IPSEC PACKAGING SECURITY MECHANISM IN 4G/LTE MOBILE COMMUNICATION NETWORKS

Hoang Van Thuc
TNU - University of Information and Communication Technology

ARTICLE INFO

Received: 22/10/2022
Revised: 22/11/2022
Published: 22/11/2022

KEYWORDS

Network security
IP security mechanism
Packet security
IP Security
Mobile network security

ABSTRACT

Today, security issue in mobile communication networks in the world as well as in Vietnam is a very important issue. Therefore, network security and remediation solutions are essential. In the ways of network protection, IP Security becomes an effective solution to help secure the packets transmitted in the mobile communication network. The article presents problems and methods related to IP Security protocol, and introduce IP Security mechanism in 4G/LTE mobile communication network and provide security simulation methods packets using IP Security. IP Security protocol and application of IP Security mechanism protect the network domain control plane, and the user plane at the backhaul link in the 4G/LTE mobile communication network. From the obtained researches, the article shows how it works when transmitting packets secured by IP Security protocol in 4G/LTE networks.

CƠ CHẾ BẢO MẬT GÓI TIN BẰNG IPSEC TRONG MẠNG THÔNG TIN DI ĐỘNG 4G/LTE

Hoàng Văn Thực
Trường Đại học Công nghệ thông tin và Truyền thông - ĐH Thái Nguyên

THÔNG TIN BÀI BÁO

Ngày nhận bài: 22/10/2022
Ngày hoàn thiện: 22/11/2022
Ngày đăng: 22/11/2022

TỪ KHÓA

Bảo mật mạng
Cơ chế IP seccurity
Bảo mật gói tin
IP Security
Bảo mật mạng di động

TÓM TẮT

Ngày nay, vấn đề bảo mật trong các mạng thông tin di động trên thế giới và tại Việt Nam là một vấn đề rất quan trọng. Vì vậy các giải pháp khắc phục và bảo mật mạng là rất cần thiết. Trong các cách bảo vệ mạng, IP Security trở thành một giải pháp hiệu quả giúp bảo mật các gói tin được truyền trong hệ thống mạng thông tin di động. Bài báo sẽ trình bày các vấn đề và phương pháp liên quan đến giao thức bảo mật IP Security, đồng thời giới thiệu cơ chế bảo mật IP Security trong mạng thông tin di động 4G/LTE và đưa ra các phương pháp mô phỏng bảo mật gói tin bằng IP Security. Giao thức IP Security và áp dụng cơ chế IP Security để bảo vệ mặt phẳng điều khiển miền mạng, bảo vệ mặt phẳng người sử dụng ở đường liên kết backhaul trong mạng thông tin di động 4G/LTE. Từ những nghiên cứu đã đạt được, bài báo đưa ra cách hoạt động khi truyền gói tin được bảo mật bằng giao thức IP Security trong mạng 4G/LTE.

DOI: https://doi.org/10.34238/tnu-jst.6748

Email: hvthuc@ictu.edu.vn

1. Giới thiệu

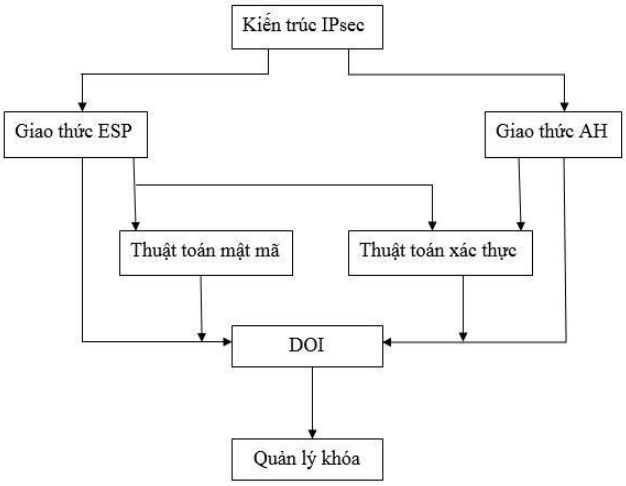
Với sự phát triển quá nhanh của công nghệ di động cũng đồng nghĩa với việc quản lý mặt thông tin ngày càng khó khăn và phức tạp. Với việc truy cập Internet tốc độ cao và các thiết bị đầu cuối di động hỗ trợ công nghệ 4G/LTE thì bất cứ ai cũng có thể trở thành nguồn cung cấp và tiếp nhận thông tin [1], [2]. Điều đó khiến các hacker lợi dụng thiết bị cầm tay như một máy trạm, chúng tấn công mạng và sử dụng thiết bị di dộng khác gây lây nhiễm mã độc dẫn đến người dùng bị ăn cắp thông tin ngân hàng, tin nhắn, danh bạ,… gây nên những hậu quả khôn lường [3], [4].

Với bất kỳ mạng IP nào việc đảm bảo an ninh là tối quan trọng, điều này là đúng với mạng 4G/LTE - một mạng di động all-IP. Trong đó, IP Security (Internet Protocol Security) là một giao thức nhằm đảm bảo tính bí mật, toàn vẹn và xác thực của thông tin trên nền giao thức Internet [5]. IP security thực hiện mã hóa packet và xác thực ở lớp network trong mô hình OSI. Nó cung cấp một giải pháp an toàn dữ liệu đầu – cuối trong bản thân cấu trúc mạng. Nhờ vào những ưu điểm trên mà IP Security đã được ứng dụng nhiều trong mạng virtual private network (VPN), cụ thể như gói phần mềm OspenS/wan,…[6], [7]. Giao thức IP Security và áp dụng cơ chế IP Security để bảo vệ mặt phẳng điều khiển miền mạng, bảo vệ mặt phẳng người sử dụng ở đường liên kết backhaul trong mạng thông tin di động [8]. Do đó, bài báo nghiên cứu để làm rõ thêm về các vấn đề bảo mật và giải pháp trong mạng thông tin di động 4G/LTE và tìm hiểu sâu hơn về giao thức IP Security trong mạng 4G/LTE.

2. Phương pháp nghiên cứu

2.1. Kiến trúc và tính năng IP Security

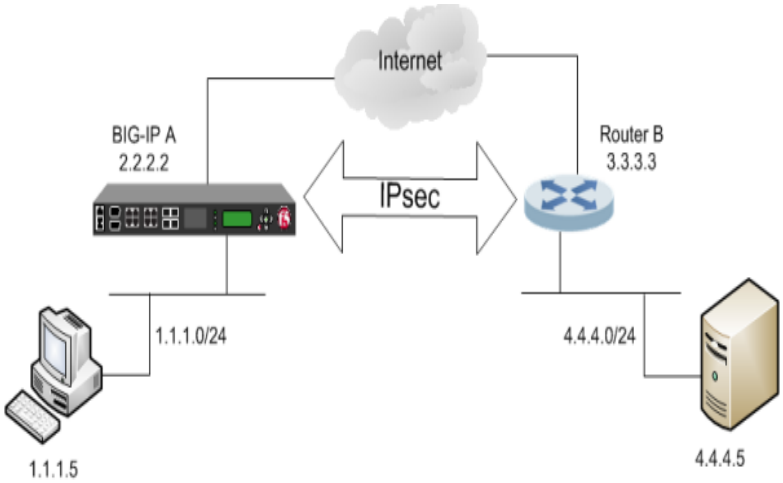
IP Security là một giao thức phức tạp, dựa trên nền của nhiều kỹ thuật cơ sở khác nhau như mật mã, xác thực, trao đổi khoá… Xét về mặt kiến trúc, IPSec được xây dựng dựa trên các thành phần cơ bản ở Hình 1 với hai thành phần cơ bản: Giao thức đóng gói, gồm AH và ESP, Giao thức trao đổi khoá IKE (Internet Key Exchange).



Hình 1. *Kiến trúc cơ bản của IP Security*

Mục đích chính của việc phát triển IPSec là cung cấp một cơ cấu bảo mật ở tầng 3 (Network layer) của mô hình OSI. IPSec là một phần bắt bược của IPv6, có thể được lựa chọn khi sử dụng IPv4. Trong khi các chuẩn đã được thiết kế cho các phiên bản IP giống nhau, phổ biến hiện nay là áp dụng và triển khai trên nền tảng IPv4.

Trong thế hệ mới này IP security cũng được viết tắt lại là IPsec. Sự khác nhau trong quy định viết tắt trong thế hệ được quy chuẩn bởi RFC 1825 – 1829 là ESP còn phiên bản mới là ESPbis [5].

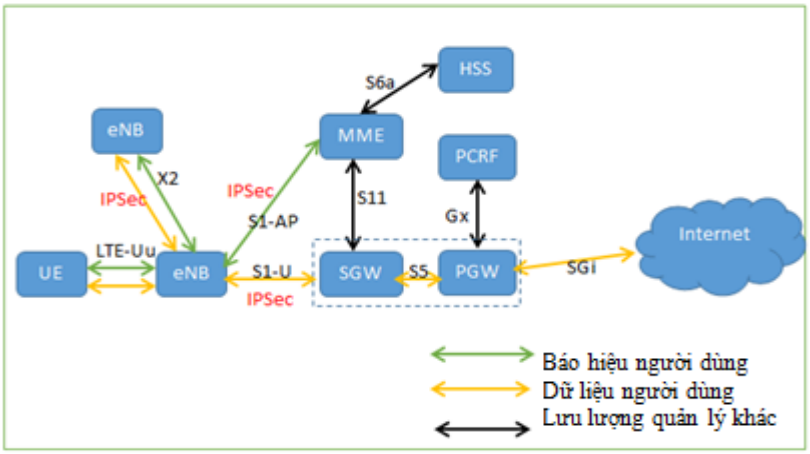


Hình 2. *Mô hình giao tiếp mạng trên cơ sở IPSec*

Mô hình giao tiếp mạng trên cơ sở IPSec thể hiện trên Hình 2 với mọi giao tiếp trong một mạng trên cơ sở IP đều dựa trên các giao thức IP. Do đó, khi một cơ chế bảo mật cao được tích hợp với giao thức IP thì toàn bộ mạng được bảo mật bởi vì các giao tiếp đều đi qua tầng 3. Ngoài ra, với IPSec, tất cả các ứng dụng đang chạy ở tầng ứng dụng của mô hình OSI đều độc lập trên tầng 3 khi định tuyến dữ liệu từ nguồn đến đích.

IPSec với các tính năng vượt trội như: Chứng thực 2 chiều trước và trong suốt quá trình giao tiếp. IPSec quy định cho cả 2 bên tham gia giao tiếp phải xác định chính mình trong suốt quy trình giao tiếp. Tạo sự tin cậy qua việc mã hóa, và xác nhận số các Packet. Tích hợp các thông tin chuyển giao và sẽ loại ngay bất kì thông tin nào bị chỉnh sửa. Chống các cuộc tấn công quay trở lại. IPSec dùng kĩ thuật đánh số liên tiếp cho các gói dữ liệu của mình, nhằm làm cho kẻ tấn công không thể sử dụng lại các dữ liệu đã chặn được, với ý đồ bất hợp pháp. Dùng Sequence numbers còn giúp bảo vệ chống việc chặn và đánh cắp dữ liệu, sau đó dùng những thông tin lấy được để truy cập hợp pháp vào một ngày nào đó [6].

2.2. Cơ chế IPSec trong mạng thông tin di động 4G/LTE



Hình 3. *Cơ chế bảo mật IPSec ở đường liên kết backhaul trong mạng 4G/LTE*

LTE có kiến trúc phẳng trong tất cả các giao thức mạng, nên phải đối mặt với những thách thức cũng như rủi ro trong việc truyền dẫn. Thông tin liên lạc giữa các trạm cơ sở được truyền đi trong các văn bản đơn giản, vì vậy dữ liệu có thể dễ dàng được giải mã, nghe trộm hay giả mạo.

Và hầu hết các trạm cơ sở đều được đặt trong môi trường không an toàn, vì thế khả năng tấn công vào các trạm cơ sở là rất cao.

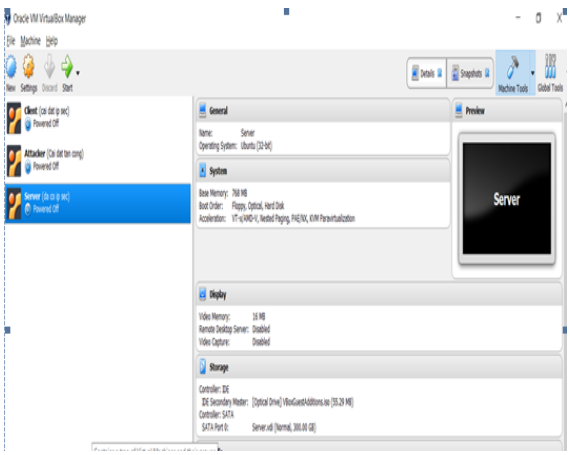
Trên hình 3 là mô hình cơ chế bảo mật IPSec ở đường liên kết backhaul trong mạng 4G/LTE. Trong đó, giao thức IKEv2 được dùng để trao đổi các SA để thiết lập IPSec tunnels. IKEv2, IPSec với bảo vệ tính toàn vẹn và bí mật là bắt buộc với tất cả luồng dữ liệu (mặt phẳng điều khiển, người dùng hay quản lý). Tuy nhiên, trong trường hợp giao diện S1 và X2 đáng tin cậy (ví dụ có bảo vệ vật lý), việc sử dụng IPSec/IKEv2 sẽ không cần thiết. Điều này được áp dụng cho cả luồng dữ liệu mặt phẳng điều khiển và quản lý [7].

Trong mặt phẳng điều khiển, IPSec được dùng để bảo mật lưu lượng dữ liệu người dùng, các đường truyền tín hiệu giao tiếp giữa eNB và MME. Trong suốt quá trình khởi tạo attach, UE gửi yêu cầu và nhận phản hồi từ eNB thông qua kết nối RRC (Radio Resource Control), eNB nhận được bản tin từ UE gửi yêu cầu và nhận phản hồi từ MME thông kết nối S1 signaling, các bản tin trong quá trình attach chứa rất nhiều thông tin định danh. Khi kẻ tấn công tấn công vào liên kết S1 signaling, mọi thông tin của UE, eNB đều có thể bị lấy cắp. Chính vì vậy, IPSec là giải pháp được lựa chọn để bảo mật đường tín hiệu giữa eNB và MME [8].

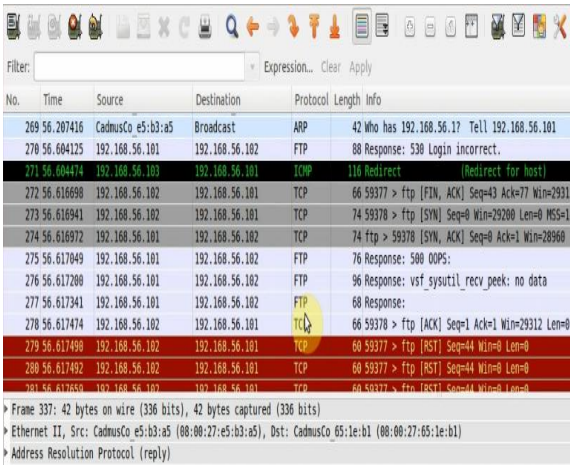
3. Mô phỏng thực nghiệm và đánh giá

3.1. Mô phỏng bảo mật gói tin bằng IPSec

Trên hình 4 là giao diện cài đặt môi trường trên máy ảo với ba máy ảo Ubuntu version 12.04, một máy server: địa chỉ 192.168.56.101, một máy client: địa chỉ 192.168.56.102, một máy attacker: địa chỉ 192.168.56.103.



Hình 4. *Cài đặt môi trường trên máy ảo*



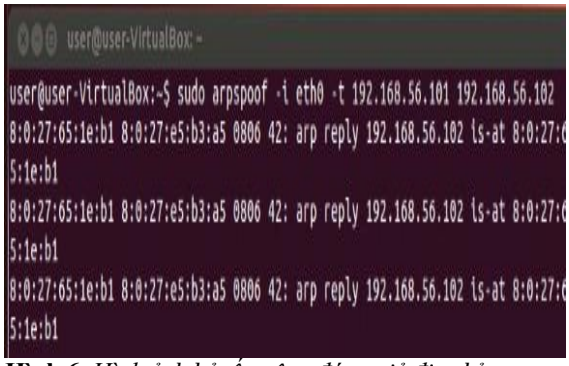
Hình 5. *Dữ liệu gói tin bắt được phía Server*

Với giao diện được thể hiện trên hình 5, người dùng truy cập vào server, tuy nhiên trên attacker không bắt được thông tin username và password của người dùng nữa. Gói tin dữ liệu được gửi từ client đến server hiển thị trong bản tin wireshark. Các gói tin đã được mã hóa bằng giao thức ESP, không bị kẻ tấn công nghe lén và ăn cắp thông tin [9].

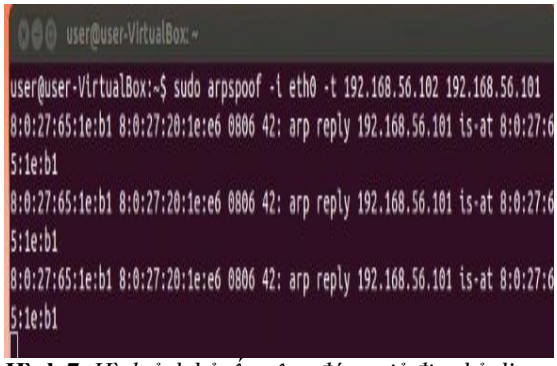
3.2. Bài toán thực nghiệm

Hình 6 thể hiện kẻ tấn công đóng giả địa chỉ client đối với server. Lúc này kẻ tấn công bật tính năng forward các bản tin IPv4 trên máy mình và bắt gói tin bằng dsniff (một công cụ giúp phân tích các gói tin trong mạng).

Kịch bản triển khai giả thiết rằng ở đây máy Server đóng vai trò là SAEGW, máy client đóng vai trò là eNB, và attacker tấn công ở giữa. Khi eNB gửi dữ liệu về phía SAEGW trên mặt phẳng dữ liệu người dùng, attacker tấn công và đánh cắp các thông tin truyền gửi giữa eNB và SAEGW được thể hiện trên Hình 7 [10].



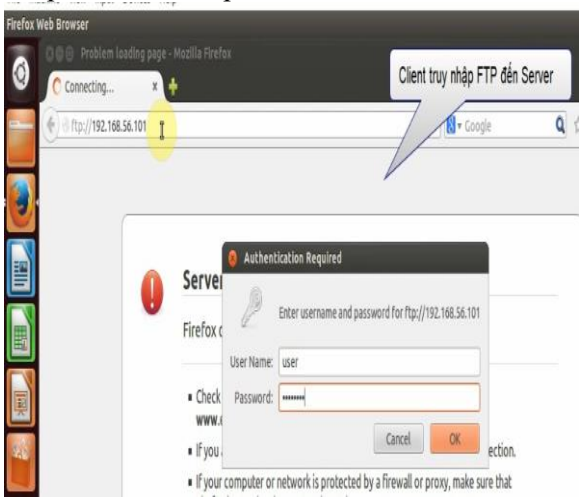
Hình 6. *Hình ảnh kẻ tấn công đóng giả địa chỉ server*



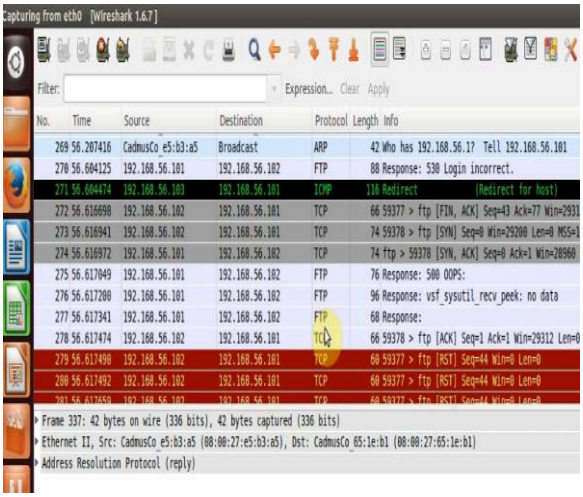
Hình 7. *Hình ảnh kẻ tấn công đóng giả địa chỉ client*

3.3. Mô phỏng nhận xét và đánh giá

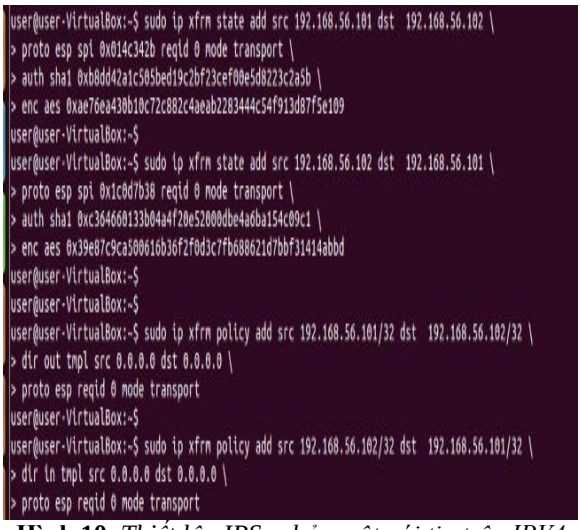
Giao diện trên Hình 8 thể hiện người dùng truy cập vào server, server yêu cầu người dùng nhập username và password xác thực.



Hình 8. *Người dùng truy cập vào địa chỉ server*



Hình 9. *Dữ liệu gói tin bắt được phía server*



Hình 10. *Thiết lập IPSec bảo mật gói tin trên IPV4 phía Server*

Hình 11. *Thiết lập IPSec bảo mật gói tin trên IPV4 phía Client*

Hình 9 là minh họa Gói tin dữ liệu được gửi từ client đến server hiển thị trong bản tin wireshark không được mã hóa. Để thiết lập IPSec hai đầu server và client, cần sử dụng IP framework cho truyền tải gói tin (xfrm). Xfrm được dùng để thực thi các bộ giao thức IPSec với state hoạt động trên cơ sở dữ liệu Security Asociation (SAD), và policy hoạt động dựa trên Cơ sở dữ liệu Security Policy (SPD).

Trên Hình 10 và Hình 11, ta nhận thấy rằng người dùng truy cập vào server, tuy nhiên trên attacker không bắt được thông tin username và password của người dùng nữa. Gói tin dữ liệu được gửi từ client đến server hiển thị trong bản tin wireshark. Các gói tin đã được mã hóa bằng giao thức ESP, không bị kẻ tấn công nghe lén và ăn cắp thông tin.

4. Kết luận

Bài báo nghiên cứu cơ chế bảo mật gói tin trong mạng thông tin di động 4G/LTE. IPSec trờ thành một giải pháp hiệu quả, nhằm bảo mật các gói tin được truyền trong hệ thống mạng thông tin di động 4G/LTE. IPSec là một giao thức được chuẩn hóa bởi IETF, là tập hợp các chuẩn mở để đảm bảo sự cẩn mật dữ liệu, đảm bảo tính toàn vẹn dữ liệu và chứng thực dữ liệu giữa các thiết bị mạng.

Bài báo đã góp phần giải quyết vấn đề bảo mật trong mạng thông tin di động 4G/LTE. Điều này đã mang lại nhiều lợi ích thiết thực cho cuộc sống, cho sản xuất và cho khoa học. Trong tương lai, các tính năng bảo mật vượt trội của IPSec như tạo sự tin cậy qua việc mã hóa, xác nhận số các gói tin, tích hợp các thông tin chuyển giao và sẽ loại ngay bất kì thông tin nào bị chỉnh sửa chống các cuộc tấn công quay trở lại. Hơn thế nữa, do các gói mã hóa của IPSec có khuôn dạng giống như gói tin IP thông thường, nên sẽ dễ dàng được định tuyến qua mạng Internet mà không phải thay đổi các thiết bị mạng trung gian, qua đó cho phép giảm đáng kể các chi phí cho việc triển khai và quản trị. Hướng nghiên cứu tiếp theo của bài báo sẽ tập trung vào các giải pháp tiên tiến về bảo mật sử dụng cơ chế IPSec không chỉ ở đường liên kết Backhauld mà còn ở phía luồng dữ liệu quản lý bên trong và ngoài mạng thông tin di động thế hệ mới.

TÀI LIỆU THAM KHẢO/ REFERENCES

[1] L. Zhu, H. Qin, H. Mao, and Z. Hu, "Research on 3GPP LTE Security Architecture," *8th Int. Conf. Wirel. Commun. Netw. Mob. Comput.*, vol. 2012, pp. 1–4, Sep. 2012.

[2] J. Cao, M. Ma, S. Member, I. H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *Ieice trans. Commun.*, vol. e100-b, no. 5, pp. 283-302, 2017.

[3] C. Kowtarapu, C. Anand, G. K, and S. Sharma, "Network separation and IPsec CA certificates-based security management for 4G networks," *Bell Labs Tech. J.*, vol. 13, no. 4, pp. 245–255, Feb. 2009.

[4] L. Yi, K. Miao and A. Liu, "A comparative study of WiMAX and LTE as the next generation mobile enterprise network," *13th Int. Conf. Adv. Commun. Technol*, 2011, pp. 654–658.

[5] N. T. T. Docomo, "Toward LTE Commercial Launch and Future Plan for LTE Enhancements LTEAdvanced," *Bell Labs Tech. J.*, vol. 12, pp. 146–150, 2010.

[6] F. Leu, I. You, Y. Huang, K. Yim, and C. Dai, "Improving Security Level of LTE Authentication and Key Agreement Procedure," *IEICE Transactions on Communications*, vol. E100, pp. 738–748, 2017.

[7] H. Shajaiah, A. Khawar, A. Abdel-hadi, and T. C. Clancy, "Resource Allocation with Carrier Aggregation in LTE Advanced Cellular System Sharing Spectrum with S-band Radar," *Conf. Wirel. Commun. Netw. Mob. Comput*, vol. 9, pp. 34–37, 2014.

[8] S. Zhiyuan, J. Zhiliang, G. Zhibin, and H. Lianfen, "Layered security approach in LTE and simulation," in *3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*, ASID 2009, vol. 12, pp. 2–4, 2009.

[9] K. Mio and A. Lau, "Network management based on ipsec," *IJRAR: International Journal of Research and Analytical Reviews*, vol. 1, no. 1, pp. 446-453, January 2014.

[10] A. Laguidi, A. Hayar, and M. Wetterwaldo, "Secure HeNB Network Management Based VPN IP Security," *NATO workshop on Advanced Security Technologies in Networking number*, vol. 10, pp. 2–4, December 2012.