A Survey on Secure and Resilient Session Schemes: Technical Comparison and Assessment

Daouda Ahmat, Damien Magoni

EAI Endorsed Transactions
on Future Internet
Research Article EAI.EU

A Survey on Secure and Resilient Session Schemes: Technical Comparison and Assessment

Daouda Ahmat[1,*], Damien Magoni[2]

[1]Virtual Univesity of Chad, 5711 N'Djamena, Chad, E-mail: daouda.ahmat@uvt.td
[2]University of Bordeaux, 33405 Talence Cedex, France, E-mail: magoni@labri.fr

Abstract

Cyber threats become more and more pervasive on the Internet and on distributed/decentralized systems. In order to secure communication over these infrastructures and respond to mobility constraint, a new class of Virtual Private Networks (VPN), which support both security and mobility, has emerged in the course of last years. Mobile Virtual Private Networks, called mobile VPN, provide not only secure tunnels but also session continuity mechanism despite location change or connection disruptions. This mechanism enables secure sessions to survive in dynamic/mobile environments without requiring a renegotiation of security keys during the session resumption phase. In this paper, on the one hand, we survey the recent literature on the mobile VPN systems followed by a detailed analysis and a technical comparison in tabulated form of existing technologies. On the other hand, we carry out experiments on open source mobile VPN infrastructures. We subsequently outline and discuss major features and performances of various assessed mobile VPN infrastructures.

Received on 8 December 2017; accepted on 20 December 2017; published on 12 January 2018

Keywords: VPN, mobile VPN, Resilent Session, Seamless Resumption

doi:10.4108/eai.12-1-2018.153558

1. Introduction

A Virtual Private Network (VPN) provides increased security between two remote entities that exchange data through untrusted networks such as the Internet [1]. VPN systems prevent against various attacks such eavesdropping or replay. However, traditional VPNs fail to support the mobility of users. Indeed, network failures automatically break-up secure tunnels and involve a subsequent renegotiation that is then necessary to reestablish broken tunnels. Such a negotiation involves expensive computational operations in order to restore tunnels as well as transport and application layers connections. This phase of negotiation causes not only significant latency but also presents risks of Man-In-The-Middle attacks. Traditional VPNs can not therefore effectively operate in dynamic and/or mobile environments.

Mobile devices and dynamic environments become pervasive in the Internet. However, for instance traditionnal VPN infrastructures do not support session continuity result from location change or network reconfiguration. After each connection disruption, key renegotiation process is needed to restore broken tunnel. In order to adress network failures resulting from location changes or network reconfigurations, several solutions were proposed in the literature [2–7] . This work surveys the state-of-the-art in the area of mobile VPN systems, identifies recent research directions and experiments on some open source mobile VPN applications.

The paper and its main contributions are structured as follows:

- We first succinctly present our previous work on the same topic (Section 2);
- We next describe proposed mobile VPN schemes in the literature and discuss their respective features (Section 3);

★Please ensure that you use the most up to date class file, available from EAI at http://doc.eai.eu/publications/transactions/latex/
*Corresponding author. Email: publications@eai.eu

- We then provide a technical comparison in tabulated form of existing mobile VPN technologies (Section 4);
- We after that evaluate various implementations of mobile VPN infrastructures and we compare detailed results for assessing their performances (Section 5);
- We finally present related work found in the literature (Section 6).

2. Background

This paper is an extension to our previous work on the same topic presented in *Africomm 2016 Conference* [8]. Indeed, we extend our previous paper by both increasing the state-of-the-art and adding new unpublished material such as a more detailed analysis of various mobile VPN schemes and a technical comparison in tabulated form.

3. Mobile VPN technologies

Up to now, several mobile VPN solutions have been proposed in various research papers. In this section, we describe some leading examples of mobile VPN systems and technical concepts in this area proposed in litterature.

3.1. P2P Mobile VPN

In opposition to most dynamic VPN systems, these systems have the advantage to be fairly scalable and to have ability to communicate across NAT and firewalls. Decentralized P2P VPN are flexible and self-organizing infrastructures that enable users to create their own secure networks upon an untrusted network. A layer 2 peer-to-peer VPN (see figure 1), called N2N [2], and ELA [9] topologies are very similar despite the fact that N2N is based on the OSI layer 2 whereas ELA is based on the OSI layer 3. However the use of super nodes in N2N limits its full scalability as these nodes have a more important role than the other nodes and thus they can weaken the overall strength of the N2N network and may even break its connectivity if they fail.

Freelan [10] is a multi-platform and open-source peer-to-peer VPN that abstracts a LAN over the Internet.

Based over the UDP protocol, the FreeLAN Secure Channel Protocol (FSCP) is designed to be secure and efficient, and it tries to reduce the network overhead. In addition, Freelan systems can be configured to act according to a client/server, peer-to-peer or hybrid model whichever suits best.

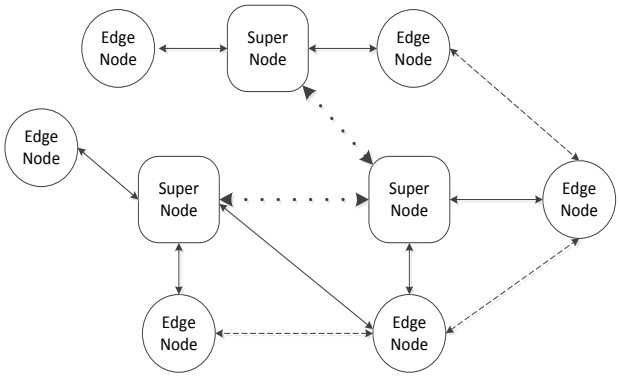

Figure 1. Example of N2N topology.

3.2. IPSec + Mobile IP

Mobile VPN systems based on both IPsec [11] and Mobile IP [12] have been proposed several times such as in [13], [7], [14], [15] and [16], in order to attempt to overcome the inherent mobility drawbacks of traditional VPNs. Nevertheless, as explained in [17], many problems arise from the combination between IPsec and MobileIP. In order to overcome these problems, a model has been proposed which is based on the use of two HAs (Home Agents) - internal HA and external HA - and two FAs (Foreign Agents) - internal FA and external FA - by Vaarala *et al.* in [18]. However, this model imposes the use of three imbricated tunnels({x-MIP{GW{i-MIP{original packet}}}}), as shown in figure 2.

In addition, a IPsec-based mobile VPN requires n tunnels (n security layers) when there are n IPsec hops between the source and destination entities. Therefore, the imbricated tunnels in such VPN systems have a negative impact on their network performances (i.e., throughput, overhead, etc).

In order to address IPsec mobility inherent issues, several improved schemes based on the IPsec architecture have been proposed by Eronen *et al.* in [4], [19], or [20]. Based on security extensions to MOBIKE [4], the solution described in [20] combines secure connectivity and Mobile IPv4. This approach resolves considerably the issues notified in [17] such as overhead, NAT traversal or mobility problems due to the combination of IPsec and Mobile IPv4. These solutions are however not free of scalability issues and network overhead that they inherit from IPsec and Mobile IP.

Based upon the NEMO architecture [21], the mobile VPN scheme presented in [22] provides secure connectivity between vehicles for public transportation. In other words, this model provides secure vehicle to vehicle (V2V) communications as well as secured communications between passengers in the same (or in a different) vehicle. As the above mobile VPN solutions,

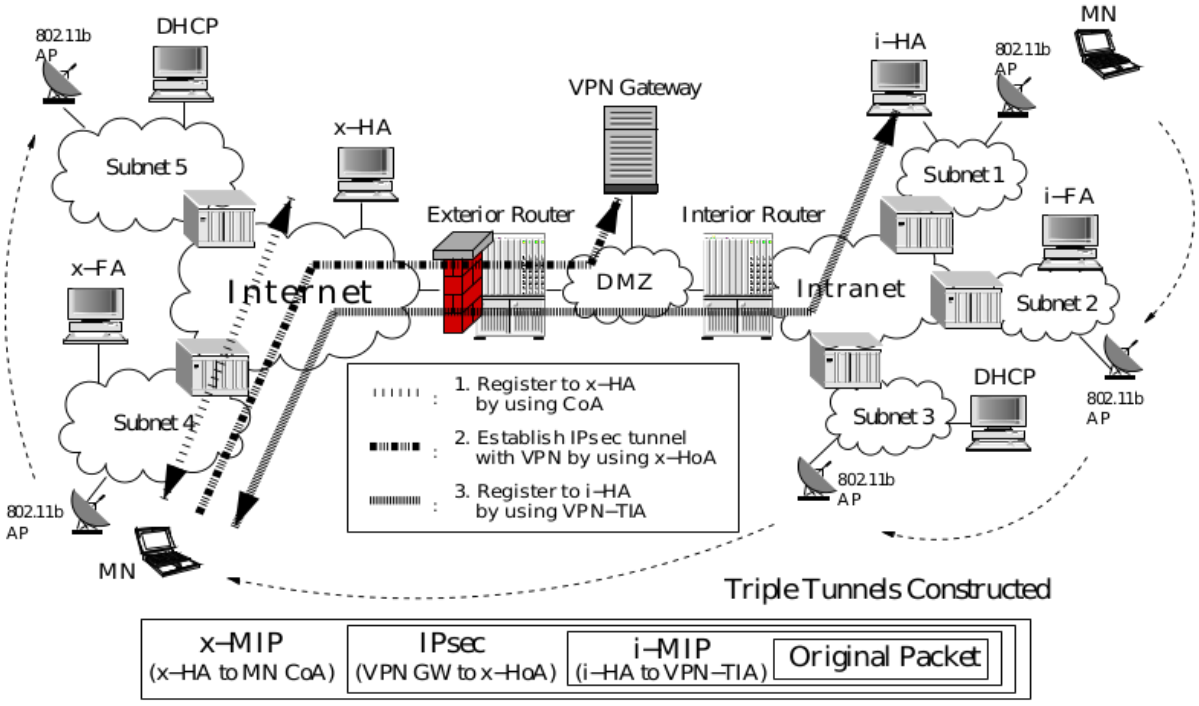

Figure 2. IETF Mobile VPN – source IETF.

this current model is designed to use the best properties of MOBIKE and Mobile IP.

The dynamic VPN approach proposed in [23] enables to use alternately IPsec in Full-Mesh mode or in Hub mode with a centralized IPsec Gateway. The first mode is only used when routing problems occur. This architecture extends MOBIKE in order to support dynamic tunnels. However, this model is not designed to support mobility.

Another proposal leveraging MOBIKE is presented by Migault in [24], where they propose an alternative End-to-End security (E2E) architecture based on their own MOBIKEX protocol, which extends the MOBIKE mobility and multihoming features to multiple interfaces and to the transport mode of IPsec. Based on a topology organized in communities, peer-to-peer (P2P) mobile VPN systems have also been proposed such as ELA [9] or N2N [25].

3.3. HIP-based mobile VPN

The Host Identity Protocol (HIP) [3, 6] is an architecture that provides both mobility and multihoming services. HIP introduces a new name space that enables the separation between the host identity, called Host Identity Tag or HIT, and the host location, as shwon in figure 3. Each HIP host is uniquely identified by the public key of its public/private key pair. When a mobile node changes its point of network attachment, its IP address is then changed and the new IP address will be communicated to its correspondent hosts. However, in addition to remaining at an experiment stage for some years, HIP introduces a new layer between the transport and the network layers in the OSI stack. This implies that the host's operating system must be modified in order to use HIP although a user-space implementation does exist.

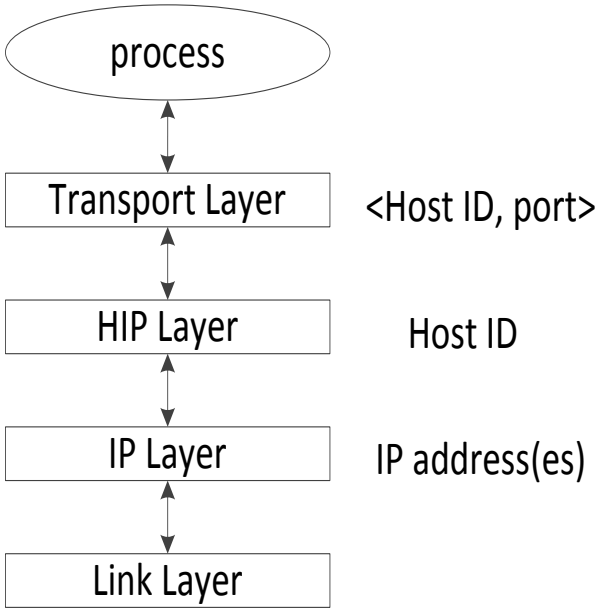

Figure 3. HIP layer within the TCP/IP stack.

In order to provide both security and mobility, HIP has been extended in two subsequent proposals: Hi3 [26] and SPEAR [27]. Previously known as P2P SIP-over-HIP (p2pship), SPEAR was originally designed for SIP-based communication applications (i.e., SIP proxy), allowing users to make peer-to-peer voice / video calls, without the help of a centralized SIP infrastructure. It now supports various protocols and applications. HIP is used as data transport, making the connections secure and enabling features such as mobility and multihoming.

3.4. SIP-based VPN

SIP-based mobile VPN systems have also been proposed in the literature in [28] and [29]. However, the centralized client/server architecture of the Session Initiation Protocol (SIP) implies scalability issues. In addition, SIP-based mobile VPNs are by design only adapted to real-time applications.

3.5. Mobile VPN based upon extension of SSH/SSL

Mobile VPN architectures based on SSH and TLS protocols have been proposed in [30] and [31]. These extensions to the SSH and the TLS protocols allow a session to survive network failures. Designed to support resilient connections, the mobile VPN system presented in [31] can span several sequential TCP connections in order to resist connection failure and IP address change.

The TLS protocol provides a way to resume a TLS session without requiring session-specific state at the TLS server as described in the RFC5077 [32]. In contrast to this technique that stops a session and restarts it later, our system has the ability to always maintain an established session active despite connection failures or network disruptions. SEMOS also makes connection disruptions transparent to the application as opposed to the TLS protocol.

The mobile VPN system presented in [30] introduces a session resumption concept in order to resume sessions without having to renegotiate new session keys. In opposition to the aforesaid schemes, another interesting mobile VPN architecture has been designed by Minglei in [33]. Based on a SOCKSv5 proxy, this mobile VPN system allows to authenticate clients and to build a secure SSL tunnel between users and a SSL gateway that protects their Intranet. However, this system is not scalable and when the SSL gateway is compromised then the entire network can be affected.

3.6. Various mobile VPN systems

FAST VPN [34] is a mobile VPN infrastructure designed for domestic networks. This VPN system creates a virtual Internet Service Provider (vISP) inside a private network. This system allows to establish a secure VPN between users and a vISP. This technical concept capitalizes not only on the high security and privacy given by the VPN but also on the mobility provided by the flexibility of wireless networks. However, FAST VPN is not scalable and provides a restricted service to a private network: it permits only to secure Internet access through an untrusted private network.

There are many other solutions that provide mobility services such as mobile socket based systems [35], [36] the *session-based mobility* [37], the *persistent connection* model [38], the *session layer mobility* (SLM) [39] and the *autonomic mobility management* [40]. Although these systems do not offer security services simultaneously, they allow session continuity despite connection failures.

4. Technical comparison

Each mobile VPN system presented above has its own features. In table 1, we provide an index of a comparison of mobile VPN classes presented in tabulated form (see table 2); we point out the specific features of the various mobile VPN.

Table 1. Index and references to mobile VPN systems.

Index	Mobile VPN solution	Reference(s)
1	Extended SSL/TLS	[31]
2	Extended SSH	[31]
3	IPsec + Mobile IP	[11], [41]
4	HIP	[3]
5	N2N	[2]
6	ELA	[9]
7	FAST VPN	[34]
8	SIP-based	[28]
9	SOCKSV5-based	[33]
10	MOBIKE	[19], [4], [20]

5. Evaluation

In this section, we present a functional analysis as well as the experiment environment and the results of the evaluation of our approach SEMOS [5] and three state-of-the-art solutions, namely: N2N, HIP and MOBIKE.

5.1. Functional Analysis

Table 3 describes the technical comparison between MOBIKE, N2N, HIP and MUSeS. Indeed, all these systems are based on UDP to exchange information in both handshake and re-handshake steps. The SEMOS middleware has the smallest number of exchanged

Table 2. Comparison of mobile/roaming VPN solutions.

Mobile VPN solutions	❶	❷	❸	❹	❺	❻	❼	❽	❾	❿
Mobility support	√	√	limited	√	√		√[a]	√	√	√
NAT traversal	√	√	√	limited	limited[b]	√	√	√	√	√
Seamless roaming	√	√		√	√		√	√	√	√
Centralized PKI	√	√	√				√		√	√
Scalability support				√	√	√				
User authentication		√							√	
Peer authentication	√	√		√	√	√	√	√	√	√
Traffic integrity	√	√	partial[c]	√	√	√	√	√	√	√
DHCP service support	√	√	√[d]	√	√	√	√	√	√	√
Multi-platform support	√		√	√	√		√		√	√
Deployment complexity			√	√				√	√	
Implementation plane	user	user	kernel	kernel	kernel	kernel	user	user	user	kernel

[a] Restricted to a domestic network.
[b] It is not possible to establish a direct connectivity between two peers placed behind symmetric NAT.
[c] Only encapsulated packet is authenticated.
[d] Currently, IPsec tunnel (or transport) mode supports dynamic addressing techniques by means of the "road-warrior" technique. This mechanism enables supporting semi-mobile users.

packets for these two phases of communication. While both HIP and SEMOS proceed through direct connection, MOBIKE is based on indirect secure connection (through an IPSec gateway) and N2N is based on triangular negotiation in both handshake and re-handshake phases. For the two first systems, mobility is limited. This means that only *N2N Edge Node* and *MOBIKE client* can be really mobile.

Security Analysis:. A Mobile VPN enables, in one hand, to secure communication and to keep open application sessions during location change. In other hand, mobile VPN is free to session key renegotiation in the resumption phase. These two technical properties are needed in secure mobile environments. Despite their interesting properties, the systems that operate in autonomous and mobile environments are constantly subject to some security challenges such as DoS and replay attacks.

To prevent replay attacks, SEMOS packets are built by adding sequence number to their headers. In other words, each packet is separately identified by its sequence number added to its header. Thus, when a packet is replayed, it will be automatically detected and subsequently it will be destroyed.

In the resumption phase, a Re-hello is generated and then sent in order to restore interrupted session without using session key renegotiation mechanism. However, Re-hello packet could be replayed because it does not contain a sequence number in order to detect replay attack. Thus, a malicious user that has infiltrated the network could then send a succession of Re-hello packets with the aim of perpetrating Denial-of-Service (DoS) attacks. In addition, the receiver peer cannot determine which oacket is the last one received among other received packets, otherwise this problem could be solved easily. In concrete terms, on receiving Re-hello, the receiver peer processes it in order to resolve and, the challenge and before finishing, it receives another, again another, etc. Finally, the target peer will be saturated by a flooding of Re-hello requests. Furthermore, HIP could be vulnerable to DoS attacks in the resumption phase as shown in the paper analyzing HIP protocol security [42].

To address this security issue, SEMOS assigns a timestamp when sending to each Re-hello packet in order to recognize the freshest request among received requests. In this way, the SEMOS system tries to prevent DoS attacks that use an uninterrupted sequence of Re-hello packets. Due to their mobility, flexibility and autonomy, P2P-based VPN systems are unfortunately not totally invulnerable to intrusion of malicious users. Indeed, in fully decentralized P2P networks, each peer can join and leave the network at any time and usually without any authentication. In our system, authentication is guaranteed by using challenge messages.

Typically, to authenticate a peer over the network, a node encrypts a random challenge message and sends it to its corresponding peer. On receiving this message, the corresponding peer decrypts it and sends the same

message to the initiator peer. Thus, the initiator peer ascertains the identity of the corresponding peer.

The HIP protocol is designed to be resistant to Denial of Service (DoS) and Man in the Middle (MitM) attacks, and when used with ESP enabled, it provides DoS and MitM protection to upper layer protocols, such as TCP and UDP.

In N2N and MOBIKE however, there can be no secure tunnels without a N2N-Super-Node or a MOBIKE-GW. In other words, when N2N-Super-Nodes and MOBIKE-GWs are unavailable, any secure communication is then impossible. The HIP protocol and SEMOS do not suffer from these impairments.

Securing Local Applicative Connections: Although SEMOS offers a solid security mechanism in remote communication between two peers, there is, however, a security weak point in local applicative connections. Unlike communication between two SEMOS peers, local communication between SEMOS and applications is not secured. This means that an unauthorized user application launched by a malicious user should establish connection with a remote honest SEMOS or eavesdrop exchanged traffic between SEMOS and local applications. This untrusted communication should cause security issues.

On the one hand, to prevent external malicious processes to connect to SEMOS, only local applications are authorized to connect to SEMOS by loopback address. On the other hand, only the root user can catch, by using *tcpdump* or *wireshark*, local traffic passed through from local applications to the SEMOS middleware and conversely. Therefore, plain text data exchanged between local applications and SEMOS are protected.

Mobility Analysis:. MOBIKE and N2N are both based upon permanent virtual addresses in order to identify separately mobile nodes. However, when N2N-Super-Node and MOBIKE-Gateway (MOBIKE-GW) change their network points of attachment, any mobility would be possible. Thus, these systems have limited mobility. Indeed, MOBIKE authorizes only the mobility for initiators. However, in addition to mobility, MOBIKE supports also multi-homing for initiators. This means that MOBIKE mobile nodes can have several network interfaces and use them in order to support network link breakdown. In opposition to MOBIKE, all two endpoints of a N2N tunnel keep up mobility.

HIP introduces an interesting scheme of mobility and multi-addressing over IPv4 and IPv6 networks and it is designed to work in a NAT-less environment. Indeed, the HIP hosts do not change identities during location changes; this implies network addresses changes. Each HIP host is identified by its public key that is self-certified, called *Host Identity* (HI). Thus, when a mobile node changes its IP address, it notifies its currently active peers by sending a control packet containing its new location. When correspondent peers change simultaneous their location, the previous notifying method fails and a deadlock will occur. However, HIP introduces a *rendezvous* mechanism in order to address this simultaneous mobility issue. Unlike previous mobility methods, SEMOS proposes a new mobility scheme based on identifiers provided by a DHT infrastructure [43–45].

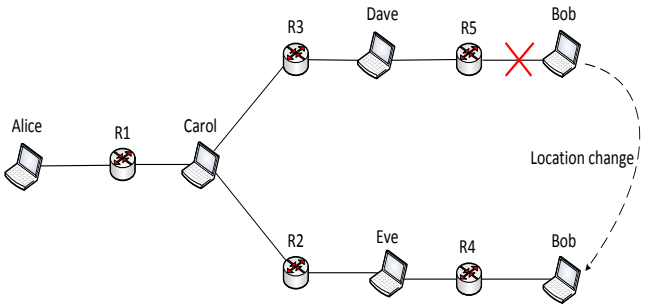

Figure 8. Scenario emulating a location change.

Each SEMOS host is identified separately by a name and an address defined as coordinates taken from the hyperbolic plane.

An *Interruption Detection* mechanism is introduced by SEMOS to detect failures and to subsequently activate the Session Reliability Module (SRM). SRM is based on keepalive messages which are periodically sent. Thus, when network failures occur within lower layers, communication will be temporarily interrupted and failures will be confined within SRM and hidden to higher layers. Due to these properties, mobility is transparent to both user applications running over SEMOS middleware and all the other SEMOS modules, except the SRM component. Therefore, loopback connections established between SEMOS and local applications survive to networks failures despite network attachment point change events, for instance.

5.2. Experiments

In order to assess those four VPN technologies in a mobility scenario, we have used a tool called Network Emulator For Mobile Universes (NEmu), developed by Vincent Autefage and presented in [49]. It is open source and available at [50]. As stated by Lochin *et al.* in [51], using network emulation allows us to accurately evaluate metrics such as delays while taking into account any issues arising from real network stacks as opposed to simulation.

Experiment environment:. An experiment has been carried out with the above implementation in a dynamic environment composed of one mobile node. A mobile

Table 3. Comparison of the evaluated mobile VPN systems.

Mobile VPN system	MOBIKE	N2N	HIP	SEMOS
Handshake packets number	8	3	3	2
Re-handshake packets number	6	3	3	2
Secure connection mode	indirect [a]	triangular [b]	direct	direct
Mobility supported by systems	limited [c]	limited [c]	√	√
Implementation	StrongSwan [46]	n2n [2]	OpenHIP [47]	SEMOS [48]

[a] An IPsec Gateway is needed to establish MOBIKE connections.
[b] Both peers connect to a Super Node before establishing a direct connection.
[c] Only a client (or Edge Node) can be mobile.

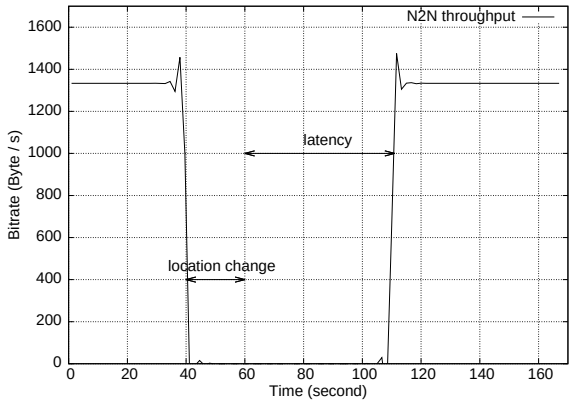

Figure 4. N2N resumption latency.

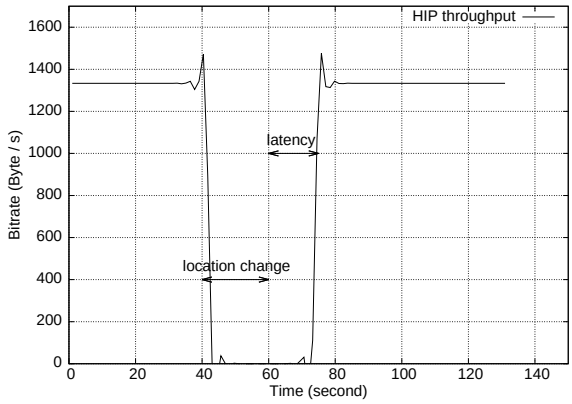

Figure 5. HIP resumption latency.

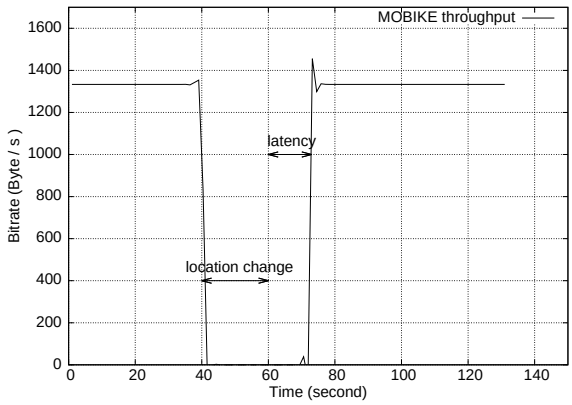

Figure 6. MOBIKE resumption latency.

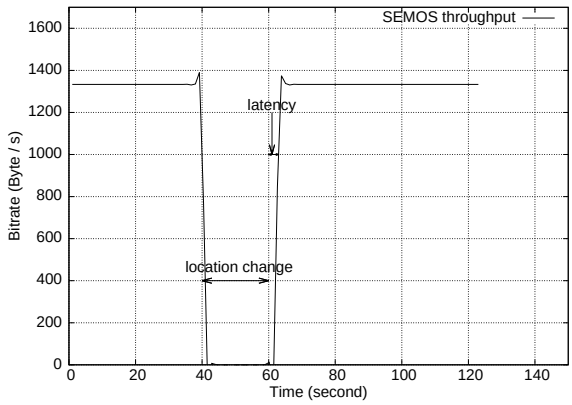

Figure 7. SEMOS resumption latency.

node inside this environment has the ability to leave one network (one virtual router) in order to join another one (another virtual router). This event causes a network failure during the move until a possible subsequent reconnection. This disruption is transparent for the application and it does not prevent the SEMOS system from continuing to run despite the fact that the mobile node is disconnected for a moment. Technically, in our experimentation shown in Figure 8, the node mobility consists in causing an artificial failure on a virtual network interface. We disconnect a virtual wire from a virtual switch and reconnect it on another virtual switch. The SEMOS system hides this network change not only to the user's application but also to the remote

corresponding node. Figure 8 illustrates this *network change* scenario. In this figure, *Bob* communicates with *Alice* when he decides to change its network location. He leaves the network on the left side of router *R5* and he joins the network on the left side of router *R4*. This location change causes a network failure. However, this network disruption is transparent to both *Alice* and *Bob* applications. Subsequently, *Bob* re-contacts *Alice* and their session is therefore transparently resumed.

Experiment results:. We have used a minimal FTP-like application based on the OpenBSD version of *nc*.

Figures 4 to 7 show the evolution of the throughput between the two corresponding applications over time. For all systems, the network interruption happens at the 40^{th} second after the start of the experiment and the throughput instantly drops to zero in the time intervals $[40s; 60s[$. This means that the disruption duration is 20 seconds. The connectivity is reestablished at the network and CLOAK level at the 60^{th} second. However, due to latency, the throughput remains at zero after the 60^{th} second until the effective recovery. This latency varies from one system to another. Indeed, whereas SEMOS middleware has a latency of 3 seconds (see Figure 7), MOBIKE, N2N and HIP protocols have respectively latencies of 12 seconds (see Figure 6), 51 seconds (see Figure 4) and 13 seconds (see Figure 5).

6. Related work

In literature, T. Berger has proposed in 2006 an analysis of current traditionnal VPN technologies [1] whitout mentioning the other class of VPN systems that combine mobility and security properties. Hence, this work could be completed by our contribution provided in this paper. According our investigation on the literature, there are not similar works proposed.

7. Conclusion

In this paper, we have presented a state-of-art on mobile VPN technologies. In this survey, we have provided, in the one hand, a detailed technical analysis on the mobile VPN systems proposed in literature and we have then carried out a comparison between them in tabulated form. In the order hand, we have did experiments on some open source mobile VPN solutions in order to assess their performances and we have pointed out their relevant technical details. Lack of means, disrupted-networks, due to both poor-quality devices and technical skills deficiency, are pervasive in developping countries, particularly in Africa. In theses areas, secured resilent sessions are needed to overcome both security and performance issues inherent to connection disruptions. Therefore, this survey proposes a state-of-the-art on mobile VPN schemes in order to provide to network/security scientists and people eager for knowledge an overview of existing technologies in this area.

References

[1] T. Berger. Analysis of current vpn technologies. In *The First International Conference on Availability, Reliability and Security, ARES 2006.*, page 8 pp., 2006.

[2] Luca Deri and Richard Andrews. N2N. http://www.ntop.org/products/n2n/.

[3] R. Moskowitz and P. Nikander. Host identity protocol (hip) architecture. http://www.ietf.org/rfc/rfc4423.txt, May 2006.

[4] P. Eronen. IKEv2 Mobility and Multihoming Protocol (MOBIKE). http://www.ietf.org/rfc/rfc4555.txt, June 2006.

[5] Daouda Ahmat and Damien Magoni. Muses: Mobile user secured session. In *the 5th IFIP Wireless Days International Conference*, November, 2012, Dublin, Irland.

[6] Andrei Gurtov. *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Wiley, 2008.

[7] Jim Binkley. An Integrated IPsec and Mobile-IP for FreeBSD. *Technical Report*, pages 01–10, October 2001.

[8] Daouda Ahmat, Mahamat Barka, and Damien Magoni. Mobile VPN Schemes: Technical Analysis and Experiments. *Africomm, 8th International Conference on e-Infrastructure and e-Services for Developing Countries, Ouagadougou, Burkina Faso*, pages 88–97, December 6-7, 2016.

[9] S. Aoyagi, M. Takizawa, M. Saito, H. Aida, and H. Tokuda. ELA: A Fully Distributed VPN System over Peer-to-Peer Network. *Proceedings of the Symposium on Applications and the Internet(SAINT'05), IEEE Computer Society, Los Alamitos, CA, USA*, pages 89–92, 2005.

[10] J. Kauffmann. The freelan secure channel protocol. https://github.com/ereOn/libfscp/blob/1.0/fscp.txt, April 2011.

[11] S. Kent and K. Seo. Security Architecture for the Internet Protocol. http://www.ietf.org/rfc/rfc4301.txt, December 2005.

[12] C. Perkins. IP Mobility Support for IPv4. http://www.ietf.org/rfc/rfc3344.txt, August 2002.

[13] Motorolla. Mobile VPN, Secure Connectivity on the Move. *White paper*, 2008.

[14] T. Braun and M. Danzeisen. Secure mobile IP communication. *Local Computer Networks, 2001. Proceedings. LCN 2001. 26th Annual IEEE Conference on*, pages 586–593, 2001.

[15] Heesook Choi, Hui Song, Guohong Cao, and T. La Porta. Mobile multi-layered ipsec. *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, 3:1929–1939, march 2005.

[16] R. Ruppelt, A. Pelinescu, C. Constantin, J. Floroiu, D. Sisalem, and B. Butscher. Building ALL-IP Based Virtual Private Networks in Mobile Environment. *Int. Works. on Informatik and Mobile communication over wireless LAN: Research and applications, Australia*, 2001.

[17] F. Adrangi and H. Levkowetz. Problem Statement: Mobile IPv4 Traversal of Virtual Private Network (VPN)

Gateways. http://www.ietf.org/rfc/rfc4093.txt, 2005.
[18] S. Vaarala and E. Klovning. Mobile IPv4 Traversal across IPsec-Based VPN Gateways. http://www.ietf.org/rfc/rfc5265.txt, 2008.
[19] V. Devarapalli and P. Eronen. Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE). http://www.ietf.org/rfc/rfc5266.txt, june 2008.
[20] M.M. Karbasioun, M. Berenjkub, and B. Taji. Securing mobile IP communications using MOBIKE protocol. *Telecommunications, 2008. ICT 2008. International Conference on*, pages 1–5, june 2008.
[21] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network Mobility (NEMO) Basic Support Protocol. http://www.ietf.org/rfc/rfc3963.txt, 2005.
[22] A. Petrescu and A. Olivereau. Mobile VPN and V2V NEMO for public transportation. *Intelligent Transport Systems Telecommunications,(ITST),2009 9th International Conference on*, pages 63–68, octobre 2009.
[23] K. Ishimura, T. Tamura, S. Mizuno, H. Sato, and T. Motono. Dynamic IP-VPN architecture with secure IPsec tunnels. *Information and Telecommunication Technologies (APSITT), 2010 8th Asia-Pacific Symposium on*, pages 1–5, june 2010.
[24] D. Migault, D. Palomares, E. Herbert, Wei You, G. Ganne, G. Arfaoui, and M. Laurent. E2e: An optimized ipsec architecture for secure and fast offload. In *Availability, Reliability and Security (ARES), 2012 Seventh International Conference on*, pages 365–374, 2012.
[25] L. Deri and R. Andrews. N2N: A Layer Two Peer-to-Peer VPN. *AIMS'08: Proceedings of the 2nd international conference on Autonomous Infrastructure, Management and Security, Berlin, Heidelberg*, pages 53–64, 2008.
[26] Andrei Gurtov, Dmitry Korzun, Andrey Lukyanenko, and Pekka Nikander. Hi3: An efficient and secure networking architecture for mobile hosts. *Comput. Commun.*, 31(10):2457–2467, 2008.
[27] Jookos and Agur. A secure peer-to-peer services overlay architecture, 2010.
[28] S. Huang, Z. Liu, and J. Chen. SIP-based mobile VPN for real-time applications . *Wireless Communications and Networking Conference, IEEE*, Vol. 4:2318–2323, 2005.
[29] T-C. Chen, J-C. Chen, and Z-H Liu. Secure Network Mobility (SeNEMO)for Real-Time Applications. *Mobile Computing, IEEE Transactions on*, Vol. 10:1113–1130, 2011.
[30] J. Schoenwalder, G. Chulkov, E. Asgarov, and M. Cretu. Session Resumption for the Secure Shell Protocol. *Integrated Network Management, 2009. IM '09. IFIP/IEEE International Symposium on*, pages 157–163, 2009.
[31] T. Koponen and P. Eronen. Resilient Connections for SSH and TLS. *Proceeding of USENIX Annual Technical Conference*, May 2006. Boston.
[32] J. Salowey, H. Zhou, P. Eronen, and H. Tschofenig. Transport Layer Security (TLS) Session Resumption without Server-Side State. http://www.ietf.org/rfc/rfc5077.txt, January 2008.
[33] S. Minglei, T. Chengxiang, and W. Haihang. Mobile VPN Scheme Based on SOCKS V5. *Machine Vision and Human-Machine Interface (MVHI), International Conference on*, pages 792–795, April 2010.
[34] A. Zúquete and C. Frade. Fast VPN Mobility Across Wi-Fi Hotspots. *Security and Communication Networks (IWSCN), 2nd International Workshop on, IEEE Karlstad, Sweden*, pages 1–7, 2010.
[35] X. Qu, J. Xu Yui, and R. P. Brent. A Mobile TCP Socket. *Proceedings of the IASTED International Conference on Software Engineering, San Francisco, CA*, November 1997.
[36] T. Okoshi, M. Mochizuki, Y. Tobe, and H. Tokuda. MobileSocket: Toward Continuous Operation for Java Applications. *Intational Conference on Computer Communications and Networks*, pages 50–57, October 1999.
[37] A. Snoeren. A Session-Based Approach to Internet Mobility. *PhD thesis, Massachusetts Institute of Technology*, 2002.
[38] Y. Zhang and S. Dao. A "Persistent Connection" Model for Mobile and Distributed Systems. *Proceedings of the 4th International Conference on Computer Communications and Networks (ICCN' 95), Las Vegas, Nevada*, September 1995.
[39] B. Landfeldt, T. Larsson, Y. Ismailov, and A. Seneviratne. SLM, a framework for session layer mobility management. *Proceedings of the 18th International Conference on Computer Communicants and Networks (ICCCN' 99), Boston, MA*, pages 452–456, October 1999.
[40] Meriem Abid, Daniel Macedo, Javier Rubio-Loyola, and Guy Pujolle. An autonomic mobility management solution for the future wireless internet. *Annals of Telecommunications*, 67(11-12):523–536, 2012.
[41] C. Perkins et al. Mobile ipv4 traversal across ipsec-based vpn gateways. http://www.ietf.org/rfc/rfc5944.txt, November 2010.
[42] Tuomas Aura, Aarthi Nagarajan, and Andrei Gurtov. Analysis of the hip base exchange protocol. In *In 10th Australasian Conference on Information Security and Privacy (ACISP 2005)*, pages 481–494, 2005.
[43] Telesphore Tiendrebeogo, Damien Magoni, and Oumarou Sié. Virtual internet connections over dynamic peer-to-peer overlay networks. In *Proceedings of the 3rd International Conference on Evolving Internet*, pages 58–65, 2011.
[44] Telesphore Tiendrebeogo, Daouda Ahmat, Damien Magoni, and Oumarou Sié. Virtual connections in p2p overlays with dht-based name to address resolution. *International Journal on Advances in Internet Technology*, 5(1):11–25, 2012.
[45] Telesphore Tiendrebeogo, Daouda Ahmat, and Damien Magoni. Évaluation de la fiabilité d'une table de hachage distribuée construite dans un plan hyperbolique. *Technique et Science Informatique, TSI, Volume 33 - n° 4/2014, Lavoisier*, pages 311–341, Juin 2014.
[46] Andreas Steffen. StrongSwan. http://www.strongswan.org.
[47] Tom Henderson. OpenHIP. http://www.openhip.org.
[48] Daouda Ahmat. SEcure MObile Session. http://www.labri.fr/perso/magoni/cape/.
[49] Vincent Autefage and Damien Magoni. Network emulator: a network virtualization testbed for overlay experimentations. In *Proceedings of the 17th IEEE International Workshop on Computer-Aided Modeling*

Analysis and Design of Communication Links and Networks, pages 38–42, 2012.
[50] Vincent Autefage. NEmu. http://nemu.valab.net/.
[51] Emmanuel Lochin, Tanguy Perennou, and Laurent Dairaine. When should i use network emulation? *Annals of Telecommunications*, 67(5-6):247–255, 2012.