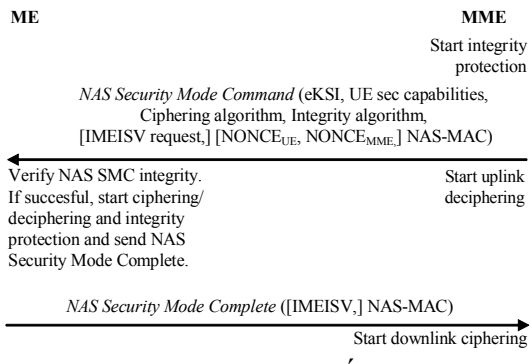
Hệ thống phân cấp khóa hoạt động như sau:

1) Giống như mạng 3G, USIM và AuC chia sẻ trước các thông tin bí mật (khóa K).
2) Khi AKA được thực thi cho nhận thực tương hỗ giữa mạng và người dùng, khóa CK cho mã hóa và IK cho bảo vệ toàn vẹn được tạo ra và được trao đổi tương ứng từ USIM tới ME và từ AuC tới HSS.
3) ME và HSS tạo ra khóa K_{ASME}tương ứng từ cặp khóa CK và IK. K_{ASME} được truyền từ HSS tới MME của mạng để phục vụ như là thông tin cơ bản trong phân cấp khóa.
4) Khóa K_{NASenc} cho mã hóa giao thức NAS giữa UE và MME; và khóa K_{NASint} cho bảo vệ tính toàn vẹn được tạo ra từ khóa K_{ASME}.
5) Khi UE kết nối tới mạng, UE và MME tạo ra khóa K_{eNB}, sau đó MME truyền khóa này cho eNodeB. Từ khóa K_{eNB} này, các khóa K_{UPenc} cho mã hóa U-Plane, khóa K_{RRCenc} cho mã hóa RRC và khóa K_{RRCint} cho bảo vệ tính toàn vẹn được tạo ra.

4.3. Chế độ AS security và NAS Security

Trong mạng LTE, các tính năng an ninh cho tín hiệu báo hiệu và tín hiệu dữ liệu người dùng được sử dụng ở hai chế độ là NAS Security và AS Security. Trong đó NAS Security được thực thi khi UE đang ở trạng thái rỗi, cho liên kết báo hiệu giữa UE và MME. Còn AS Security được thực thi khi UE ở trạng thái kết nối, cho liên kết truyền tải dữ liệu người dùng giữa UE và eNB. Đây là nhóm chức năng thuộc về nhóm tính năng an ninh (II).

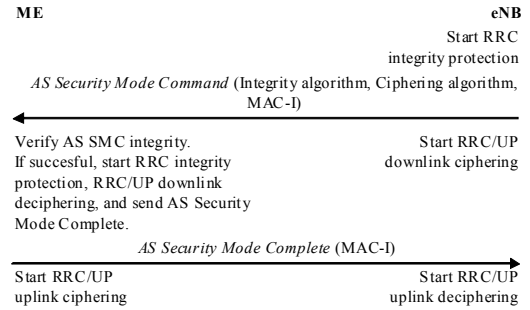
Sau khi nhận thực UE tiến vào trạng thái rỗi, chế độ an ninh NAS được thực thi.Chế độ này sẽ chỉ huy đàm phán thuật toán mã hóa và bảo vệ toàn vẹn cho truyền thông NASsử dụng các khóa K_{NASenc} và K_{NASint}.



Hình 3. Thủ tục thực hiện chế độ NAS Security

MME gửi bản tin *NAS Security Mode Command* tới UE, bao gồm tham số eKSI cho xác định khóa K_{ASME}, tham số chứa khả năng an ninh của UE, thuật toán mã hóa và toàn vẹn, và các tham số $NONE_{UE}$ và $NONCE_{MME}$ dùng khi chuyển giao. Bản tin này được bảo vệ toàn vẹn với khóa toàn vẹn NAS trên cơ sở khóa K_{ASME} được chỉ ra từ tham số eKSI trong bản tin. UE kiểm tra toàn vẹn của bản tin này, vànếu kiểm tra thành công thì UE bắt đầu mã hóa/giải mã hóa, bảo vệ toàn vẹn.Sau đó UE gửi bản tin phản hồi *NAS Security Mode Complete* tới MME.

Còn chế độ AS Security được thực hiện ngay sau khi UE tiến vào trạng thái kết nối, và áp dụng tới tất cả kết nối giữa UE và eNB, sử dụng các khóa K_{RRCenc}, K_{RRCint} và K_{UPenc}.



Hình 4. Thủ tục thực hiện chế độ AS Security

Trong chế độ AS Security, eNodeB gửi bản tin AS Security Mode Command tới ME, bao gồm tham số về các thuật toán mã hóa và toàn vẹn. Bản tin này được bảo vệ toàn vẹn với khóa toàn vẹn RRC trên cơ sở khóa K_{ASME} hiện tại.Tại eNodeB, mã hóa downlink RRC và UP được thực hiện ngay sau khi gửi bản tin này đi.UE kiểm tra toàn vẹn của bản tin này, nếu thành công thì UE bắt đầu mã hóa downlink RRC và UP, và gửi bản tin phản hồi AS Security Mode Complete tới

eNodeB.eNodeB sau khi nhận bản tin phản hồi thì bắt đầu mã hóa uplink RRC và UP. Tại những nơi không cho phép mã hóa, AS security có thể đàm phán một chế độ cung cấp an ninh không có mã hóa.

Các thuật toán mã hóa và bảo vệ toàn vẹn sử dụng trên LTE được dựa trên cơ sở Snow 3G và AES (Advanced Encryption Standard) đã được chuẩn hóa, và thuật toán sử dụng cho AS được đàm phán độc lập với thuật toán sử dụng cho NAS. Hai thuật toán này cung cấp đầy đủ tính năng an ninh, và khác nhau về cấu trúc sử dụng cơ bản trong 3GPP. Do đó trong trường hợp một thuật toán bị hủy hoại thì thuật toán còn lại vẫn tiếp tục đảm bảo cho hệ thống LTE.

4.4. Bảo vệ nhận dạng (Identity Protection)

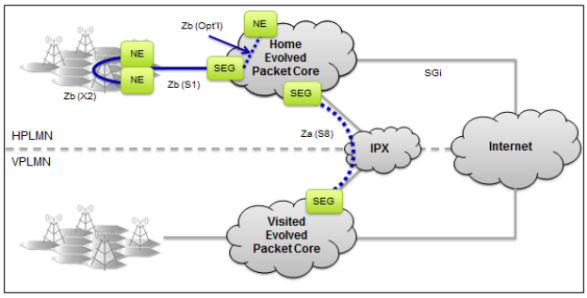
Nhóm tính năng an ninh (I) cũng cung cấp tính năng an ninh thông qua việc sử dụng hai thông số nhận dạng vĩnh viễn UE là:

- IMEI: dùng để nhận dạng thiết bị phần cứng. IMEI chỉ được gửi tới MME trên NAS, sau khi NAS Security được thiết lập thành công (bảo vệ được mã hóa và toàn vẹn).
- IMSI: dùng để nhận dạng thuê bao. IMSI hạn chế gửi qua môi trường vô tuyến, mà thay vào đó là tham số tạm thời GUTI.

4.5. NDS (Network Domain Security)

Để bảo vệ cho các lưu lượng trên cơ sở IP tại các giao diện của mạng truy cập/truyền tải (E-UTRAN), của mạng lõi (EPC), hay giữa các mạng lõi với nhau, 3GPP đưa ra chức năng **NDS/IP** (trừ giao diện S1-U do đây đã là giao diện được bảo vệ của 3GPP). NDS được định nghĩa trong tiêu chuẩn 3GPP TS 33.210 và là chức năng thuộc nhóm tính năng an ninh (II).

Đối với mạng LTE, kiến trúc NDS được triển khai như sau:



Hình 5. Kiến trúc triển khai NDS trên mạng LTE

- Mạng LTE được chia thành hai loại miền an ninh gồm miền E-UTRAN và miền EPC. Trong đó:
  - Miền EPC: tại biên đặt các SEG (Security Gateway), và trong miền có các NE là các node mạng được triển khai; ví dụ như MME, …
  - Miền E-UTRAN: do số lượng miền E-UTRAN lớn và kết nối với nhau qua một mạng lưới phức tạp do cùng tồn tại hai giao diện S1 và X2 nên giải pháp đặt SEG tại biên của mỗi miền EUTRAN là không hợp lý. Vì vậy tại các miền E-UTRAN chỉ có các NE là các node mạng (eNodeB) .
- Giao diện Za (giữa các SEG) song hành cùng giao diện S8 giữa Home-PLMN và Visited-PLMN, hoặc giữa Home-PGW và Visited-PGW.
- Giao diện Zb (giữa các NE hoặc giữa NE và SEG) song hành cùng giao diện S1 và X2 trong một mạng LTE của một nhà cung cấp. Giao diện này phải được triển khai giống với giao diện Za, nhưng không cần đầy đủ chức năng của SEG.
- Giao diện Zb giữa SEG và NE của EPC là tùy chọn do các node có thể được bảo vệ về mặt vật lý (cùng một mạng LAN).
- NDS/IP không đảm bảo an ninh cho kết nối giữa EPC và Internet (giao diện SGi).

NDS/IP cung cấp các dịch vụ an ninh như sau:

- Nhận thực dữ liệu gốc: bảo vệ một node khỏi các dữ liệu không rõ nguồn gốc.
- Toàn vẹn dữ liệu: bảo vệ dữ liệu được truyền không bị thay đổi (man-in-the-middle).

- Bảo vệ chống quá trình replay.
- Bảo mật dữ liệu: bảo vệ chống lại việc đánh cắp dữ liệu (eavesdropping).
- Bảo vệ giới hạn chống lại việc phân tích luồng dữ liệu.

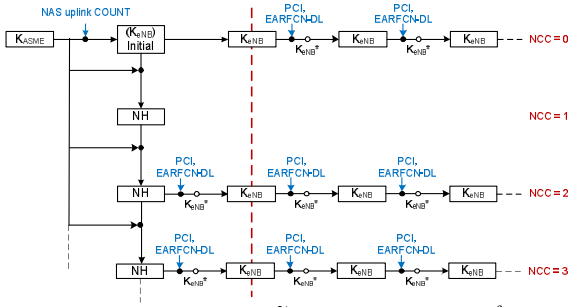
Các cơ chế bảo vệ được thực hiện thông qua IPsec, đặc biệt là IPsec ESP (Encapsulating Security Payload) trong chế độ đường hầm, với IKE (Internet Key Exchange) được sử dụng để thiết lập mối liên hệ an ninh IPsec giữa các SEG hoặc giữa SEG và NE. IPsec EPS cung cấp các tính năng bảo vệ an ninh, mà mỗi tính năng là tập hợp của nhiều thuật toán an ninh:

- Nhận thực: cung cấp ban đầu thông qua nhận thực tương hỗ và trao đổi khóa bảo mật giữa các SEG hoặc SEG và NE sử dụng giao thức IKE, và thông qua AH (Authentication Header) của các gói tin IPsec để đảm bảo nhận thực trên mỗi gói, ví dụ như sử dụng SHA-1.
- Toàn vẹn: cung cấp thông qua cơ chế băm gói mã hóa IPsec, ví dụ SHA-1.
- Bảo mật: cung cấp thông qua việc mã hóa IPsec đóng gói gói tin, ví dụ AES.
- Anti-replay.
- Bảo mật giới hạn luồng dữ liệu.

4.6. Forward Security

Đây là cơ chế thuộc nhóm tính năng an ninh (I), được đưa ra để ngăn chặn việc lộ thông tin các khóa K_{eNB}. Cơ chế này đảm bảo rằng một eNodeB với các thông tin về khóa K_{eNB} chia sẻ giữa nó và UE, sẽ không thể tính toàn được các khóa K_{eNB} tương lai được dùng giữa UE đấy với các eNodeB khác. Đặc biệt hơn, cơ chế N-hop Forward Security đảm bảo rằng một eNodeB không thể tính toán các khóa sẽ được sử dụng giữa một UE và các eNodeB khác mà UE sẽ kết nối sau N lần hoặc nhiều hơn N lần chuyển giao (N=1 hoặc 2).Cơ chế này được thực hiện thông qua khóa NH (Next-Hop) được lưu trữ trên MME.

Nguyên lý hoạt động cụ thể của cơ chế Forward Security như sau:



Hình 6. Mô hình chuỗi khóa cho chuyển giao

Khi AS Security cần được thiết lập giữa UE và eNodeB, MME và UE phải tạo ra các khóa K_{eNB} và NH từ khóa K_{ASME}.Trong thiết lập khởi tạo, K_{eNB} được tạo ra trực tiếp từ K_{ASME} và NAS uplink COUNT, tương ứng chuỗi khóa NCC = 0.Khóa K_{eNB} được sử dụng làm khóa cơ sở cho việc bảo vệ truyền thông giữa UE và eNodeB. Tiếp đó khóa NH được tạo ra từ K_{ASME}và K_{eNB} ở trên, và khóa này được sử dụng cho chuỗi khóa NCC=1 hoặc lớn hơn.Khi chuyển giao trực tiếp giữa các eNodeB xảy ra, thì một khóa mới K_{eNB}^* được tạo ra từ khóa K_{eNB} đang hoạt động hoặc từ NH.Quá trình lấy khóa K_{eNB}^* từ K_{eNB} đang tồn tại được mô tả bởi quá trình lấy khóa theo chiều ngang, K_{eNB}^* được tạo ra từ K_{eNB} với thông số EARFCN-DL (E-UTRAN Absolute Radio Frequency Channel Number – Downlink) của kết nối và PCI (Physical Cell Identity) của mục tiêu..Còn quá trình lấy khóa K_{eNB}^* từ NH được mô tả bởi quá trình lấy khóa theo chiều dọc, K_{eNB}^* được tạo ra từ NH với thông số EARFCN-DL và PCI.

Do NH chỉ có thể tính toán duy nhất bởi UE và MME, nên việc sử dụng quá trình lấy khóa từ NH đảm bảo được cơ chế Forward Security cho quá trình chuyển giao qua nhiều eNodeB.Chức năng này có thể giới hạn phạm vi của tổn hại, thậm chí nếu một khóa bị rò rỉ, bởi vì các khóa tương lai sẽ được tạo ra mà không sử dụng khóa K_{eNB} hiện tại trong trường hợp lấy khóa theo chiều dọc.

5. KẾT LUẬN

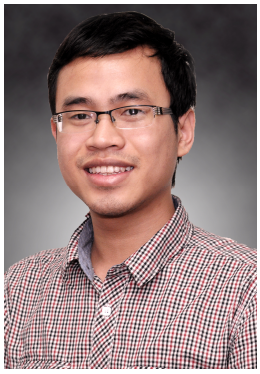
Cấu trúc mạng LTE là khác biệt so với các mạng di động trước đó nên mạng LTE đã được áp dụng nhiều cơ chế khác nhau để đáp ứng các yêu cầu an ninh được đặt ra. Trong đó, một số cơ chế là kế thừa từ các cơ chế của mạng 3G như EPS AKA, Identity Protection, hay NDS. Một số cơ chế là sự phát triển mới dành riêng cho mạng LTE như hệ thống phân

cấp khóa, AS Security, NAS Security hay Forward Security. Các cơ chế này có thể triển khai một cách dễ dàng trên thực tế do được kế thừa từ mạng 3G (các cơ chế kế thừa) hoặc được gắn liền với hoạt động của mạng LTE (các cơ chế mới). Ngoài các cơ chế ở trên, còn các cơ chế khác thuộc nhóm tính năng an ninh (I) và (II), được cung cấp cho LTE nhưng không đề cập chi tiết trong bài báo này như Home eNodeB Security, M2M (Machine-to-Machine) Security, Security for VoLTE. Và để tạo thành một kiến trúc an ninh đầy đủ cho mạng LTE, các cơ chế an ninh cho các nhóm tính năng an ninh (III), (IV), (V) cũng cần được sử dụng.

6. TÀI LIỆU THAM KHẢO

1. *Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller, Valtteri Niemi (2010), LTE Sercurity, Wiley;*
2. *Alf Zugenmaier, Hiroshi Aono, Technology Reports: Security Technology for SAE/LTE, NTT DOCOMO Technical Journal Vol. 11 No. 3;*
3. *Stoke, Inc WHITE PAPER - LTE Security Concepts and Design Considerations;*
4. *3GPP TS 33.401 v12.9.0 3GPP System Architechture Evolution (SAE); Sercurity architecture (Release 12);*
5. *3GPP TS 33.210 v12.2.03G security; Network Domain Security (NDS); IP network layer security (Release 12);*
6. *3GPP TS 33.310 v12.0.0 Network Domain Security (NDS); Authentication Framework (AF) (Release 12);*

Thông tin tác giả: **Bùi Trung Thành**



Năm sinh: 1988

Lý lịch khoa học: Tốt nghiệp Trường ĐHBK Hà Nội, 2006, Chuyên ngành: Điện tử - Viễn thông)

Hướng nghiên cứu: SDN, 4G-LTE, Networking

Email: thanhbt@ptit.edu.vn; thanhbt@cdit.com.vn