SECURITY AND COMMUNICATION NETWORKS
*Security Comm. Networks* 2016; **9:**1198–1215
Published online 11 January 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1411

RESEARCH ARTICLE

# Novel secure VPN architectures for LTE backhaul networks

Madhusanka Liyanage[1]*, Pardeep Kumar[2], Mika Ylianttila[1] and Andrei Gurtov[3]

[1] Centre for Wireless Communications, University of Oulu, Oulu, Finland
[2] Department of Computer Science, UiT The Arctic University of Norway, Tromso, Norway
[3] Helsinki Institute for Information Technology HIIT, Aalto University, Espoo, Finland and ITMO University,Saint Petersburg, Russia

## ABSTRACT

In this paper, we propose two secure virtual private network architectures for the long-term evolution backhaul network. They are layer 3 Internet protocol (IP) security virtual private network architectures based on Internet key exchange version 2 mobility and multihoming protocol and host identity protocol. Both architectures satisfy a complete set of 3GPP backhaul security requirements such as authentication, authorization, payload encryption, privacy protection, and IP-based attack prevention. The security analysis and simulation results verify that the proposed architectures are capable enough to protect long-term evolution backhaul traffic against various IP-based attacks. Copyright © 2016 John Wiley & Sons, Ltd.

**KEYWORDS**
VPN; LTE; backhaul; IPsec; MOBIKE; IKEv2; HIP

***Correspondence**
Madhusanka Liyanage, Centre for Wireless Communications, University of Oulu, PO Box 4500, FI-90014 Oulu, Finland.
E-mail: madhusanka@ee.oulu.fi

## 1. INTRODUCTION

Mobile broadband usage is growing faster than the fixed Internet usage because of the rapid increment of mobile subscribers and bandwidth-hungry mobile applications. It is envisioned that high speed packet access (HSPA) and HSPA+ architectures are not adequate to facilitate future mobile networks services. Thus, long-term evolution (LTE)/LTE-advance architectures will dominate in the near future. LTE architecture consists of a new all-Internet protocol (IP) backhaul network. The existing non-IP-based security mechanisms are not adequate enough to provide a sufficient level of security for all-IP-based LTE backhaul networks. Thus, 3GPP specified new security requirements for the LTE backhaul network [1–6]. For example, LTE core elements now establish connections with less secure noncore elements such as evolved NodeBs (eNBs) and microcell base stations (BSs). The capturing of such devices is comparably easier than core backhaul element, and the number of entry points is comparably higher in LTE networks because of femtocell deployments [5]. Thus, denial of service (DoS) attacks are highly probable in LTE networks. However, the existing LTE traffic architectures are incapable to provide a sufficient level of security for the backhaul network against such IP-based attacks. The primary focus of this research is to study these security requirements of LTE backhaul network and build a secure LTE backhaul traffic architecture to protect the LTE backhaul communication channels from the IP-based attacks.

On the other hand, LTE backhaul supports heterogeneous traffic types, such as S1-U traffic from eNBs to the service gateway (S-GW), S1-C traffic from eNBs to the mobility management entity (MME), and X2-U and X2-C traffic between eNBs (Figure 1) [7]. It is a crucial traffic transport issue to provide different levels of quality of service (QoS), queuing priorities and fault management services for different traffic classes. Virtual private network (VPN)-based backhaul traffic architectures successfully solve above traffic transport issues, and several research studies verified the applicability of such VPN architectures [7–10]. However, none of these VPN architectures consider the security aspect of LTE backhaul network. However, 3GPP specifications [1–3] have specified the requirements of IP security (IPsec) in order to protect the S1 and X2 control plane. For both S1-MME and X2-C interfaces, Internet key exchange version 2 (IKEv2) certificates-based authentication shall be implemented [3].

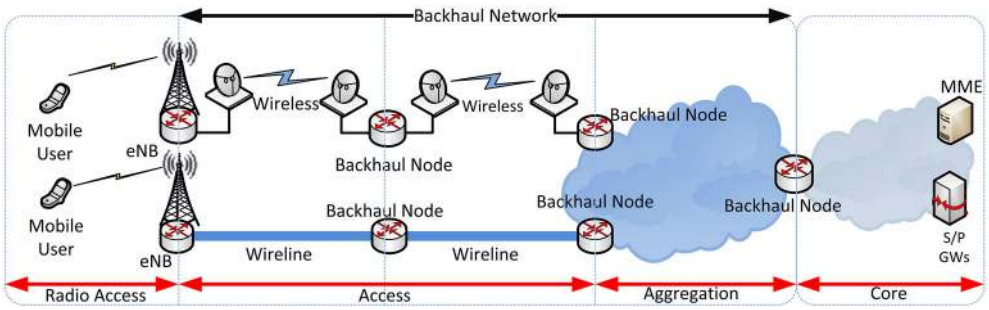


**Figure 1.** The long-term evolution transport network. eNB, evolved NodeB; MME, mobility management entity.

Therefore, it is required to design a new LTE backhaul VPN architecture that not only solves traffic transport issues but also provides the protection against IP-based attacks by implementing IPsec tunneling.

- Our contribution

To satisfy the aforementioned LTE backhaul network security requirements, this paper contributes the following:

(1) Proposal of two secure VPN-based backhaul traffic architectures. Namely, IPsec tunnel mode VPN architecture based on Internet key exchange version 2 mobility and multihoming protocol (MOBIKE) and IPsec bound end-to-end tunnel (BEET) mode VPN architecture based on host identity protocol (HIP).
(2) Proposal of novel message exchange procedures to dynamically and securely add new network nodes/devices to the LTE backhaul network.
(3) Proposal of a novel tunnel-established procedure to establish secure VPN tunnels between backhaul devices.

The security analysis reveals that proposed architectures satisfy a complete set of 3GPP security requirements such as authentication, authorization, payload encryption, and privacy protection and protect the backhaul network against IP-based attacks. On the other hand, the proposed VPN-based traffic architectures also solve the aforementioned traffic transport issues. Moreover, the material in this paper was presented in part at [11].

The rest of the paper is organized as follows. The background of LTE backhaul network and its security issues are presented in Section 2. Related works are mentioned in Section 3. The proposed VPN architectures are presented in Sections 4 and 5. We discuss simulation models and the protection from IP-based attacks in Section 6. The security and performance analysis of the proposed architectures are presented in Sections 7 and 8, respectively. The future directions and additional features of the proposed architectures are discussed in Section 9. Finally, Section 10 concludes the paper.

## 2. LONG-TERM EVOLUTION MOBILE BACKHAUL NETWORK MODEL, SECURITY ISSUES, AND REQUIREMENTS

### 2.1. Long-term evolution mobile backhaul network

The LTE transport network contains three segments, namely, radio access, backhaul, and core networks. The backhaul network further subdivides into two sections: access and aggregation networks. Figure 1 illustrates a simple LTE transport network.

The *access network* connects eNBs sites to aggregation nodes. Usually, it has a tree and/or chain topology. The *aggregation network* very often has a ring and/or mesh topology. It is normally terminated at the core network where S-GWs and MME devices are located. Hence, the *backhaul network* extends from the first transport equipment connecting cell sites (e.g., eNBs sites) to the transport aggregation equipment connecting central sites (e.g., S-GWs/MME sites) [12]. In addition, the LTE backhaul network contains several traffic transport interfaces (e.g., S1 and X2).

### 2.2. Security issues of long-term evolution backhaul network

3GPP specifications propose an entirely new flatten and all-IP-based architecture for the LTE backhaul network. It distributes some of the control functionality throughout the network. Hence, it pushes more intelligence to end nodes such as eNBs. These properties redefine the security and other service requirements of the LTE backhaul network.

Long-term evolution networks face new security threats that did not exist before or were harder to exploit in previous 2G/3G mobile backhaul networks. The security threats originate at various sections of LTE network, namely, customer nodes, backhaul network, customer provider interface network, radio access network, and core network. Hence, it is necessary to implement dedicated security mechanisms in each section to avoid these potential threats. This research focuses on the possible threats only on the

backhaul network. Three main reasons are identified for security threats in LTE backhaul [4–8,13,14].

First, LTE backhaul consists of IP-based control/service devices (e.g., MMEs, S-GWs, and eNBs) and interfaces (e.g., X2 and S1). As a result, the backhaul network is now vulnerable to IP-based attacks and breaches [5]. Moreover, an intruder can directly attack core gateways even from a breach at the access network because of the IP-base communication (e.g., address spoofing attacks) [13].

Second, LTE backhaul network is now a carrier Ethernet environment with hundreds or thousands of end nodes (e.g., eNBs). Hence, an intruder has thousands of potential entry points in the backhaul network [4,5,13]. Moreover, the flat architecture concept proposes to distribute the certain control functionalities even for eNBs [6]. Hence, a single eNB acquisition is sufficient enough for an attacker to do a significant damage to the network. On the other hand, LTE architecture introduces new interfaces to mobile networks. For instance, X2 interface is used to transport the peer-to-peer data and control traffic between eNBs and S1 interfaces is used to transport the user data and control traffic between eNBs and core elements. LTE networks allow an eNB to connect to multiple core network elements (up to 16) via S1 interfaces and multiple eNBs (up to 32) via X2 interface to achieve better performance and lower latency performance [15,16]. In contrast to prior 2G/3G networks, LTE eNBs now have more connections not only with other eNBs but also core network elements.

Third, the focus of security in 2G networks was the air interface, which was terminated at the BS for circuit-switched voice services. The backhaul network based on circuit-switched links was considered trusted. For 3G, it was a design decision that termination of the encryption for both services would move further into the core network at the radio network controller, for example, to encompass microwave links and most of the backhaul network. However, LTE backhaul does not have built-in security in bearer data as it was the case with 2G/3G networks. Prior to LTE architecture, traffic in backhaul network was secured by radio network layer protocols, and they encrypt the backhaul traffic [6,14]. However, these air interface encryptions of user and control plane traffic terminate at eNBs in LTE networks. As a result, LTE backhaul traffic can be eavesdropped by unauthorized users, and this information can be used to pose the DoS and man-in-the-middle attacks to the backhaul network.

Some research studies have already highlighted the potential risks that related to new LTE backhaul network [17–20]. A single event triggered on the phone (for instance, a state transition in the radio resource control state machine) implies a substantial number of messages exchanged among several LTE backhaul nodes. This could be exploited to become a distributed DoS (DDoS) attack by infecting many phones [19]. Bassil *et al.* [17] investigate the effects of signaling attacks that consist of malicious users who repeatedly trigger the dedicated bearers requests. Jover [18] analyzes attacks that can affect the LTE backhaul network availability. Moreover, common DoS and DDoS attacks on other IP networks could have a severe effect on network performance on new IP-based LTE backhaul, for instance, by a fortuitous error in an android application that created havoc in one of the mobile networks [19]. In [17], the authors identify that advanced persistent threats, which are well organized and financed, can have very negative effects and provoke both general and very targeted attacks. Such attacks were not possible in prior non-IP mobile backhaul networks. Although, most of these IP attacks are common to other IP networks, these attacks are still new for mobile networks as they were not vulnerable to such attacks before.

### 2.3. Internet protocol-based attack scenarios in the long-term evolution backhaul network

Above security issues in an LTE backhaul network motivate many attackers, such as cyber terrorists, individual competitors, and hackers. They can perform IP-based attacks on LTE backhaul to disturb the operation of the mobile network. These attacks can be categorized as follows.

- DoS attacks

Long-term evolution architecture is also used to centralize control devices similar to previous 2G/3G networks. For instance, home subscriber server (HSS) is a central authentication node that stores information for every subscriber in the network. It contains the subscriber-related information including QoS profiles, roaming restrictions, billing and account information, cryptographic primitives, and keys to perform authentication of subscribers [15]. These centralized network elements are honeypots for DoS attackers. DoS attacker can insert excessive amount of forged packets to the backhaul to disturb the operation of vital devices. As a result, unexpected service breakdowns and system failures may occur. Ultimately, the whole mobile network may be unresponsive to provide services for mobile subscribers. For instance, a successful attack on HSS can jeopardize the entire operation of LTE network [5]. Therefore, it is required to implement proper DoS attack mitigation mechanism to protect centralized entities in LTE backhaul networks.

Distributed DoS attacks are another variation of DoS attacks. In DDoS attack, more than one attacker is releasing forge packets to the backhaul network. Most of the LTE backhaul entities are connected to multiple other entities. For instance, HSS can be connected to several MMEs [15]. An eNB can be connected to at most 16 other eNBs. This feature motivates DDoS attackers. The attacker can impersonate or capture multiple entities in the backhaul networks to attack the important network elements [5]. In contrast to 2G/3G networks, LTE core elements now establish connections with less secure non-core elements such as eNBs and microcell BSs. Capturing of such devices is comparably easier than core backhaul element, and the number of entry

points is comparably higher in LTE networks because of femtocell deployments [5]. Thus, DDoS attacks are highly probable in LTE networks.

- Spoofing attacks

All-IP-based LTE networks are vulnerable to IP address spoofing attacks [4,13]. IP spoofing is a serious threat in LTE backhaul networks. An attacker can eavesdrop the control signaling data and hijack the IP address of a legitimate node. If the attacker hijacks the IP address while it is being returned to the IP pool, the other party will not be able to detect this threat. Thus, the other party will provide the services without identifying the attacker [4].

- Message modification attacks

Integrity protection is one of the key security requirement in mobile networks. The data modification attacks impose serious issues in LTE backhaul networks. The integrity violation of LTE control signaling directly affects performance of network. For instance, the attacker can modify the control signaling data to reduce buffer sizes, queue lengths, and timer values of backhaul components. It degrades the overall performance of the network. Modifying data transport in S6a interface may result to provide unauthorized services to mobile subscribers [15].

- Reset attacks

Long-term evolution backhaul devices exchange a significant number of control messages during the bearer establishment and disconnecting instances. A reset attacker can perform reset attack by sending malicious reset requests to terminate an ongoing bearer sessions or re-establish these bearer sessions. In that way, the attacker can generate massive amount of signaling data to overload the LTE backhaul networks. For instance, a reset attacker who gets the access to eNBs can reset up to 32 X2 and 16 S1 interface bearers [13,15].

- Eavesdropping attacks

Long-term evolution core elements now establish connections with less secure non-core elements such as eNBs and microcell BSs. Capturing of such devices is comparably easier than core backhaul element, and the number of entry points is comparably higher in LTE networks because of femtocell deployments [5]. Therefore, eavesdropping is also a serious security issue in LTE networks. For instance, an attacker can tap in to the S1 interface; he or she can extract signaling and user information. Later, this information can be used to perform reset and spoofing attacks. If an attacker taps in to the X2 interface, it is possible to track mobile users' location and movements by monitoring the handoff operations [13]. It seriously violates the privacy of mobile users. Moreover, the attacker can steal the credentials of mobile users to perform overbilling attacks on the particular users [4]. If an attacker taps into the control interfaces such as S11, SGi, G7, or S3, he or she can obtain the important information about backhaul elements [13,15]. This information can be used to modify the configurations of LTE backhaul network components (e.g., routers, switches, and GWs).

In contrast to 2G/3G networks, LTE backhaul networks are lacking of radio network layer encryption. Moreover, IP-based backhaul traffic transportation attracts a huge set of IP sniffer to attack the mobile networks. Therefore, eavesdropping is also a serious security issue in LTE networks. For instance, if an attacker taps into the S1 interface, he or she can extract signaling and user information. Later, this information can be used to perform reset and spoofing attacks. If an attacker taps into the X2 interface, it is possible to track mobile users' location and movements by monitoring the handoff operations [13]. It seriously violates the privacy of mobile users. Moreover, the attacker can steal the credentials of mobile users to perform overbilling attacks on the particular users [4]. If an attacker taps into the control interfaces such as S11, SGi, G7, or S3, he or she can obtain the important information about backhaul elements [13,15]. These information can be used to modify the configurations of LTE backhaul network components (e.g., routers, switches, and GWs).

## 2.4. Security requirements of the long-term evolution backhaul network

According to 3GPP specifications, security is an indispensable requirement of a backhaul traffic architecture. In order to make the backhaul network as secure as possible, 3GPP specified security services including the following: node authentication, node authorization, payload encryption, privacy protection, and IP-based attack prevention [1–6].

*Node authentication and authorization* prevent unauthorized access to the backhaul network. It ensures that the backhaul traffic is transported only between the legitimate devices (i.e., no impersonation of legitimate device has occurred). *Payload encryption* prevents eavesdropping attacks on backhaul traffic. In addition, it secures the integrity of the backhaul traffic by preventing in-flight message modifications. *Privacy protection* hides the identities of the important devices and secures them from being a target of attackers. *IP-based attack prevention* insures the availability and smooth operation of the network devices.

## 2.5. Internet key exchange version 2 mobility and multihoming protocol

Internet key exchange was defined by Internet Engineering Task Force (IETF) [21–23]. IKE uses to set up security associations (SAs) for an IPsec tunnel. SAs define the manner that two end points should communicate securely. For instance, it defines traffic encryption

algorithms, hash functions, and message authentication codes. On the other hand, IKE protocol mutually authenticates the users and exchanges a secure key for the encryption.

Because the specifications for IKE were covered in various request for comments (RFCs), IETF specified IKEv2 [24] to integrate all these RFCs. IKEv2 is the version 2 of the IKE protocol that not only combines all the IKE RFCs but also provides additional features such as network address translation traversal support, stream control transmission protocol support, simplify the cryptographic mechanisms, DoS attack resilience, and support for firewall traversal.

However, either IKE or IKEv2 protocols cannot support the mobility and/or multihoming features. In [25], authors proposed a mobility and multihoming extension to IKEv2 that is called MOBIKE. MOBIKE allows users to move from one IP address to another without re-establishing all SAs and IPsec tunnels. This will become more important with the introduction of LTE backhaul nodes such as vehicular and mobile femtocells [26].

## 2.6. Host identity protocol

Host identity protocol is a new security and mobility protocol that is standardized by IETF [27,28]. It separates the dual roles of IP address as an end-point identifier and a locater. HIP introduces a new layer to transmission control protocol (TCP)/IP model. It operates in between the transport and Internet working layer. A self-generated public–private key pair is used to generate the host identity (HI). Thus, HIP defines to use the public keys as new HI name space and the end-point identifiers. However, an HI may have variable length. Thus, a 128-bit hash of HI is called host identity tag (HIT), which is used by upper-layer applications as the end-point identifier. Hence, typical IP addresses are used only for the locater role.

Host identity protocol nodes follow an initial procedure called base exchange (BEX) before any data transfer event. HIP BEX is a four-way handshake between end nodes to establish SAs for an IPsec tunnel. HIP specification is recommended to use IPsec BEET mode tunnel between nodes. Furthermore, HIP BEX mutually authenticates end nodes [27].

## 2.7. Comparison with existing Internet protocol security solutions

Several key exchange mechanisms are widely used to set up SAs for an IPsec tunnel, namely, Internet key exchange version 1 [23], IKEv2 [24], MOBIKE [25], and HIP [27].

However, it is not possible to implement existing IPsec solutions in LTE networks because of various issues. The main issues in existing IPsec solutions are listed as follows:

- Lack of access control: Access control plays a major role to ensure the confidentiality of the network. The existing IPsec tunnel mechanisms establish

**Table I.** Comparison of the proposed security architecture.

| Security feature | IPsec with Internet key exchange [23] | IPsec with Internet key exchange version 2 [24] | IPsec with Internet key exchange version 2 mobility multihoming protocol [25] | Host identity protocol [27] | Proposed Tunnel mode | Proposed Bound end-to-end tunnel mode |
|---|---|---|---|---|---|---|
| Denial of service/distributed denial of service attack protection | No | No | No | Yes | Yes | Yes |
| Eavesdropping attack protection | Yes | Yes | Yes | Yes | Yes | Yes |
| Spoofing attack protection | No | No | No | Yes | Yes | Yes |
| Replay attack protection | No | No | No | Yes | Yes | Yes |
| Access control and node authorization | No | No | No | No | Yes | Yes |
| Virtual private network-based traffic classification | No | No | No | No | Yes | Yes |
| Seamless mobility support | No | No | Yes | Yes | Yes | Yes |
| Dynamic tunnel establishment and automatic update | No | No | No | No | Yes | Yes |
| Coordinated tunnel establishments | No | No | No | No | Yes | Yes |

IPsec, Internet protocol security.

end-to-end tunnels and support only mutual authentication. It does not provide the access control to prevent unauthorized access to the network. Thus, existing IPsec tunnel mechanisms fail to offer the required confidentiality for mobile networks.

- Lack of protection over IP-based attacks: None of the existing IPsec solutions can protect the communication channel against the spoofing, replay, and man-in-the-middle attacks.
- Lack of traffic classification: The existing IPsec solutions establish end-to-end tunnels without any traffic classifications. However, LTE backhaul network transports various traffic types that need different service levels. Therefore, traffic classification (such as VPN-based traffic classification) is required for LTE backhaul networks.
- Distributed tunnel establishments: Legacy IPsec mechanisms establish tunnels independently in distributed manner. However, LTE backhaul network requires the coordination among the backhaul tunnels to prevent unauthorized access to backhaul and unnecessary tunnel establishments.

Therefore, it is clear that existing IPsec solutions cannot be implemented in LTE backhaul network. The proposed traffic architecture provides the required modification to implement IPsec tunneling-based secure traffic architecture in LTE backhaul networks.

Table I contains a comparison of the proposed architectures (tunnel and BEET mode VPN architectures) with the existing IPsec-based solutions.

Therefore, it is clear that we need a new IPsec tunnel architecture by modifying the operation of IPsec tunneling to implement in LTE backhaul networks. Such architectures should be able to provide not only the integrity but also the confidentiality, visibility, and the ability to coordinate via a centralized location. The proposed architectures satisfy these requirements.

## 3. RELATED WORK

Long-term evolution backhaul networks need to satisfy several LTE architectural requirements such as traffic transportation, mobility management, topology management, and security. These requirements are specified by 3GPP, and a summary of these requirements can be found in [7,8]. On the other hand, LTE architecture consists of an all-IP backhaul network. Hence, most of the operators have to move from an existing pure L2 (layer 2) topology to a full L3 (layer 3) topology. Furthermore, operators should adapt not only new network appliances but also new network technologies, especially new security technologies [5,6,8,12]. As a result, network operators encounter a number of migration challenges when they move from the existing 2G/3G backhaul to LTE backhaul. These challenges are discussed in [4,12,29,30].

The backhaul network security is one of the key challenges of the future LTE architecture [1,6,30]. Network appliance providers and operators identified that a secured LTE backhaul model is a crucial demand for the future LTE networks [1,6,7]. Basically, the mutual authentication of eNBs and IP attack prevention is required for steady operation of the LTE backhaul. Furthermore, 3GPP specification demands to encrypt data and signaling traffic that is transported via an untrusted network [1]. However, the existing backhaul architectures lack such security features. In [7], authors proposed to secure LTE backhaul traffic by using upper layer techniques. However, these upper layer solutions are vulnerable to L3 TCP/IP-based attacks such as TCP DoS [31], TCP reset [32], and IP spoofing attacks [33].

Multiple types of traffic are transported in LTE backhaul. Proper backhauling and providing different levels of QoS for these heterogeneous traffics are critical challenges for network operators. Various L2 and L3 VPN architectures can be used to overcome these issues [7,8]. In [8], authors compared the advantages and disadvantages of different L2/L3 VPN architectures. However, moving from a pure L2 topology to a full L3 VPN architecture has many advantages such as less provisioning complexity, high operational flexibility, and high network scalability [12].

Several techniques can be used to develop VPN models, and they can be categorized based on the operational layer of open systems interconnection model. Transport layer security (TLS) [34] and secure sockets layer (SSL) [35] based VPNs are capable of providing secure VPN service at application later. However, these VPN architectures are vulnerable lower-layer attacks [36].

Most of the L3 backhaul traffic architectures are developed based on multiprotocol label-switching protocol [7,37,38]. However, multiprotocol label-switching-based VPN models do not provide any security features like node authentication, data encryption, and privacy protection. On the other hand, the control protocol of these architectures is based on border gateway protocol and label distribution protocol. The control protocol is responsible to establish and maintain the VPN tunnels between the backhaul nodes. However, both label distribution protocol [39] and border gateway protocol[40] use insecure layer 4 TCP sessions that are vulnerable to TCP/IP-based attacks such as TCP DoS and TCP reset attacks [32].

Several other research articles proposed various mechanisms to enhance the security and resilience of different sections of LTE network [41–43]. In [41], authors propose a novel key derivation method to prevent eavesdropping attacks in LTE radio network. Security analysis of handover key management in LTE networks is presented in [43]. Lai *et al.* presented a unified end-to-end security scheme for machine-type communication in LTE networks in [42]. However, none of these security solutions provide a complete security framework to prevent IP-based attacks on LTE backhaul network.

# 4. INTERNET PROTOCOL SECURITY TUNNEL MODE VIRTUAL PRIVATE NETWORK ARCHITECTURE

## 4.1. Description of the architecture

The first proposed architecture is an L3 IPsec tunnel mode VPN. Figure 2 exhibits the protocol stack of the proposed architecture.

Here, two VPNs are used in this exemplary scenario, one VPN to deliver for the traffic towards the core network and other one for the X2 interface traffic. However, it is possible to define any number of backhaul VPNs according to the requirements of operator.

The proposed architecture dynamically and securely adds new nodes/devices to the backhaul network and establishes the secure VPN tunnels between them. The user and control backhaul traffic will be transported via these secure VPN tunnels. In this paper, we use the term "node" to represent a device in the LTE backhaul. Figure 3 illustrates the *nine steps* node addition and VPN tunnel establishment procedure of the proposed architecture.

In step 1, the network operator attaches the new node to the backhaul network. In step 2, he or she adds the node ID to the access control lists (ACLs). The proposed tunnel mode architecture uses authorization server (AS) for the access control. The mobile operator updates ACLs with the list of legitimate nodes for each VPN. These ACLs are used by AS to execute the access control decisions.

Thereafter, the new backhaul node is able to join the network after following the three procedures, namely, node authentication (steps 3–4), node authorization (steps 5–8), and tunnel establishment (step 9) procedures. Therefore, we propose a novel node addition procedure based on

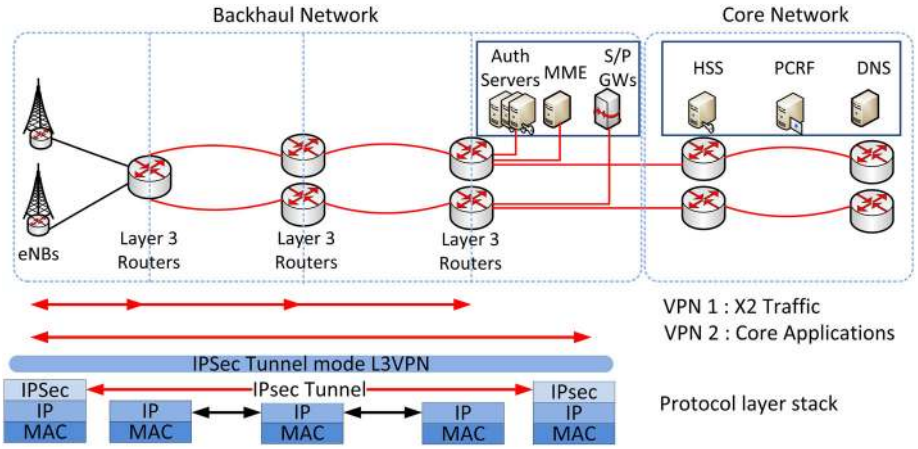


**Figure 2.** The protocol stack of Internet protocol security (IPSec)/Internet key exchange version 2 virtual private network (VPN). MME, mobility management entity; HSS, home subscriber server; PCRF, policy and charging rules function; DNS, domain name system; MAC, media access control; eNBs, evolved NodeBs.

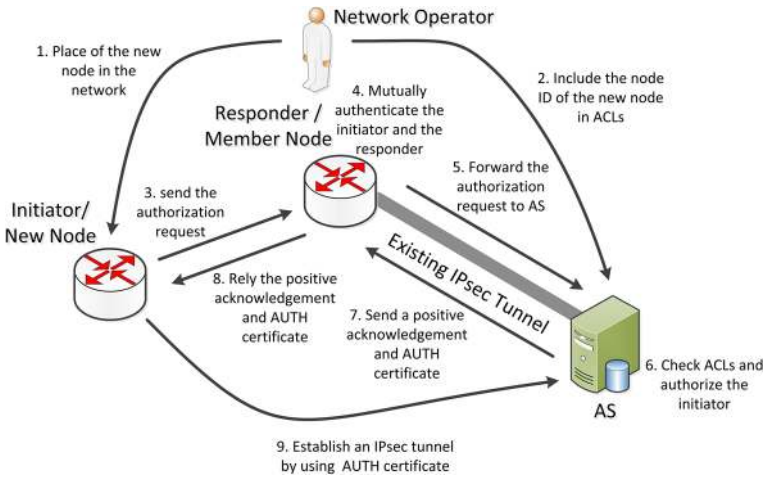


**Figure 3.** The flow of the dynamic node addition and tunnel establishment procedures. ACLs, access control lists; AS, authorization server; IPsec, Internet protocol security.

IKEv2 and novel tunnel establishment procedure based on MOBIKE to carry out the rest of the steps of the proposed procedure.

### 4.2. Node addition procedure

Node addition procedure is able to authenticate (steps 3–4) and authorize (steps 5–8) the new nodes. Figure 4 illustrates the proposed message exchange mechanism for node addition procedure. Here, the initiator is the potential node, and the responder is a member VPN node. A member VPN node is a legitimate node who already has access to the backhaul VPN. We use the same terminology, which was used in [24], and the proposed modifications are highlighted in Figure 4.

The procedure starts by sending INT1 message to a responder by the initiator (step 3).

M1: This initial INT1 message contains header (HDR), SA payloads, cryptographic key parameters, and a nonce. HDR contains the security parameter indexes (SPIs) of both nodes, the type of the next payload, version numbers, the message identifier (ID), and various flags [24].

*KEi* contains the initiator's parameters to generate a Diffie–Hellman (D-H) key.

M2: Upon the arrival of INT1 message, the responder sends RES1 message to the initiator without allocating any resources. RES1 message contains HDR, a cryptographic puzzle, a sequence number, and a cookie. The cryptographic puzzle protects the responder from DoS attacks. The task of the proposed puzzle is to find a solution *J*, which produces *K* number of zeros when it passed through SHA-1 hash function.

M3: Upon the arrival of RES1 message, the initiator sends an INT2 message that contains an HDR, the puzzle solution, SA payloads, cryptographic key parameters, a nonce, and the cookie. SA payload, HDR, and cryptographic key parameter are the same as in INT1, except that INT2 carries SPIs of both nodes in HDR parameters.

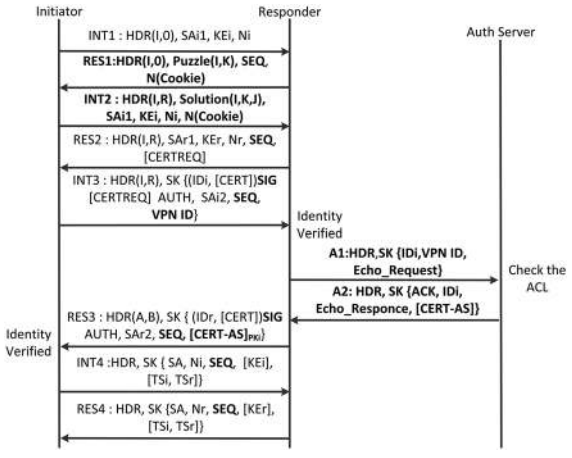


**Figure 4.** The Internet key exchange version 2 protocol-based message exchange mechanism for node addition procedure. ACL, access control list.

M4: Upon the arrival of INT2 message, the responder recalculates the cookie to verify the integrity of the puzzle and then checks the solution of the puzzle. Thereafter, the responder sends RES2 message that contains HDR, SA payload, cryptographic key parameters, a nonce, a sequence number, and a certificate request.

M5: The initiator sends INT3 message that contains an HDR, IDs, certificates, the authentication payload, a sequence number, and VPN ID. The initiator indicates the potential VPN ID in VPN ID field. Because the D-H key establishment is completed after the arrival of RES2 message, all payload sections are encrypted in INT3 other than HDR.

The identity of the initiator is verified after the arrival of INT3 message (step 4). Thereafter, the responder relays the initiator's credentials to AS in order to complete the authorization function. AS accepts only encapsulating security payload (ESP) packets that are transported through IPsec tunnels. Therefore, it is required to maintain an IPsec tunnel between each member VPN node and AS to support this authorization function.

M6: The responder sends A1 message that is encrypted and wrapped in ESP payload (step 5). A1 message contains an HDR, the identity of the initiator (*IDi*), VPN ID, and an echo request. The identity of the initiator and VPN ID are required to check against ACLs to authorize the initiator (step 6).

M7: After the validation of A1 message, AS sends an A2 message to the responder, which is also encrypted and wrapped in ESP payloads (step 7). A2 message contains an HDR, an acknowledgment, the ID of the initiator, the echo request, and a certificate. If the potential node is a legitimate node for the VPN, AS sends an A2 packet with a positive acknowledgment. A positive acknowledgment grants the access to the VPN. If the potential node is not a legitimate node, then a negative acknowledgment is sent, and the responder discards the connection request from the initiator. The certificate is signed by AS. This certificate is used by the initiator to establish IPsec tunnels with peer nodes in the same VPN.

M8: Upon the reception of a positive acknowledgment from AS, the responder sends RES3 message to complete the initial exchange procedure (step 8). RES3 message contains an HDR, ID of the responder, the responder's certificates, an authentication payload, a sequence number, and AS's certificate.

M9: Thereafter, the initiator sends INT4 message to create a child SA for the IPsec tunnel. It contains an SA payload, a nonce, a sequence number, and cryptographic key parameters.

M10: Then, the responder sends RES4 message to complete the creation of the child SA. RES4 has similar obligatory fields as INT4.

The proposed BEX provides higher level of security than IKEv2 because our procedure contains all security mechanisms that are present in IKEv2 and few extra

security features such as cryptographic puzzles, echo requests, sequence counters, and certificates to avoid replay and DoS attacks. In contrast to the original IKEv2 protocol, the proposed message exchange mechanism not only authenticates the node but also authorizes the node based on its node ID. Moreover, the novel message exchange mechanism enhances the DoS attack resilience of the system.

### 4.3. Tunnel establishment

Every member VPN node has two responsibilities related to the VPN management, namely, support node authorization function (i.e., steps 5 and 7) and data traffic forwarding. These functions required to establish separate IPsec tunnel instances.

First, the node authorization procedure needs an IPsec tunnel between the member VPN node and AS (step 9). Hence, first task of a newly joined node is to establish an IPsec tunnel with AS. Second, we propose an encrypted data communication mechanism for LTE backhaul. Hence, an IPsec tunnel establishment is mandatory prior to any kind of communication between other backhaul devices.

We propose a novel tunnel establishment procedure based on MOBIKE protocol. Here, we propose to use MOBIKE instead of IKEv2, because MOBIKE protocol provides additional multihoming and mobility support for end nodes. It is a requirement of some LTE backhaul nodes such as vehicular and mobile femtocells [26].

Figure 5 illustrates the proposed message exchange mechanism for IPsec tunnel establishment. We use the same terminology that was used in [24,25], and the proposed modifications are highlighted in Figure 5.

The format of INT1, RES1, INT2, RES2, INT4, and RES4 message exchanges is similar to the corresponding message exchanges in the previously described node addition procedure (Figure 4). Here, the initiator sends an authentication token (Auth-token) instead of VPN ID in INT3 in contrast to the previous INT3 message. In INT3 and RES3 messages, nodes exchange the Auth-tokens and the format of an Auth-Token as follows:

$$Auth - Token = Hash(Certificate - AS \mid IDi \mid IDr) \quad (1)$$

*IDi* and *IDr* are the identities of the initiator and the responder. *Certificate – AS* is the certificate that is received during the node addition phase. An intruder cannot establish an IPsec tunnel with a legitimate member VPN node without a valid Auth-token.

Furthermore, both INT3 and RES3 messages contain N(MOBIKE_SUPPORTED) payload to notify that both peers are supporting MOBIKE specification. Finally, N(ADDITIONAL_ADDRESSES) payload contains the set of addresses available for each peer that can change during the lifetime of SA without terminating the IPsec tunnel.

The proposed message exchange provides a higher level of security than MOBIKE protocol. Our procedure contains all the security mechanisms that are available in MOBIKE and contains extra security features such as cryptographic puzzles, echo requests, sequence counters, and certificates to avoid replay and DoS attacks.

Tunnel establish procedures for both node authorization function and data traffic forwarding are almost similar. However, we propose to use ingress filter before AS for extra protection. The ingress filter drops all the connection requests from unauthenticated nodes. Once a node is authenticated, AS updates the filter list. This will prevent the unauthorized connection requests and potential DoS attacks (resource consuming) on AS.

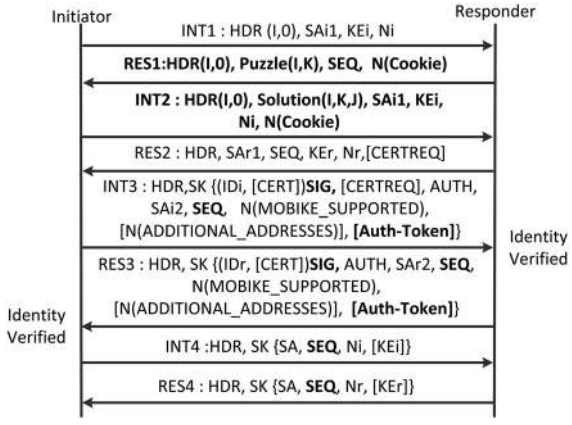


**Figure 5.** The Internet key exchange version 2 mobility and multihoming protocol-based message exchange mechanism for tunnel establishment.

## 5. INTERNET PROTOCOL SECURITY BOUND END-TO-END TUNNEL MODE VIRTUAL PRIVATE NETWORK ARCHITECTURE

### 5.1. Description of the architecture

The second proposed architecture is an L3 VPN architecture based on HIP. It proposes to create IPsec BEET mode tunnels on top of the backhaul network.

The underline protocol stack of IPsec BEET mode VPN architecture is illustrated in Figure 6. We interchangeably called IPsec BEET mode VPN architecture as HIP VPN architecture in the rest of the paper.

Internet protocol security BEET mode VPN architecture also allows to dynamically add new nodes to the backhaul network. It also follows the nine steps, the node addition, and tunnel establishment procedures that is shown in Figure 3.

In step 1, the network operator attaches the new node to the backhaul network, and he or she updates the node ID to ACLs in step 2. Thereafter, the new backhaul node is able to join the network after following the three procedures, namely, node authentication (steps 3–4), node

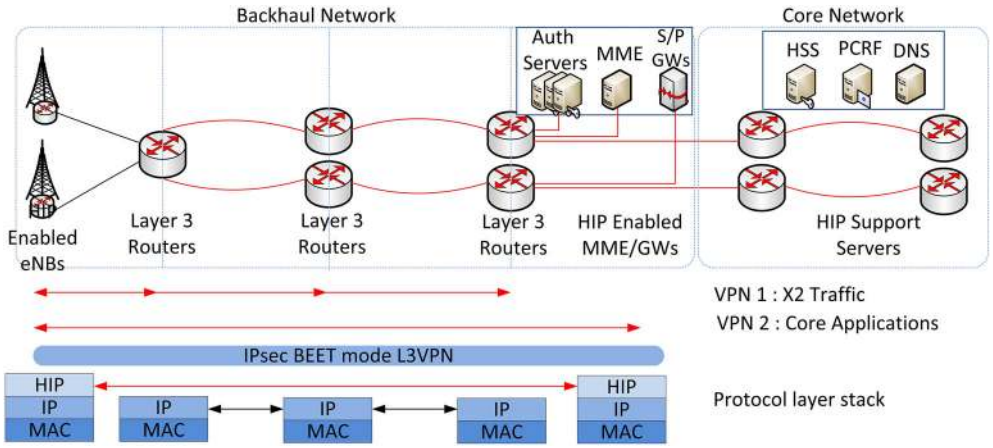


**Figure 6.** The protocol stack of Internet protocol security (IPsec) bound end-to-end tunnel (BEET) mode virtual private network (VPN) architecture. MME, mobility management entity; HSS, home subscriber server; PCRF, policy and charging rules function; DNS, domain name system; eNBs, evolved NodeBs; HIP, host identity protocol; MAC, media access control.

authorization (steps 5–8), and tunnel establishment (step 9). Therefore, we propose a novel node addition procedure and novel tunnel establishment procedure based on HIP to carry out the rest of the steps of the proposed procedure.

## 5.2. Node addition procedure

Node addition procedure is able to authenticate (steps 3–4) and authorize (steps 5–8) the new nodes. Figure 7 illustrates the proposed BEX procedure for node addition procedure. Here, the initiator is the potential node, and the responder is a member VPN node. We use the same terminology that was used for HIP BEX in [27], and the proposed modifications are highlighted in Figure 7.

M1: The first message (I1) contains only HITs of the initiator and responder. It triggers the BEX procedure (step 3).

M2: Upon the arrival of I1 message, the responder sends R1 message to the initiator. R1 message contains a cryptographic puzzle, D-H key parameters, the public key of the responder, ESP transforms, HIP transforms, an echo request, a sequence number, and a signature. The cryptographic puzzle avoids DoS attacks. The responder does not allocate any resource for the initiator until the arrival of the correct solution for the puzzle in I2 packet. D-H key parameters are used to generate a symmetric key for ESP payload encryption.

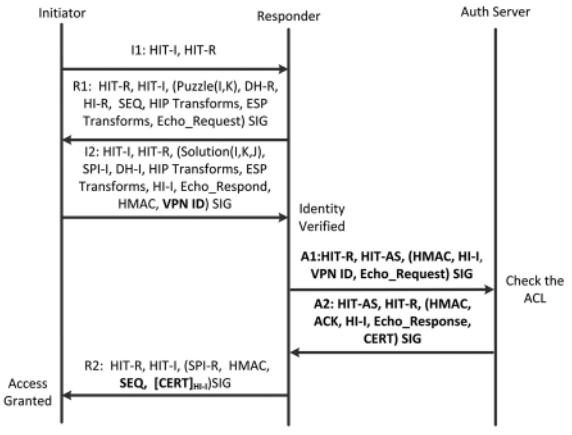


**Figure 7.** The base exchange procedure for node addition procedure. ACL, access control list.

M3: After the arrival of R1 message, the initiator sends I2 message that contains hash message authentication code (HMAC), the solution to the puzzle, encrypted D-H key parameters, the public key of the initiator, ESP transforms, HIP transforms, SPIs, the echo reply, VPN ID, and a signature. I2 has similar obligatory fields as R1, except that the puzzle parameter contains the solution.

The identity of the initiator is verified after the arrival of the I2 message (step 4). Then, it is a duty of the responder to relay the initiator's credentials to AS in order to complete the authentication function. AS only accepts ESP packets that are transported through HIP tunnels. Therefore, it is required to maintain an HIP tunnel between each member VPN node and AS to support such an authentication function.

M4: The responder sends A1 message that is wrapped within the ESP payload (step 5). A1 message has same format as I1, R1, and I2, except it is encrypted and wrapped in ESP payload. It contains HMAC, HIT of the initiator, an echo request, VPN ID, and a signature. HIT of the initiator and VPN ID are checked with ACLs to authorize the initiator (step 6).

M5: After the validation of A1 message, AS sends an A2 message to the responder, which is also encrypted and wrapped in ESP payload (step 7). A2 message contains HMAC, an acknowledgment, HIT of the initiator, the echo reply, a certificate, and a signature.

M6: Upon the reception of a positive acknowledgment, the responder sends R2 message to complete the BEX procedure (step 8). R2 message contains HMAC, SPIs, the

encrypted certificate, a sequence number, and a signature. The responder completes SPI agreement by sending its SPI in R2. Also, it relays the certificate that is issued by AS. It is encrypted by using the public key of the initiator. The sequence number contains the monotonically increasing "R2 generation counter" value that is used to protect the initiator from R2 messages-based replay attacks.

Similar to the original HIP BEX, the proposed BEX procedure is capable to mutually authenticate nodes based on public key infrastructures, establish SAs for IPsec communication, negotiate keys for encryption, prevent DoS, and replay attacks. Thus, the proposed BEX provides the similar level of security as the original HIP BEX because our procedure contains all the security mechanisms, which are available in HIP BEX. In addition to the features of the original HIP protocol, the proposed message exchange mechanism is able to authorize the node based on its node HI. The proposed exchange mechanism is somewhat longer than original HIP BEX and adds extra overhead because of new A1 and A2 message exchanges. However, it will not effect significantly to the overall performance because the authorization phase will be called only once for each node.

### 5.3. Tunnel establishment

Every member VPN node has two responsibilities related to the VPN management, namely, support node authorization function (i.e., steps 5 and 7) and data traffic forwarding. These functions required two separate IPsec tunnel instances.

First, the node authorization procedure needs an IPsec tunnel between the member VPN node and AS (step 9). Hence, the first task of a newly joined node is to establish an IPsec tunnel with AS. Second, we propose an encrypted data communication mechanism for LTE backhaul. Hence, an IPsec tunnel establishment is mandatory prior to any kind of communication between two nodes.

We propose a novel exchange procedure for these HIP tunnel establishment instances. Similar to the previous authentication phase, this procedure is also based on HIP BEX [27]. Figure 8 illustrates the proposed BEX procedure for HIP tunnel establishment.

The format of the message exchanges is similar to the corresponding messages in the BEX procedure of the node addition phase. However, the initiator sends an Auth-token instead of VPN ID in I2 in contrast to the previous I2 message. In I2 and R2 messages, nodes exchange the Auth-tokens and the format of an Auth-Token as follows:

$$Auth-Token = Hash(Certificate-AS \mid HI-I \mid HI-R) \quad (2)$$

$HI-I$ and $HI-R$ are the identities of the initiator and the responder. $Certificate-AS$ is the certificate that is received during the node addition phase. An intruder cannot establish an IPsec tunnel with a legitimate member VPN node without a valid Auth-token.

Tunnel establish procedures for both node authorization function and data traffic forwarding are almost similar. However, we propose to use ingress filter before AS for extra protection. The ingress filter drops all the connection requests from unauthenticated nodes. Once a node is authenticated, AS updates the filter list. This will prevent the unauthorized connection requests and potential DoS attacks (resource consuming) on AS.

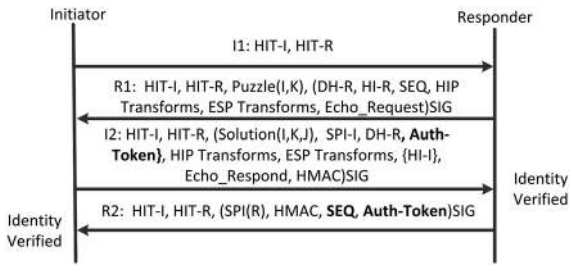


**Figure 8.** The base exchange procedure for host identity protocol tunnel establishment.

## 6. PROTECTION FROM INTERNET PROTOCOL-BASED ATTACK

The proposed VPN architectures are simulated on OMNET++ and conducted several extended simulations to study the performance under DoS, DDoS, TCP reset, and IP spoofing attacks. 3GPP specifications [1–3] have specified the requirements of IPsec in order to protect some of the backhaul interfaces. However, present mobile services achieve the end-to-end security at the application level [7,8]. Thus, we use a TLS/SSL VPN as our reference model here. TLS/SSL VPN is a layer 4 secured VPN that provides end-to-end security at the application layer. Similar to the existing LTE backhaul traffic architectures, it does not provide any L3 protection.

### 6.1. Impact of denial of service/distributed denial of service attack

Transmission control protocol synchronization (SYN) packet flooding attack is used to model DoS attack. Our system model contains a single VPN that has 60 nodes and a server. Nodes are randomly connected with other nodes with maximum of four neighbors. All nodes upload data traffic to the server, and this server is under attack. We use an application server here. This application server will represent any of the backhaul core network element such as MME, P/GW, or AS. The attacker (TCP packet generator) sends forged TCP SYN packets to the server by changing the port number and the source IP address (one change per packet). The server allocates one server port for every successfully arrived SYN packet. As the TCP timeout value is 270 s [31], such an attacked port will not be released until the TCP timeout expires. Likewise, the attacker occupies all ports (64,000 per IP address) [31].

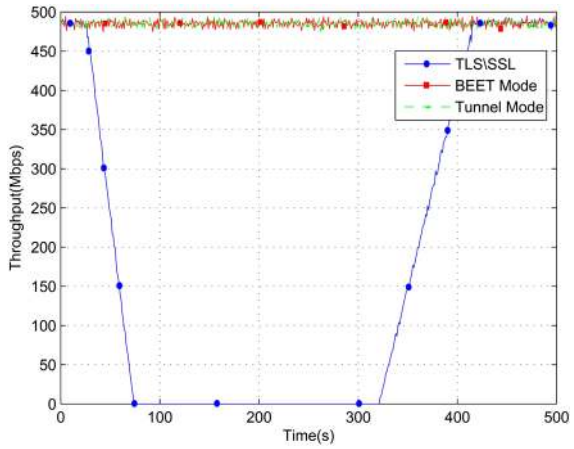


**Figure 9.** Impact of transmission control protocol synchronization denial of service attack. TLS, transport layer security; SSL, secure sockets layer; BEET, bound end-to-end tunnel.

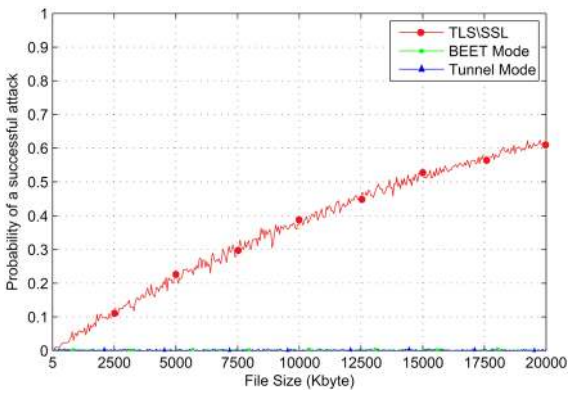


**Figure 10.** Impact of transmission control protocol reset attack. TLS, transport layer security; SSL, secure sockets layer; BEET, bound end-to-end tunnel.

The LTE backhaul bandwidth is set to 500 Mbps, and attackers have 100 Mbps connection. The simulation runs for 500 s, and the attack is placed from 25 to 125 s.

In the first experiment, we use only one attacker. According to Figure 9, we observe that proposed VPN architecture has no significant throughput drop during the attack period. It achieves the maximum throughput similar to the non-attacking period. However, TLS/SSL VPN has almost 0 throughput during the DoS attack. TLS/SSL VPN takes at least the duration of a TCP timeout in addition to the attack duration to fully recover from the attack.

## 6.2. Impact of transmission control protocol reset attack

The TCP reset attack is an IP-based attack where an attacker sends fake TCP packets to end points by setting the reset bit to 1. However, the attacker must include correct IP addresses, port numbers, and a valid sequence number in the packet header. Once these fake TCP packets match all these parameters, end-point nodes reset the ongoing TCP connection [32].

If the attacker eavesdrops the ongoing TCP session traffic, he or she can learn about IP addresses and TCP port. Now, the attacker needs to know only the sequence number. In such a case, the attacker sends fake TCP packets (with no payload) by increasing the sequence number until it resets the attacked TCP connection. For each packet, the sequence number is increased by a window size that is 16,384 (typical value for Cisco routers) [32]. Otherwise, the attacker has to randomly guess all the parameters. Thus, we use TCP reset attack to illustrate the impact of eavesdropping attacks. In our experiment, the attacker has the same bandwidth (500 Mbps) as other nodes.

The probability of successful attack (Figure 10) is calculated against the file size. By considering the file sizes in the Internet, it is found that the minimum file size is 4.5 KB, and the maximum size is 20 MB [44].

Because the attacker cannot eavesdrop the IP addresses and port numbers from the ESP payload, proposed VPN architecture has minimum/no effect from TCP reset attack. Thus, the proposed architecture has zero probability to be attacked. However, the probability of a successful attack for the TLS/SSL VPN increases with the file size. A TLS/SSL VPN is lacking of encryption at L3. Hence, the attacker learns all the parameters by eavesdropping the VPN session. He or she needs to find only the correct sequence number, and larger file sizes provide more time (higher transmission time) for the attacker to guess the correct sequence number parameters to reset the connection falsely.

## 6.3. Impact of Internet protocol spoofing attack

During an IP spoofing attack, the attacker generates IP packets with forged IP address to impersonate as a legitimate node [33]. There are three common types of IP spoofing attacks, namely, random spoofing, subnet spoofing, and fixed spoofing [45]. In random spoofing attacks, the attacker generates IP packets with randomly generated 32-bit numbers as IP addresses. In subnet spoofing attacks, the attacker uses IP addresses that are taken from the address space corresponding to the network subnet. In fixed spoofing attacks, the attacker selects IP addresses from a given list. It is a subset of subnet spoofing attacks.

In this experiment, we simulate random spoofing and subnet spoofing attacks. Here, we use the same simulation model for previous experiments. In this experiment, the attacker has the same bandwidth (500 Mbps) as other nodes.

The simulation results (Figure 11) verify that TLS/SSL VPN architecture is vulnerable to both subnet and random spoofing attacks. By utilizing an ingress filter, the server drops the connection request outside the subnet address

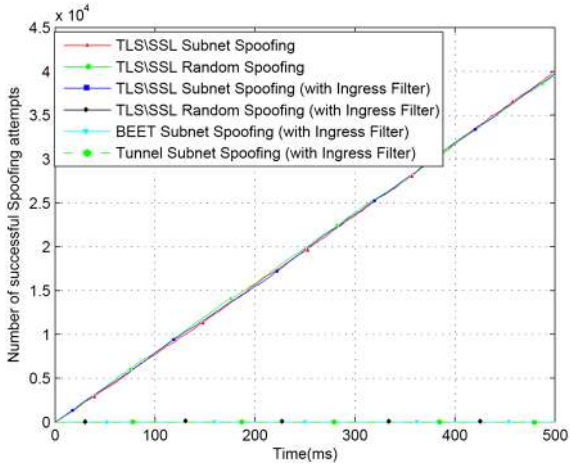


**Figure 11.** Impact of Internet protocol spoofing attack. TLS, transport layer security; SSL, secure sockets layer; BEET, bound end-to-end tunnel.

space. It significantly reduces the impact of random spoofing attacks. However, TLS/SSL VPN is still vulnerable to subnet spoofing attacks even with ingress filters.

On the other hand, proposed architecture has no effect from both IP spoofing attacks. As we have similar results for all the tests, we present results-related subnet spoofing attacks with the ingress filter scenario only.

# 7. SECURITY ANALYSIS

In this section, we analyze security features of proposed VPN architectures.

## 7.1. Protection against denial of service and distributed denial of service attacks

Denial of service attacks are the most common IP-based attack scenarios in IP-based networks. In most DoS attacks, attackers send an extensive amount of connections requests (e.g., TCP SYN requests). However, they will not continue the rest of the steps or message exchanges. In LTE backhaul, a compromise eNB can try to overload an MME or PGW by sending lots of connection establishment requests [5]. However, our architectures propose to establish an IPsec tunnel before the communication. These tunnel establishments are protected from DoS and DDoS attacks.

If attackers send a series of INT1 packets in tunnel mode architecture, the responder replies with RES1 packet for each INT1 without allocation of any resources such as memory space and port. Each RES1 contains a precomputed puzzle, and it increases the commitment requirement of the attacker. Furthermore, the responder does not spend any extra processing power other than the processing of a general packet. Even a simple switch can handle thousands of connection requests (e.g., 1 Gbps switch can process 1,488,095 packets per second). Thus, the impact of the first INT1 is negligible although the responder sends an RES1 message for every INT1 request.

If attackers send a series of I1 packets in BEET mode architecture, the responder replies with R1 packet for each I1 without allocation of any resources such as memory space and port. Each R1 contains a precomputed puzzle, and it increases the commitment requirement of the attacker.

However, our architecture does not prevent volume-based DoS attacks such as user datagram protocol floods, Internet control message protocol floods, and other spoofed-packet floods. In volume-based DoS attacks, the attackers dump excessive amount of junk traffic to overload the network links. Such attacks can be easily prevented by implementing firewalls, ingress filtering, and enforcing rate bounds [46,47]. These security solutions are independent of our architecture, and we recommend to implement them in the backhaul network. Moreover, filtering mechanisms are commonly used in almost all the network because volume-based DoS attacks are very common in present networks.

## 7.2. Protection against replay attacks

Replay attacks are possible at three stages such as data communication, node addition, and tunnel establishment phases.

Both architectures use IPsec ESP mode for the data communication. IPsec ESP mode utilizes sequence numbers to protect the messages against the replay attacks. A sequence number is assigned for each IPSec packet, and it is monotonically increasing. Any IPsec packet without a proper sequence number will be dropped by nodes. If an intruder tries to replay an IPSec-encrypted packet, then the sequence number will not fit because the counter values have already increased by the original packets.

During the node addition and tunnel establishment phases, tunnel mode architecture uses the following mechanisms against replay attacks. Virtue of the stateless response to INT1 messages with pre-calculated RES1 messages is used to protect responders against attacker's replays of INT1 messages. A monotonically increasing "RES1 generation counter", which is included in RES1, is used to protect the initiator from RES1 replays. RES1 generation counter is a 64-bit counter, and it can be initialized to any value randomly. Again, responders are protected against attacker's replays of INT2 messages by using the puzzle mechanism and cookies. Both puzzle and cookies use time stamps to avoid replay attacks. Similar to the "RES1 generation counter", the rest of the messages, namely, RES2, INT3, RES3, INT4, and RES4, use similar counter mechanism to avoid the replay attacks.

Bound end-to-end tunnel mode architecture uses the following mechanisms to prevent replay attacks during the node addition and tunnel establishment phases. Virtue of the stateless response to I1s with pre-calculated R1 messages is used to protect responders against attacker's

replays of INT1 messages. A monotonically increasing "R1 generation counter", which is included in R1, is used to protect the initiator from R1 replays. Again, responders are protected against attacker's replays of I2 messages by using the puzzle mechanism and optional use of opaque data. Finally, a monotonically increasing "R2 generation counter", which is included in R2, is used to protect the initiator from R2 replays. Moreover, the use of less expensive HMAC verification preceding HIP signature verification also provides the additional replay attack protection for I2, R2, A1, and A2 messages.

Both architectures use IPsec ESP mode messages to deliver A1 and A2 messages. These messages are protected from the sequence number-based replay-attack prevention mechanism of IPsec ESP mode tunnels.

### 7.3. Protection against Internet protocol spoofing attacks

One method of preventing IP spoofing attacks is to verify the node identity behind the IP address. Both architectures use strong node authentication mechanisms based on public key authentication. Proposed mutual authentication mechanisms use node IDs (trusted certificate or cryptographic key) to prove the identity of the node than the IP address. Thus, mutual authentication mechanisms are capable to verify identity of the entity behind the IP address.

In addition, both architecture uses signature to sign messages with the private key of the node. This signature also reveals spoofed identifiers.

### 7.4. Protection against eavesdropping attacks

Active attackers eavesdrop the ongoing communication channels and use the gathered information to perform various attacks such as IP spoofing, TCP reset, and replay attacks. Among them, TCP reset attack is the most common IP-based attack on TCP sessions. Here, we use the TCP reset attack scenario as a reference to illustrate the impact of eavesdropping attacks. On the other hand, we already discuss the protection against IP spoofing and replay attacks.

The first step in a TCP reset attack is to eavesdrop the ongoing TCP session and extract the TCP header information to perform the reset attack. An attacker needs to find five header fields to perform the reset attack. Those parameters are the source IP address (32 bits), the destination IP address (32 bits), the source port (16 bits), the destination port (16 bits), and a matching sequence number (32 bits) [32]. If the attacker is able to successfully eavesdrop an ongoing TCP session, he or she can collect four parameters, that is, IP addresses and ports. Then, he or she has to guess only a sequence number (32 bits).

In [32], authors mathematically analyze the TCP reset attack scenarios. In this case, the average time that is required to reset a TCP connection can be calculated as follows:

$$Time = \frac{SequenceNumberRange}{WindowSize} * \frac{PacketSize}{DataRate} \quad (3)$$

By using the typical values (window size = 65,535, data rate = 500 Mbps, and packet size = 320 bits) [32], the average time that is required to reset a TCP connection is below 50 ms.

However, both architectures use IPsec ESP mode messages, and all TCP header information is encrypted. Therefore, the attacker cannot eavesdrop the TCP header information, and the attacker has to guess not only a sequence number but also other four parameters. In this case, the average time that is required to reset a TCP connection is over 2 months. Thus, the data communication is protected from TCP reset attacks.

Moreover, simulation results (Section 6) verify that proposed architectures are protected from TCP reset attacks.

### 7.5. The protection of the authorization server

A new node cannot initiate a direct communication session with AS. Every new node including a potential attacker has to pass two authentication steps to communicate with AS. First, an outsider has to connect an existing member VPN node to gain the access to a VPN. Then only, he or she can establish an IPsec tunnel with AS. However, these two steps are secured by strong public key infrastructure authentication and authorization procedures. Hence, AS is double protected compared with any other backhaul node.

However, if the attacker is anyhow able to compromise an authenticated node (a member VPN node), then the attacker can send an excessive amount of requests. To prevent such situations, we propose to utilize an ingress filter with rate bound limits. AS sets a rate bound for each member node. Once the node's traffic flow has reached to this rate bound limit, AS resets the connection with the node. In that way, AS can easily terminate the communication with jeopardized nodes.

Because this paper only addresses the security issues in LTE backhaul network, the proposed security mechanisms are sufficient enough to secure AS from the IP-based attacks that are originated within the backhaul network. Furthermore, we propose to use a logically centralized distributed AS system to avoid the single point of failure.

## 8. PERFORMANCE ANALYSIS

### 8.1. The impact on file transmission delay

We investigate the performance penalty on the file transmission delay of the proposed architectures. Three nodes are used for the simulation as the initiator, the responder,

and the AS. We compare the performance under three scenarios, namely, (1) the tunnel is already established between the initiator and responder; (2) the initiator is authenticated and authorized, but no tunnel is established; and (3) the initiator is not even authenticated.

We change the file sizes from 5 KB to 20 MB by considering the file sizes in the Internet [44]. The bandwidth of the connections between the nodes is set to 100 Kbps. Figure 12 illustrates the transmission delay of the BEET architecture as a percentage of the transmission delay of non-secure traffic (without any encryption).

$$DelayPercentage = \frac{Delay_{VPN} - Delay_{NonSecure}}{Delay_{NonSecure}} * 100\% \quad (4)$$

According to simulation results in Figure 12, BEET mode VPN has similar performance as the original HIP with the presence of already established tunnels. Hence, we can conclude that the proposed changes do not affect the performance of HIP at the steady state operation of VPN.

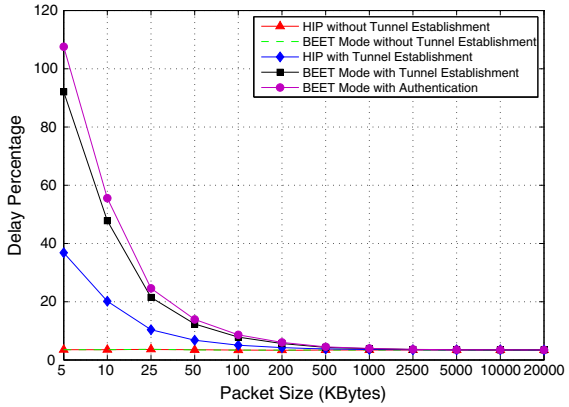


**Figure 12.** The impact on file transmission delay on bound end-to-end tunnel (BEET) mode tunnel virtual private network. HIP, host identity protocol.

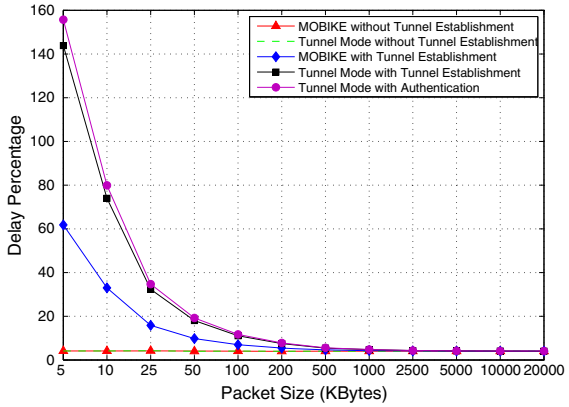


**Figure 13.** The impact on file transmission delay on tunnel mode tunnel virtual private network. MOBIKE, Internet key exchange version 2 mobility and multihoming protocol.

Furthermore, the tunnels establishment and node addition (node authentication and authorization) phase have deficient performance than the original HIP. However, the difference between HIP and the BEET mode VPN tunnels is gradually decreasing with the increment of file size. Hence, we can conclude that the performance penalty due to tunnels establishment and node addition phases can be compensated by keeping the established tunnels for a longer period.

According to the simulation results in Figure 13, the tunnel mode VPN has similar performance as the original MOBIKE with the presence of already established tunnels. Hence, we can conclude that the proposed modifications do not affect the performance of the MOBIKE protocol at the steady state operation of VPN. Furthermore, the tunnels establishment and node addition phases have inefficient performance than the original MOBIKE protocol. However, the difference between MOBIKE protocol and the tunnel mode VPN tunnels is gradually decreasing with the increment of file size. Hence, this performance penalty can be compensated by keeping the established tunnels for a longer period.

## 8.2. The impact on file transmission overhead

We investigate the performance penalty on the throughput of proposed architecture by measuring the impact on file transmission overhead. Three nodes are used for the simulation as the initiator, the responder, and the AS. We compare the performance under the same three scenarios as the previous experiment.

Figure 14 illustrate the total overhead for the BEET mode VPN architecture as a percentage of the file size.

$$OverheadPercentage = \frac{TotalOverhead}{FileSize} * 100\% \quad (5)$$

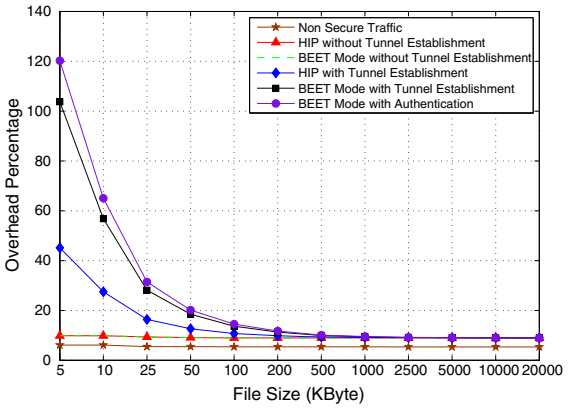


**Figure 14.** The performance penalty of security on throughput of bound end-to-end tunnel (BEET) mode architecture. HIP, host identity protocol.

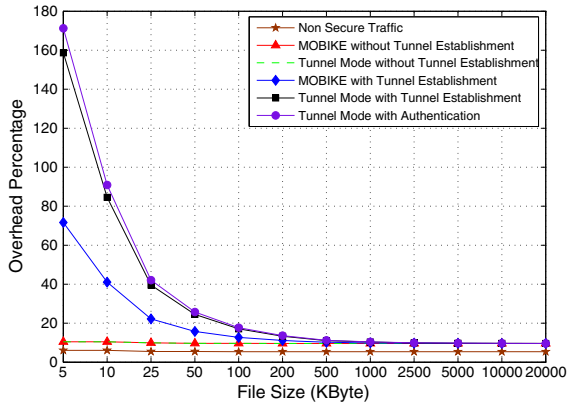


**Figure 15.** The performance penalty of security on throughput of tunnel mode architecture.

According to the simulation results in Figure 14, the BEET mode VPN has similar performance as the original HIP with the presence of already established tunnels. Hence, we can conclude that the proposed modifications do not affect the performance of HIP at the steady state operation of the VPN. Furthermore, both HIP tunnels and BEET mode VPN tunnels increase the overhead only by 3.8% at steady state operation. Thus, the overhead penalty at steady state operation is less significant for the BEET mode VPN architecture compared with the non-secure scenario.

However, the tunnel establishment and node addition phases add extra overhead to the BEET mode VPN tunnels. This extra overhead between HIP and the BEET mode VPN tunnels is gradually decreasing with the increment of file sizes. Hence, this performance penalty can be compensated by keeping the established tunnels for a long period.

According to the simulation results in Figure 15, the tunnel mode VPN has similar performance as the original MOBIKE with the presence of already established tunnels. Hence, we can conclude that the proposed modifications do not affect the performance of MOBIKE at the steady state operation of the VPN. Furthermore, both MOBIKE and tunnel mode VPN tunnels increase the overhead only by 4.4% than non-secure scenario. Thus, the overhead penalty at steady state operation is very low in tunnel mode architecture.

However, the tunnel establishment and node addition phases add extra overhead for the tunnel mode VPN tunnels. This extra overhead between MOBIKE and the tunnel mode VPN tunnels is gradually decreasing with the increment of file size. Hence, this performance penalty can be compensated by keeping the established tunnels for a longer period.

# 9. DISCUSSION

## 9.1. Comparison of Internet protocol security tunnel mode and Internet protocol security bound end-to-end tunnel mode virtual private networks

Internet protocol security BEET mode VPN architecture anticipates several benefits than IPsec tunnel mode architecture. First, a single HI can represent several physical/logical interfaces with different IP addresses. Hence, multihomed nodes can obtain advantages such as high throughput and extra security for packet sniffing attacks by using proper load-balancing mechanisms. Second, HIP supports the "rendezvous" mechanism. It helps to provide automatic redundancy support in the event of two simultaneous network outages that can occur at both ends of the tunnels. Third, the BEET mode VPN architecture has better performance in the tunnel establishment phase and the node addition phase than IPsec tunnel mode VPN architecture. Fourth, a HIP-enabled backhaul architecture can be used to provide new services for mobile networks, for example, L2-secured automatic virtual private local area network service for mobile nodes [48].

Although BEET mode VPN architecture provides many advantages compared with the IPsec tunnel mode VPN, it has a very high initial capital cost. BEET mode VPN architecture requires new HIP-enabled backhaul network elements such as switches, routers, eNBs, MMEs, ASs, servers, and S-GWs. Hence, network appliance providers have to develop new HIP-enabled equipments, and an operator has to implement these new network appliances in their network. This is a protracted and expensive process. However, most of the existing network element supports IPsec tunnel mode VPN architecture. Hence, operators can deploy it with a minimum initial cost by using existing network appliances.

# 10. CONCLUSION

We presented two secure VPN-based traffic architectures for the LTE backhaul network. The proposed architectures are L3 IPsec VPNs based on MOBIKE and HIP. We proposed novel BEX procedures to authenticate and authorize new nodes and novel tunnel establishment procedures to establish secure VPN tunnels between LTE backhaul devices. The proposed architectures secure the backhaul traffic by satisfying the LTE backhaul security requirements, namely, node authentication, node authorization, payload encryption, privacy protection, and IP-based attacks prevention.

The security analysis and simulation results verified that proposed architectures provide a secured backhaul traffic transportation during TCP SYN DoS, TCP reset, and IP spoofing attacks. Furthermore, proposed VPN architectures have similar performance penalty of security as original protocols, that is, MOBIKE and HIP in the steady state of operation and the availability of long-lasting tunnel establishments.

This research forms the base for several future research topics, namely, develop a secure distributed authentication server architecture for the LTE backhaul, study the impact of mobile backhaul nodes such as mobile femtocells to the VPN architecture, and study an optimum load-balancing mechanisms for multihomed nodes. Moreover, we are focusing to extended these architectures

to provide additional load balancing, automatic redundancy, and best path-routing features in future mesh backhaul networks.

## ACKNOWLEDGEMENTS

This work has been performed in the framework of the CELTIC project CP2012 SIGMONA. The authors would like to acknowledge the contributions of their colleagues. This information reflects the consortium's view, but the consortium is not liable for any use that may be made of any of the information contained therein. This research was supported in part by TEKES, Finland and the Russian Fund for Basic Research (RFBR) according to the research project # 14-07-00252.

## REFERENCES

1. 3GPP system architecture evolution (SAE); security architecture—3GPP TS 33.401 release 12, 2013. (Available from: http://www.3gpp.org/ftp/Specs/html-info/33401.htm) [Accessed on 30 December 2015].
2. 3G security; network domain security (NDS); IP network layer security—3GPP TS 33.210 release 12, 2014. (Available from: http://www.3gpp.org/DynaReport/33210.htm) [Accessed on 30 December 2015].
3. Network domain security (NDS); authentication framework (AF)—3GPP TS 33.310 release 12, 2014. (Available from: http://www.3gpp.org/DynaReport/33310.htm) [Accessed on 30 December 2015].
4. Bikos AN, Sklavos N. LTE/SAE security issues on 4G wireless networks. *IEEE Magazine on Security & Privacy* 2013; **11**(2): 55–62.
5. Cao J, Ma M, Li H, Zhang Y, Luo Z. A survey on security aspects for LTE and LTE-A networks. *Communications Surveys & Tutorials, IEEE* 2014; **16**(1): 283–302.
6. Alvarez MA, Jounay F, Volpato P. Security in LTE backhauling. *Technical Report*, Next Generation Mobile Networks Alliancen, 2012.
7. Alvarez MA, Jounay F, Major T, Volpato P. LTE backhauling deployment scenarios. *Technical Report*, Next Generation Mobile Networks Alliancen, 2011.
8. Architectural considerations for backhaul of 2G/3G and long term evolution networks. *Technical Report*, CISCO Cooperation, 2010.
9. 3G/LTE mobile backhaul network MPLS-TP based solution. *Technical Report*, UTStarcom, Inc, 2009.
10. Liyanage M, Ylianttila M, Gurtov A. IP-based virtual private network implementations in future cellular networks. *Handbook of Research on Progressive Trends in Wireless Communications and Networking* 2014; **1**: 44.
11. Liyanage M, Gurtov A. Secured VPN models for LTE backhaul networks, *Vehicular Technology Conference (VTC fall), 2012 IEEE*, IEEE, Quebec City, Canada, 2012; 1–5.
12. LTE backhaul—security imperative. *Technical Report*, Stoke, Inc, 2013.
13. Forsberg D, Horn G, Moeller WD, Niemi V. *LTE Security*, Vol. 1. John Wiley & Sons: West Sussex, United Kingdom, 2012.
14. Liyanage M, Ylianttila M, Gurtov A. A case study on security issues in LTE backhaul and core networks. *Case Studies in Secure Computing: Achievements and Trends* 2014; **1**: 167.
15. Dahlman E, Parkvall S, Skold J. *4G: LTE/LTE-Advanced for Mobile Broadband*. Academic Press: Cambridge, Massachusetts, USA, 2013.
16. Kumar A, Sengupta J, Liu Yf. 3GPP LTE: the future of mobile broadband. *Wireless Personal Communications* 2012; **62**(3): 671–686.
17. Bassil R, Elhajj IH, Chehab A, Kayssi A. Effects of signaling attacks on LTE networks. *2013 27th International Conference on Advanced Information Networking And Applications Workshops (WAINA)*, Catalonia, Spain, 2013; 499–504.
18. Jover RP. Security attacks against the availability of LTE mobility networks: overview and research directions. *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, New Jersey, USA, 2013; 1–9.
19. Dano M. The android IM app that brought T-mobiles network to its knees. *Fierce Wireless* 2010.
20. Bassil R, Chehab A, Elhajj I, Kayssi A. Signaling oriented denial of service on LTE networks. *Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access*, Paphos, Cyprus Island, 2012; 153–158.
21. Piper D. The Internet IP security domain of interpretation for ISAKMP, RFC 2407, November 1998.
22. Maughan D, Schertler M, Schneider M, Turner J. Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, November 1998.
23. Harkins D, Carrel D. The Internet key exchange (IKE), RFC 2409, November 1998.
24. Kaufman C. Internet key exchange (IKEv2) protocol, RFC 4306, December 2005.
25. Eronen P. IKEv2 mobility and multihoming protocol (MOBIKE), RFC 4555, June 2006.
26. Namal S, Liyanage M, Gurtov A. Realization of mobile femtocells: operational and protocol requirements. *Wireless Personal Communications* 2013; **71**(1): 339–364.

27. Moskowitz R, Nikander P, Jokela P. Host identity protocol, RFC 5201, April 2008.
28. Gurtov A. *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Wiley: West Sussex, United Kingdom, 2008.
29. Mobile backhaul solutions for LTE-advanced. *Technical Report*, ADVA Optical Networking SE, 2013.
30. A new era of mobile backhaul, Alcatel-Lucent, 2013. (Available from: http://www.alcatel-lucent.com/solutions/mobile-backhaul) [Accessed on 30 December 2015].
31. Eddy WM. TCP SYN flooding attacks and common mitigations. RFC 4987, August 2007.
32. Watson PA. Slipping in the window: TCP reset attacks. *Technical Report*, 2004.
33. CA CERT Advisory. 01 IP spoofing attacks and hijacked terminal connections, 2001.
34. Dierks T, Rescorla E. The transport layer security (TLS) protocol version 1.2, RFC 5246, August 2008.
35. Freier A, Karlton P, Kocher P. The secure sockets layer (SSL) protocol version 3.0, RFC 6101, August 2011.
36. Meyer C, Schwenk J. Lessons learned from previous SSL/TLS attacks—a brief chronology of attacks and weaknesses. *IACR Cryptology ePrint Archive* 2013; **2013**: 49.
37. Mersh R, Shah N. Mobile backhaul networks—the next generation, 2012. (Available from: http://www.tmcnet.com/voip/departments/articles/306439-mobile-backhaul -networks-next-generation.htm).
38. Li Z, Li L, Morillo L, Yang T. Seamless MPLS for mobile backhaul, Internet Draft, 2014.
39. Lasserre M, Kompella V. Virtual private LAN service (VPLS) using label distribution protocol (LDP) signaling, RFC 4762, 2007.
40. Kompella K, Rekhter Y. Virtual private LAN service (VPLS) using BGP for auto-discovery and signaling, RFC 4761, 2007.
41. Peng J, Zhang W, Huang K. A novel key derivation method for eavesdropper in LTE system, In *Proceeding of International Conference on Information Science and Technology (ICIST),* IEEE, Tangier, Morocco, 2013; 1535–1539.
42. Lai C, Li H, Lu R, Shen XS, Cao J. A unified end-to-end security scheme for machine-type communication in LTE networks, *IEEE/CIC International Conference on Communications in China (ICCC '13),* IEEE, Xi'an, China, 2013; 698–703.
43. Han CK, Choi HK. Security analysis of handover key management in 4G LTE/SAE networks. *IEEE Transactions on Mobile Computing* 2014; **13**(2): 457–468.
44. Keller GU, Beylot AL. Improving flow level fairness and interactivity in WLANs using size-based scheduling policies. *The 11th International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile System*, Vancouver, Canada, 2008.
45. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review* 2004; **34**(2): 39–53.
46. Chang RK. Defending against flooding-based distributed denial-of-service attacks: a tutorial. *Communications Magazine,* IEEE 2002; **40**(10): 42–51.
47. Protecting the network from denial of service floods. *Technical Report*, Juniper Networks, Inc, 2008.
48. Henderson T, Venema S, Mattes D. *HIP-based virtual private LAN service (HIPLS)*, Internet Draft, September 2011.