Enhancing Security, Scalability and Flexibility of Virtual Private LAN Services

Madhusanka Liyanage[1], Mika Ylianttila[2], Andrei Gurtov[3]
[1,2] Centre for Wireless Communications (CWC), University of Oulu, Finland
[3] Department of Computer and Information Science, Linköping University, Sweden
Email: [1]madhusanka.liyanage@oulu.fi, [2]mika.ylianttila@oulu.fi, [3]gurtov@acm.org

***Abstract*—Ethernet based VPLS (Virtual Private LAN Service) networks are now becoming attractive in many enterprise applications due to simple, protocol-independent and cost efficient operation. However, new VPLS applications demand additional requirements, such as elevated security, enhanced scalability and improved flexibility. This paper summarized the results of a thesis which focused to increase the scalability, flexibility and compatibility of secure VPLS networks. First, we propose a scalable secure flat-VPLS architecture based on Host Identity Protocol (HIP) to increase the forwarding and security plane scalability. Then, a secure hierarchical-VPLS architecture has been proposed by extending the previous proposal to achieve control plane scalability as well. To solve the compatibility issues of Spanning Tree Protocol (STP) in VPLS networks, a novel Distributed STP (DSTP) is proposed. Lastly, we propose a novel SDN (Software Defined Networking) based VPLS (SoftVPLS) architecture to overcome tunnel management limitations in legacy secure VPLS architectures. Simulation models and testbed implementations are used to verify the performance of proposed solutions.**

I. Introduction

Global spanned companies obtain connectivity services from communication service providers to interconnect their offices over the public Internet. Initially, L3VPNs (Layer 3 Virtual Private Networks) were the preferred choice of many service providers. Due to high operating costs and compatibility issues in L3VPNs, L2VPNs (Layer 2 Virtual Private Networks) such as VPLS are now becoming popular. In 2012, 47 percent of VPN (Virtual Private Networks) traffic was operated via VPLS [27]. IETF (Internet Engineering Task Force) has standardized two basic frameworks for VPLS networks by using the Border Gateway Protocol (BGP) [28] and the Label Distribution Protocol (LDP) [29]. Thereafter, several VPLS architectures were proposed to improve the performance of these frameworks [30]–[40].

VPLS networks were initially utilized only in industrial networks [41]–[45]. Presently, VPLS networks are used in many enterprise applications such as DCI (data center interconnect), voice over IP (VoIP) and videoconferencing servicesdo [27]. However, new VPLS applications demand additional requirements, such as elevated security, enhanced scalability, optimum utilization of network resources and further reduction in operational costs. Hence, the motivation of this paper is to increase the scalability, flexibility and compatibility of secure VPLS networks to achieve these requirements.

The first contribution is the proposal of a scalable secure flat-VPLS architecture based on Host Identity Protocol (HIP). It contains a novel session key-based security mechanism to increase the forwarding and security plane scalability of secure VPLS networks. The second contribution is the proposal of a scalable and secure hierarchical-VPLS architecture based on HIP. This increases the scalability of the previously proposed flat-VPLS architecture by providing control plane scalability as well. The third contribution is the proposal of a novel Distributed STP to solve the compatibility issues of traditional STP in VPLS networks. The fourth contribution is the proposal of a novel SDN based VPLS architecture to overcome the tunnel management limitations of legacy secure VPLS architectures. Extensive simulations and test bed implementations are used reveal the expected advantages of proposed architectures.

The rest of the paper is organized as follows. Section II contains an introduction to VPLS architecture and the limitations. The main contributions are presented in Section III. Simulation and testbed experiment results are presented in Section IV. Section V contains the conclusion.

II. Background

A. Virtual Private LAN Service (VPLS)

VPLS provides the multipoint-to-multipoint Ethernet communication over IP/MPLS based provider networks. Figure 1 illustrates a simple VPLS architecture.

Main components of a VPLS are Customer edge Equipment (CE), Provider edge Equipment (PE), VPN tunnels and the provider network. CEs are the middleboxes between the customer sites and the provider network. PEs have all the VPLS intelligence. A full mesh of PWs/tunnels are established over the provider network to interconnect these PEs. The provider network can be a public network such as the Internet.

This work has been performed in the framework of the SIGMONA, SECUREConnect, Naked Approach, Towards Digital Paradise and CENIIT 17.01 projects. This research is funded by Academy of Finland and TEKES, Finland.

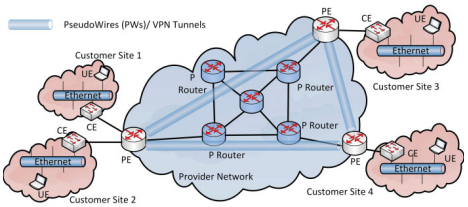


Fig. 1: Simple VPLS architecture

B. Key Challenges in Legacy VPLS Architectures

1) Security Limitations: Generally, the customer's private network is a closed and trusted network. However, VPLS networks expose customer's private data to third-party attackers while transport over the public provider network. Moreover, L2 devices are very primitive devices and do not have any inbuilt security mechanisms to prevent serious attacks. On the other hand, PE devices are also vulnerable to third party attacks which can jeopardize the operation of VPLS.

2) Scalability Limitations: First, flat VPLS architectures require a VPN tunnel between every pair of PEs. Thus, the number of tunnels in the network is exponentially increasing with the number of PEs. This is called the "N-square scalability problem". Thus, flat VPLS networks suffer from massive signaling overhead which is required to establish/maintain these tunnels. It reduces the control plane scalability [4], [9]. Second, each PE has a maximum limit to support hardware ingress replications. If a PE is not able to support required number of hardware ingress replications, then a broadcast frame needs resend several times over the same network link [4], [9]. It unnecessarily consumes the bandwidth and increase the frame transport delay. It reduces the forwarding plane scalability. Third, existing secure VPLS architectures have a massive key storage complexity and inefficient security mechanisms. It reduces the security plane scalability [2], [8].

3) Compatibility Limitations: In a VPLS network, connections through the provider network are invisible to L2 protocols. These transparent links cause many negative effects on L2 protocols [10]. Moreover, the provider networks has the extensive propagation and queuing delays than L2 networks. Thus, the combination of L2 and L3 network characteristics in VPLS jeopardize the operation of L2 protocols [10].

4) Complex and Static Tunnels Management: Legacy secure VPLS architectures have static, inflexible and decentralized tunnel management mechanisms [18]. The tunnel characteristics of each VPN tunnel are predefined by the network administrators and they behave similarly regardless of the traffic demand between the customer sites. Moreover, tunnel establishment delay of legacy secure VPLS architectures is highly depending on communication link quality and distance between PEs. However, legacy secure VPLS networks do not consider these physical layer constraints or adjust the tunnel parameters to mitigate the impact [18].

III. Proposed Architectures

A. S-HIPLS: A Scalable and Secure Flat-VPLS Architecture

We propose a scalable and secure flat-VPLS architecture [2], [8] based on HIP. It propose to establish HIP tunnels on top of the provider network. HIP tunnels securely interconnect L2 customer sites. In contrast to per tunnel keying mechanism in HIP [46], we propose a novel session key-based security mechanism. Figure 2 illustrates the proposed S-HIPLS architecture.

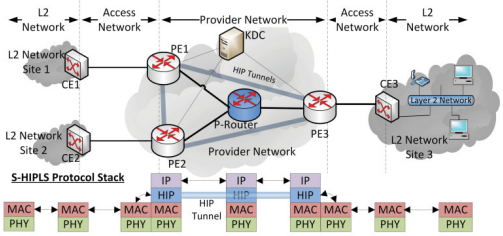


Fig. 2: The network topology of S-HIPLS architecture

S-HIPLS uses two types of keys as Content Encryption Key (CEK) and Key Encryption Key (KEK). CEK is used to encrypt and decrypt all packets belong to a single provider VPN. Every PE has a unique KEK which is used to encrypt and decrypt the corresponding CEKs. There is a Key Distribution Center (KDC) is responsible for distributing the encrypted CEKs among PEs. KDC also works as the Authentication Server (AS) which maintains the Access Control Lists (ACL) of each provider VPN. Our architecture comparatively reduces the complexity of key storage at a node and the overall key storage of the network. Further, the propose keying mechanism reduces the number of encryptions per broadcast frame. These features increase the security plane scalability of secure VPLS architectures.

Moreover, our architecture proposes an efficient broadcast mechanism which significantly reduces the number of encryption and packet generation per broadcast frame at the entry PE. S-HIPLS requires only one encryption per broadcast frame and it can be replicated along the broadcast or multicast tree. Thus, S-HIPLS increases the forwarding plane scalability.

B. H-HIPLS: Secure Hierarchical-VPLS Architecture

We propose a novel hierarchical VPLS architecture [4], [9] based on previous S-HIPLS to overcome the control plane scalability limitation. The proposed architecture establishes HIP tunnels between PEs in a hierarchical manner to form the VPLS network. Figure 3 illustrates the proposed H-HIPLS architecture.

H-HIPLS also uses two types of keys (i.e. CEK and KEK) similar to previous S-HIPLS architecture. In contrast to S-HIPLS, H-HIPLS uses two types of PEs as u-PE and n-PE. u-PEs are user facing PEs, while n-PEs are network facing PEs. n-PEs are responsible for packet forwarding, address learning and auto discovery functions. Moreover, mesh connected VPN tunnels are established only between n-PEs. u-PEs encrypts

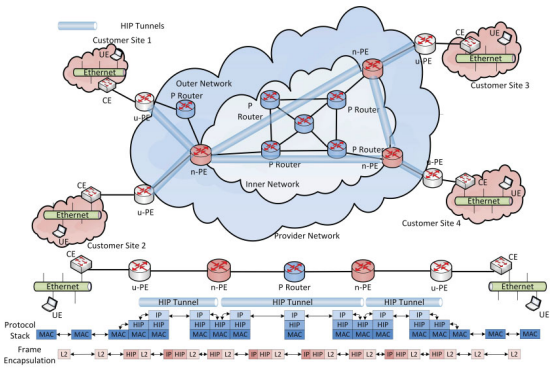
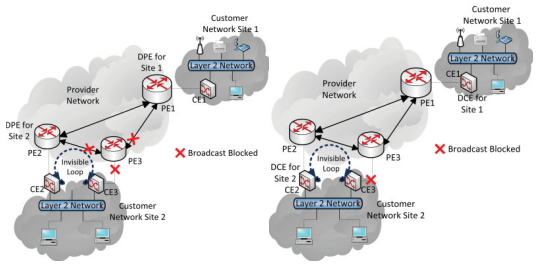


Fig. 3: The protocol stack of the H-HIPLS architecture



(a) PARIM (b) CARIM

Fig. 4: Proposed Redundancy Identification Mechanisms

the L2 Frames and forwards to the connected n-PE. We also propose a novel encrypted label based secure frame forwarding mechanism to transport L2 frames over the hierarchical VPLS network. When a u-PE receives a data frame from a CE, the source u-PE encrypts an L2 frame using the corresponding CEK of the provider VPN. Then, it will wrap this within ESP (Encapsulating Security Payload) packet. The source u-PE inserts the encrypted label into the standard ESP header of the packet and forwards the frame to the n-PE. The encrypted label is the encrypted destination MAC (Media Access Control) address of the frame. It encrypts by using CEK of the control VPN.

The proposed hierarchical architecture significantly reduces the total number of tunnels in the VPLS network. It provides additional control plane scalability in addition to the security and forwarding plane scalability provided by previous S-HIPLS architecture.

C. DSTP: Distributed Spanning Tree Protocol

In a VPLS network, connections through the provider network are invisible to L2 protocols. These transparent links cause many negative effects on L2 protocols such as STP. We proposed a novel Distributed STP (DSTP) to solve the implementation issues of STP in VPLS networks [10]. DSTP proposes to run a customized version of STP on each remote customer site and prevents the transmission of STP BPDUs (Bridge Protocol Data Units) over the provider network. However, the existing STP versions cannot be used as local STP instances since they are not capable of identifying loops over the provider network. Thus, we integrate two Redundancy Identification Mechanism (RIM) to DSTP, namely Provider Associated RIM (PARIM) and Customer Associated RIM (CARIM).

In PARIM, VPLS provider performs RIM. Initially, every PE broadcasts a Network Advertisement Packet (NAP) through the provider network and elect a Designated PE (DPE) for each network segment. Then, all other PEs are set to the broadcast blocking state. Only DPEs are allowed to flood broadcast frames. In CARIM, customer performs RIM. Initially, every CE broadcasts a Network Advertisement Frame (NAF) through customer network segments and elect a Designated CE (DCE) for each segment. All other CEs are set to the broadcast blocking state. Only DCEs are allowed to forward/accept broadcast frames to/from PEs.

Therefore, the first step of proposed DSTP is to run the RIM procedure. RIM elects the DPEs or DCEs. Thereafter, a customized version of STP can run on each remote customer site. Proposed DSTP mechanism solves the compatibility limitation of STP in VPLS networks.

D. Soft-VPLS: Software Defined Networking (SDN) based VPLS architecture

We propose a novel SDN based VPLS (SoftVPLS) architecture to overcome tunnel management limitations in legacy secure VPLS architectures [18]. It proposes three key changes. First, legacy PEs are replaced with IPsec enabled SDN switches. Second, VPLS tunnel management functions are controlled by a centralized controller. Third, a Tunnel Management Application (TM App) dynamically decides the tunnel parameters based on real-time network statistics. Figure 5 illustrates the proposed Soft-VPLS architecture.

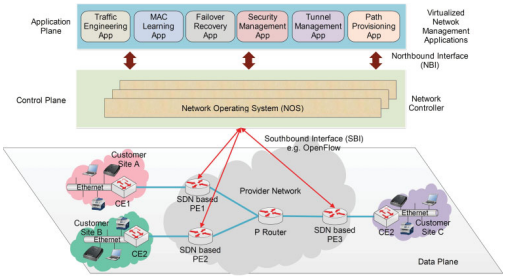
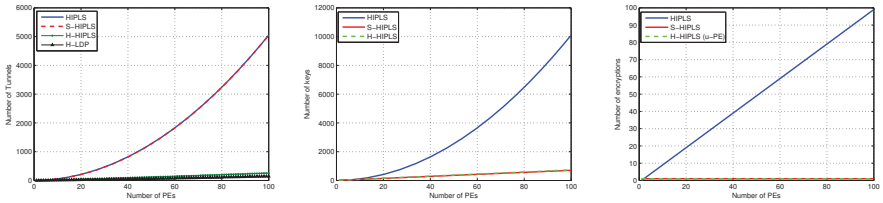


Fig. 5: The proposed Soft-VPLS architecture

Moreover, we propose three new mechanisms to improve the performance of legacy tunnel management functions. 1) A dynamic tunnel establishment mechanism: To dynamically change the tunnel parameter based on real-time network statistics, 2) A tunnel resumption mechanism : To reduce the tunnel establishment delay of subsequent tunnel establishments between authorized PEs and 3) A fast transmission mechanism : To reduce the average data transmission delay for geographically distant customer sites.



(a) (b) (c)

Fig. 6: a) The total number of VPN tunnels in the network, b) The total number of keys stored in the VPLS network compared to PEs, c) The maximum number of encryptions per broadcast frame

TM app periodically estimates the tunnel parameter for each tunnel based on real time and historical traffic patterns. As a result, the proposed architecture reduces the average number of tunnels per PE, the total number of tunnels, subsequent tunnel establishment delay and average file transfer delay than legacy secure VPLS architectures.

IV. Performance Evaluation

A. Scalability Analysis of S-HIPLS and H-HIPLS

The proposed S-HIPLS and H-HIPLS architecture was simulated on OMNET++ simulator [47] and the performance of the scalability was evaluated. We compared the performance of the proposed architecture with HIPLS [30], and H-LDP [29] architectures.

1) Comparison of the Control Plane Scalability: Figure 6a illustrates the total tunnel establishment complexity of the VPLS network compared to the number of PEs. A significant reduction in the total number of tunnels in hierarchical architectures (i.e. H-LDP and H-HIPLS) was observed compared to flat architectures. Therefore, the experiment results indicated that the tunnel establishment complexity of the proposed H-HIPLS is significantly lower than other secured architectures i.e. HIPLS and S-HIPLS. Thus, H-HIPLS improves the control plane scalability.

2) Comparison of the Security Plane Scalability: The key storage requirement is one of the main metrics to measure security plane scalability. Figure 6b illustrates the total key storage complexity of the VPLS network compared to the number of PEs. Here also, the number of provider VPNs was set to 5 and the number of PEs ranged from 1 to 100. The experiment results clearly show that the key storage requirement in the proposed S-HIPLS and H-HIPLS architectures is significantly lower than HIPLS. Thus, S-HIPLS and H-HIPLS improves the security plane scalability.

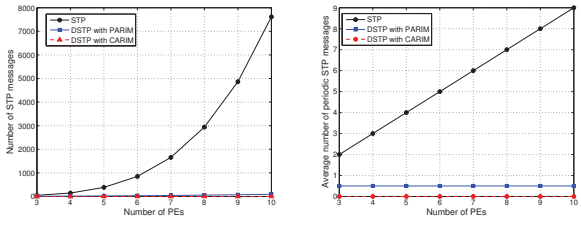
3) Comparison of the Forwarding Plane Scalability: We compared the performance of the frame broadcasting mechanism by measured the number of encryptions at each PE. Figure 6c illustrates the maximum number of encryptions per broadcast frame at a PE for each VPLS architecture. We can see a linear increment for HIPLS while both S-HIPLS and H-HIPLS remains constant at 1. Thus, S-HIPLS and H-HIPLS improves the forwarding plane scalability than HIPLS.

B. Testbed implementation of S-HIPLS and H-HIPLS

A test bed implementation [13] was used to analyze the data plane performance of existing secure VPLS architectures. Proposed architecture had about 20% throughput reduction for both UDP and TCP sessions than non-secure VPLS architecture. Moreover, jitter of the secure VPLS architecture is two times higher than the non-secure VPLS scenario. The additional layer of encryption was the main reason for the reduced average throughput of the secure VPLS architecture. Moreover, the secure VPLS architecture increased the latency approximately by 87% due to encryption and tunneling delays in PE devices. Moreover, the experiment results revealed that H-HIPLS architecture has almost similar throughput performance (2% less) as S-HIPLS. It had only 3% higher latency than other secure VPLS architectures. This performance penalty had occurred due to the extra label encryptions.

C. Performance Analysis of DSTP

We simulated the proposed DSTP (with PARIM and CARIM) and traditional STP [48] on the OMNET++ network simulator [47] to compare performance. We analyzed the performance of each scheme by increasing the number of PEs in the network. Figure 7a illustrates the total number



(a) (b)

Fig. 7: a) Number of messages over the provider network during the root bridge selection phase, b) Number of periodic STP messages over the provider network per second

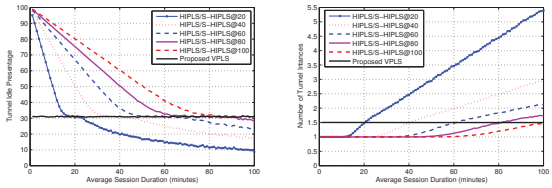
of STP messages transmitted through the provider network during the root bridge selection phase. The experiment results showed that the number of STP messages through the provider network increases exponentially with the number PEs for the traditional STP scenario. Although the number of STP

messages transmitted through the provider network had a nearly linear increment for DSTP with PARIM scenario, it was significantly lower than with the traditional STP scenario. On the other hand, DSTP with CARIM does not exchange any STP messages via the provider network. Figure 7b illustrates the average number of periodic STP messages transmitted over a 1 s time period. The experiment results verified that the number of periodic STP messages through the provider network increases linearly for traditional STP while it remains constant for the DSTP with PARIM scenario. DSTP with PARIM transmits periodic STP messages only for PEs in the same network site. Thus, it depends only on the number of PEs in the same network site. Thus, the number of periodic STP messages is significantly lower in DSTP with PARIM than the traditional STP scenario. On the other hand, DSTP with CARIM does not exchange any periodic STP message via the provider network.

Thus, we can conclude that traditional STP is not suitable for implementation in a large scale network with a large number of PEs. In a large scale network, DSTP offers scalability by significantly reducing the number of STP messages transmitted through the provider network. Ultimately, it reduces the additional overhead and STP operational cost of the customer.

D. Performance Analysis of Soft-VPLS Architecture

We simulated Soft-VPLS architecture in an OMNET++ simulation environment [47] to compare the performance with other secure VPLS architectures (i.e. HIPLS [30] and S-HIPLS [8]). We measured the number of tunnel establishment instances and the tunnel idle percentage per active session by changing the average session duration. Here, we considered five cases for HIPLS and S-HIPLS where the tunnel duration is predefined as 20, 40, 60, 80 and 100 minutes. Figure 8 illustrates the simulation results. The simulation results in



(a) (b)

Fig. 8: a) Tunnel Idle Percentage, b) Number of Tunnel Instances per Session

Figure 8a verified that the percentage of tunnel idle time in Soft-VPLS is independent of the session duration. It reduces the tunnel idle time percentage to 30% under the utilized algorithm. On the other hand, the performance of legacy secure VPLS architectures highly depend on the session duration. Their performance is always lower than the proposed SoftVPLS architecture as long as the session duration is lower than the pre-defined tunnel duration. After that, the performance of legacy architectures is better than the SoftVPLS architecture. The simulation results in Figure 8b verified that the number of tunnel instances per session of the proposed architecture is independent of the session duration. This reduced the number of instances to 1.5 per session. However, the performance of legacy secure VPLS architectures depends highly on the session duration and always lower than the proposed SoftVPLS architecture as long as the session duration was higher than the pre-defined tunnel duration.

E. Testbed implementation of Soft-VPLS Architecture

The Soft-VPLS architecture was implemented in a testbed to analyze the performance of the data plane with other secure VPLS architectures (i.e. HIPLS [30] and S-HIPLS [8]). The data plane performance (throughputs, latency and jitter) of Soft-VPLS architecture had almost similar to other secure VPLS architectures. Thus, the utilization of Soft-VPLS architecture does not reduce the data plane performance of existing secure VPLS architectures. However, the proposed SoftVPLS architecture with Tunnel Resumption Procedure significantly reduced (about 44% reduction) the tunnel establishment delay compared to other secure VPLS architectures.

V. Conclusion

This paper presented four main contributions to increase the scalability, flexibility and compatibility of secure VPLS networks. First, we proposed a scalable and secure flat-VPLS architecture (S-HIPLS). It used a session key based security mechanism to offered security plane scalability by reducing the complexity of key storage at a node and the network. The proposed efficient broadcast mechanism reduced the number of encryptions per broadcast and increased the forwarding plane scalability. Second, we proposed a scalable and secure hierarchical-VPLS architecture (H-HIPLS) which had further improved the features of S-HIPLS. H-HIPLS significantly increased the control plane scalability by reducing the total number of VPN tunnels in the network. Third, we proposed a novel Distributed STP (DSTP) to solve the incompatibility issues of STP in VPLS networks. DSTP runs a modified STP instance in each remote segment of the VPLS network. Furthermore, we proposed two Redundancy Identification Mechanisms (RIMs) called Customer Associated RIM (CARIM) and Provider Associated RIM (PARIM) to prevent functional issues which may arise due to invisible loops in the provider network. Finally, we proposed a novel SDN based VPLS (Soft-VPLS) architecture to overcome the tunnel management limitations of legacy secure VPLS architectures. The proposed architecture dynamically adjusts the tunnel parameters by analyzing the traffic patterns of each tunnel. Soft-VPLS reduced the average number of tunnels in the network and tunnels establishment delay compared to legacy secure VPLS architectures.

Thus, the results of the paper will help for more secure, scalable and efficient development of VPLS networks. It will optimize the utilization of network resources and further reduction in operational costs of future VPLS networks.

REFERENCES

[1] M. Liyanage, "Enhancing security and scalability of virtual private lan services," Ph.D. dissertation, University of Oulu, 2016. [Online]. Available: http://jultika.oulu.fi/Record/isbn978-952-62-1376-7

[2] M. Liyanage and A. Gurtov, "Securing Virtual Private LAN Service by Efficient Key Management," *Security and Communication Networks*, vol. 7, no. 1, pp. 1–13, 2014.

[3] S. Namal, M. Liyanage, and A. Gurtov, "Realization of Mobile Femtocells: Operational and Protocol Requirements," *Wireless personal communications*, vol. 71, no. 1, pp. 339–364, 2013.

[4] M. Liyanage, M. Ylianttila, and A. Gurtov, "Secure Hierarchical VPLS Architecture for Provider Provisioned Networks," *Access, IEEE*, vol. 3, pp. 967–984, 2015.

[5] M. Liyanage, A. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security Perspective," *IEEE Security and Privacy Magazine*, 2015.

[6] M. Liyanage, P. Kumar, M. Ylianttila, and A. Gurtov, "Novel Secure VPN Architectures for LTE Backhaul Networks," *Security and Communication Networks*, 2016.

[7] M. Liyanage and A. Gurtov, "Secured VPN Models for LTE Backhaul Networks," in *Vehicular Technology Conference (VTC Fall), 2012 IEEE*. IEEE, 2012, pp. 1–5.

[8] ——, "A Scalable and Secure VPLS Architecture for Provider Provisioned Networks," in *IEEE Wireless Communication and Networking Conference: WCNC 2013*. IEEE, 2013.

[9] M. Liyanage, M. Ylianttila, and A. Gurtov, "Secure Hierarchical Virtual Private LAN Services for Provider Provisioned Networks," in *Communications and Network Security (CNS), 2013 IEEE Conference on*. IEEE, 2013, pp. 233–241.

[10] ——, "A Novel Distributed Spanning Tree Protocol for Provider Provisioned VPLS Networks," in *IEEE Conference on Communications: ICC 2014*. IEEE, 2014.

[11] M. Liyanage, J. Chirkova, and A. Gurtov, "Access Point Selection Game for Mobile Wireless Users," in *The 8th IEEE WoWMoM Workshop on Autonomic and Opportunistic Communications*. IEEE, 2014.

[12] M. Liyanage, M. Ylianttila, and A. Gurtov, "Securing the Control Channel of Software-Defined Mobile Networks," in *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on*. IEEE, 2014, pp. 1–6.

[13] M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Secure Virtual Private LAN Services: An Overview with Performance Evaluation," in *IEEE ICC 2015 - Workshop on Advanced PHY and MAC Techniques for Super Dense Wireless Networks*. IEEE, 2015, pp. 10 297–10 303.

[14] J. Costa-Requena, J. Llorente Santos, V. Ferrer Guasch, K. Ahokas, G. Premsankar, S. Luukkainen, I. Ahmad, M. Liyanage, M. Ylianttila, O. Lopez Perez *et al.*, "SDN and NFV Integration in Generalized Mobile Network Architecture," in *Networks and Communications (EuCNC), 2015 European Conference on*. IEEE, 2015, pp. 154–158.

[15] M. Liyanage, I. Ahmed, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, E. M. d. Oca, A. Valtierra, and C. Jimenez, "Security for Future Software Defined Mobile Networks," in *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*. IEEE, 2015, pp. 256–264.

[16] J. Okwuibe, M. Liyanage, and M. Ylianttila, "Performance Analysis of Open-Source Linux-Based HIP Implementations," 2015.

[17] M. Liyanage, I. Ahmad, M. Ylianttila, A. Gurtov, A. B. Abro, and E. M. de Oca, "Leveraging LTE Security with SDN and NFV," in *IEEE 10th International Conference on Industrial and Information Systems (ICIIS)*. IEEE, 2015.

[18] M. Liyanage, A. Gurtov, and M. Ylianttila, "Improving the Tunnel Management Performance of Secure VPLS Architectures with SDN," *Proc. of IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA. IEEE*, 2016.

[19] I. Ahmad, M. Liyanage, S. Namal, M. Ylianttila, A. Gurtov, M. Eckert, T. Bauschert, Z. Faigl, L. Bokor, E. Saygun, H. A. Akyildiz, O. L. Perez, M. U. Itzazelaia, B. Ozbek, and A. Ulas, "New Concepts for Traffic, Resource and Mobility Management in Software-Defined Mobile Networks," *Proc. of 12th Wireless On-demand Network systems and Services Conference (WONS), Cortina d'Ampezzo, Italy. IEEE*, 2016.

[20] M. Liyanage, P. Kumar, S. Soderi, M. Ylianttila, and A. Gurtov, "Performance and Security Evaluation of Intra-Vehicular Communication Architecture," *Proc. of IEEE ICC 2016 - Workshop on Convergent Internet of Things (Convergent IoT), Kuala Lumpur, Malaysia. IEEE*, 2016.

[21] J. Okwuibe, M. Liyanage, and M. Ylianttila, "Provider Assisted Wi-Fi Offloading Leveraging on SDN," *Proc. of 22nd European Wireless conference, Oulu, Finland*, 2016.

[22] M. Liyanage, P. Kumar, and A. Gurtov, "Zone-based Security Architecture for Intra-Vehicular Wireless Communication," 2015.

[23] M. Liyanage, A. Gurtov, and M. Ylianttila, *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*. John Wiley & Sons, 2015.

[24] M. Liyanage, M. Ylianttila, and A. Gurtov, "A Case Study on Security Issues in LTE Backhaul and Core Networks," *Case Studies in Secure Computing: Achievements and Trends*, p. 167, 2014.

[25] ——, "IP-Based Virtual Private Network Implementations in Future Cellular Networks," *Handbook of Research on Progressive Trends in Wireless Communications and Networking*, p. 44, 2014.

[26] N. Zhang, J. Lehmusvuori, M. Liyanage, R. Kantola, J. salo, T. Bauschert, Z. Vince, A. Ulaş, and J. Costa, "Software-Defined and Virtualized Mobile Networks," 2016.

[27] "Virtual Private LAN Service (VPLS) Technical Primer for Government Agencies ," Alcatel-Lucent Inc., Tech. Rep., 2008. [Online]. Available: http://www3.alcatel-lucent.com/solutions/mpls4ips/docs/VPLS_Tech_govt_agc_twp.pdf

[28] K. Kompella and Y. Rekhter, "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling," RFC 4761, IETF, January 2007.

[29] M. Lasserre and V. Kompella, "Virtual Private LAN Service (VPLS) using Label Distribution Protocol (LDP) Signaling," RFC 4762, IETF, January 2007.

[30] T. Henderson, S. Venema, and D. Mattes, "HIP-based Virtual Private LAN Service (HIPLS)," IETF, September 2011.

[31] E. R. H. Shah and G. Heron, "IP-Only LAN Service (IPLS)," *Internet Draft*, IETF, February 2007.

[32] "H-VPLS N-PE Redundancy for QinQ and MPLS Access," CISCO Cooperation, Tech. Rep., 2011. [Online]. Available: http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/

[33] "Demystifying H-VPLS," Juniper Networks, Inc, Tech. Rep., 2010. [Online]. Available: http://www.juniper.net/us/en/local/pdf/app-notes/3500116-en.pdf

[34] S. Khandekar, V. Kompella, J. Regan, *et al.*, "Hierarchical Virtual Private LAN Service," *Internet Draft*, IETF, June 2002.

[35] A. Sodder, K. Ramakrishnan, C. DelRegno, , and J. Wils, "Virtual Hierarchical LAN Services," *Internet Draft*, IETF, April 2003.

[36] C. Hu, C. Yuan, K. Liu *et al.*, "Enhanced H-VPLS Service Architecture using Control Word," Aug. 4 2009, US Patent 7,570,648.

[37] D. Zelig, L. Bruckman, and Y. Kotser, "Hierarchical Virtual Private LAN Service Protection Scheme," Oct. 16 2007, US Patent 7,283,465.

[38] G. WARNOCK, "Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide: Preparing for the NRS II Certification Exams Self-Study Guide (paperback)," 2011.

[39] N. Chowdhury and R. Boutaba, "A Survey of Network Virtualization," *Computer Networks*, vol. 54, no. 5, pp. 862–876, 2010.

[40] R. Sofia, "A Survey of Advanced Ethernet Forwarding Approaches," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 1, pp. 92–115, 2009.

[41] T. Henderson, "Boeing HIP Secure Mobile Architecture," Tech. Rep. [Online]. Available: http://www.ietf.org/proceedings/73/slides/HIPRG-0.pdf

[42] "Tempered networks," Tech. Rep. [Online]. Available: http://www.temperednetworks.com/

[43] "Tofino Security Appliance," Tech. Rep. [Online]. Available: http://www.tofinosecurity.com/products/tofino-security-appliance

[44] X. Dong and S. Yu, "VPLS: An Effective Technology for Building Scalable Transparent LAN Services," in *Asia-Pacific Optical Communications*. International Society for Optics and Photonics, 2005, pp. 137–147.

[45] S. A. Boyer, *SCADA: Supervisory Control and Data Acquisition*. International Society of Automation, 2009.

[46] R. Moskowitz, P. Nikander, and P. Jokela, "Host Identity Protocol," RFC 5201, 2008.

[47] A. Varga, "The OMNeT++ Discrete Event Simulation System," in *Proceedings of the European Simulation Multiconference (ESM-2001)*, 2001.

[48] "IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges," *IEEE Std 802.1D-2004 (Revision of IEEE Std 802.1D-1998)*, pp. 1–277, 2004.