An SD-WAN Approach for EUt+ Network

Iustin-Alexandru IVANCIU, Ph.D.
Eng. Robert BOTEZ
Eng. Călin-Marian IURIAN
Eng. Aron-Valeriu DUMITRESCU
Tudor-Mihai BLAGA, Ph.D.
Virgil DOBROTĂ, Ph.D.

E-mail: iustin.ivanciu@com.utcluj.ro

Outline

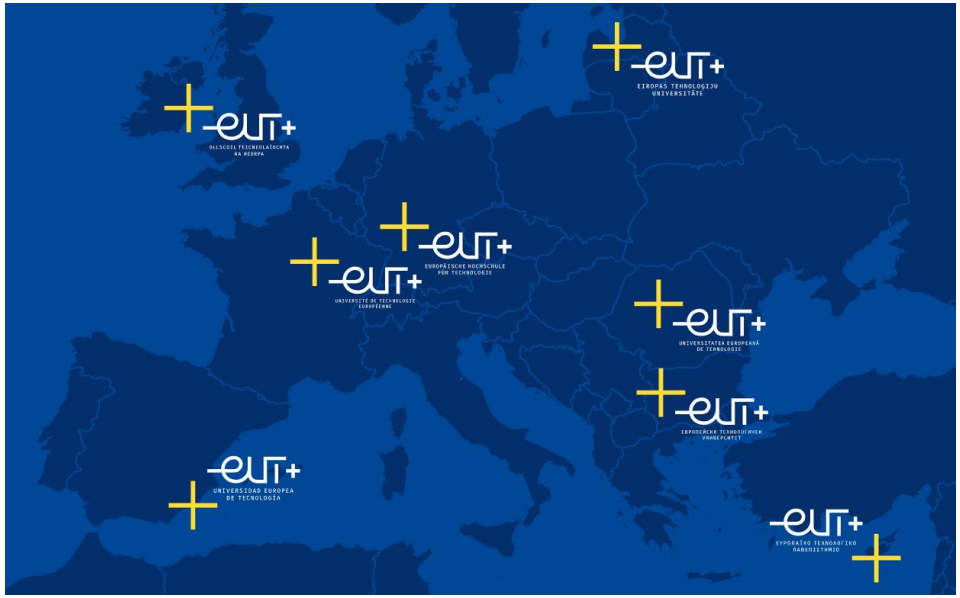
- Introduction
- Software-Defined Wide Area Network (SD-WAN)
- Management and Orchestration (MANO)
- Homomorphic Encryption
- Implementation
- Experimental Results
- Conclusions and Future Work

Introduction

- **European University of Technology (EUt+)**
  - 8 European universities
  - 100,000 students
  - Physical and virtual mobility
  - Recognized diploma and qualification for labor market
  - European Credit Transfer and Accumulation System

Introduction

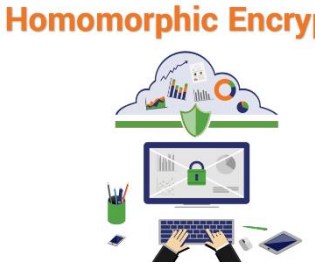
- **Framework**
  - Mobility
  - Quality of Experience
  - Data privacy



Introduction

- **Challenges**
  - Flexibility and scalability
  - Accessibility
  - Traffic engineering
  - Security

- **Solutions**
  - SD-WAN
  - MANO
  - Homomorphic encryption



SD-WAN

- **Goals**
  - Simplify networking operations
  - Optimize management and control
  - Enable better scalability and flexibility

- **Solutions**
  - B4 by Google, SWAN by Microsoft
  - ONOS, HyperFlow, Onix
  - OpenFlow, Payless

MANO

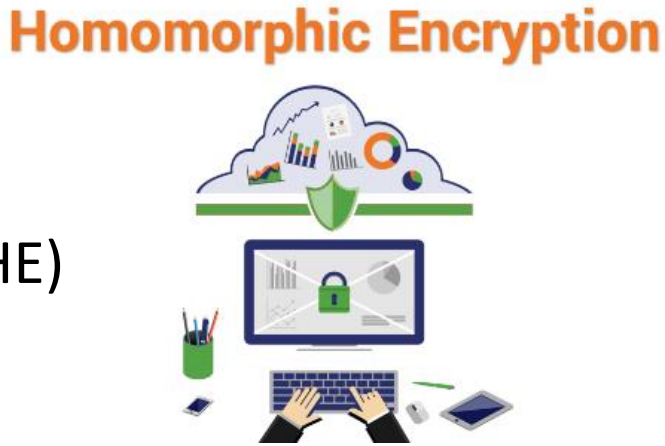
- **Network Functions Virtualization (NFV)**
  - Decouple the network functions from the hardware
  - Virtualized Network Functions (VNF)
  - Create, manage, scale and migrate VNFs
  - Management and Orchestration (MANO)

- **NFV MANO**
  - Framework proposed by the ETSI ISG NFV
  - Open Network Automation Platform
  - Open Source MANO

Homomorphic Encryption

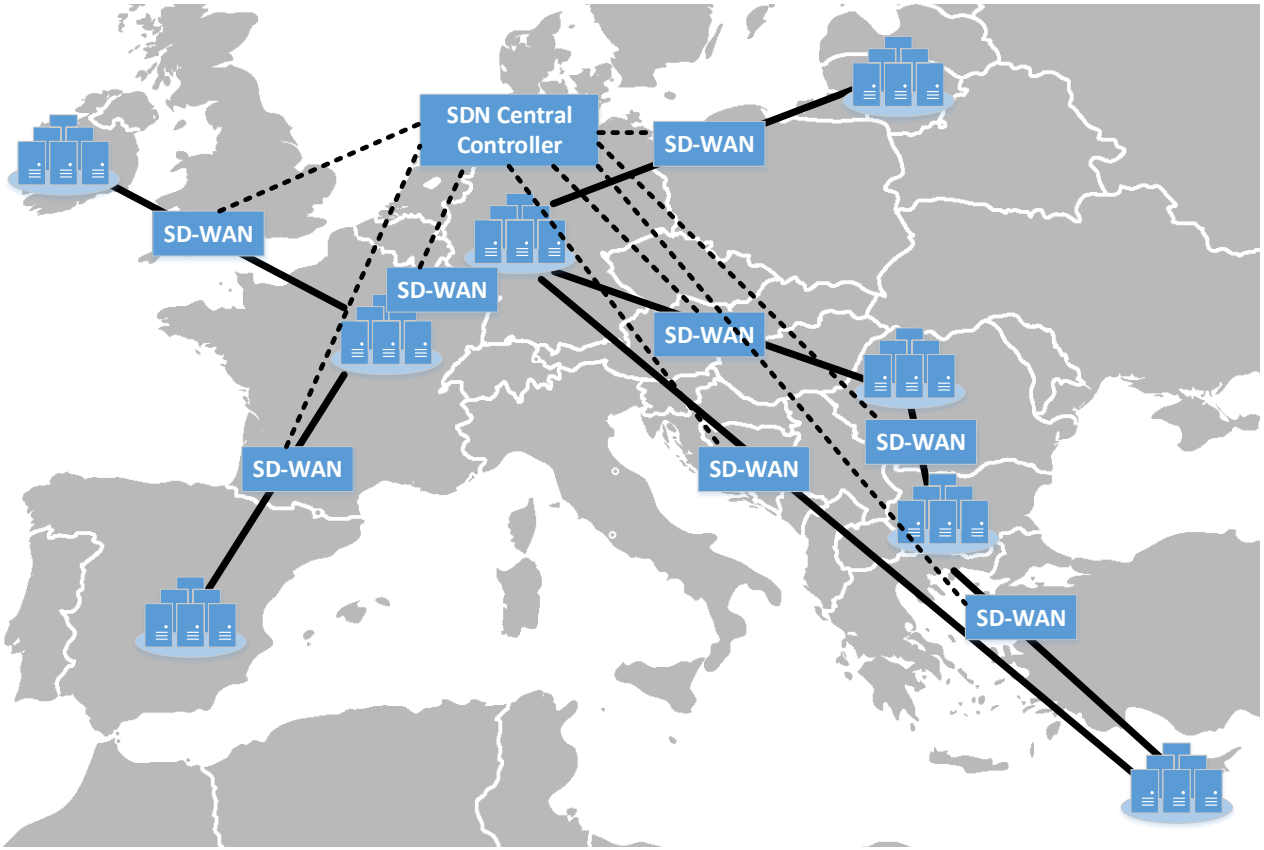
- **Legacy encryption techniques**
  - Processing on unencrypted data
  - Complex processing on the client side
  - Numerous data transfers = vulnerability to attacks

- **Homomorphic encryption**
  - Processing on encrypted data
  - Fully homomorphic encryption (FHE)
  - Practical in certain scenarios



Implementation

- **Proposed architecture**



Implementation

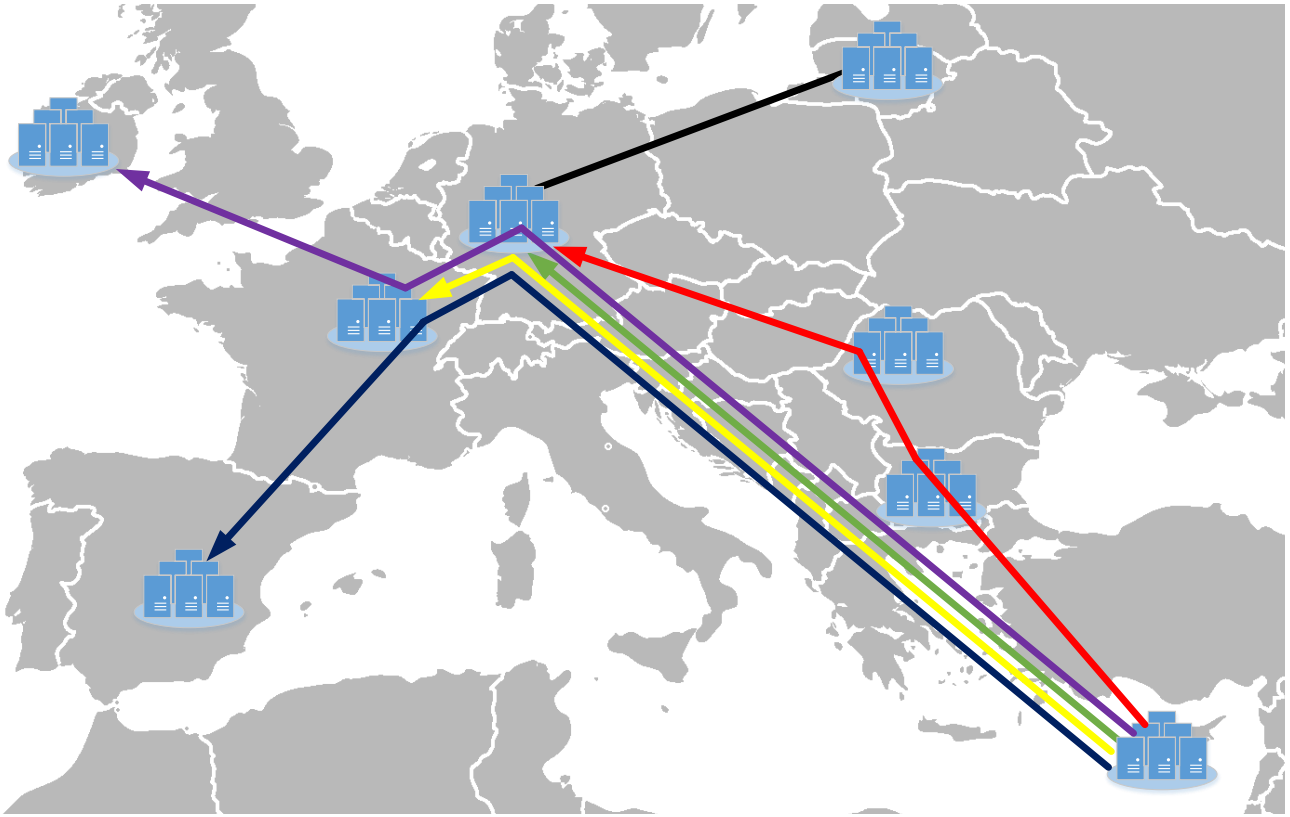
- **Network deployment and scalability**
  - Open^3++ software package
  - Multi-domain NS deployment
  - Orchestration-proxy daemon
  - Resource Orchestrator
  - Virtual Infrastructure Manager (VIM) – compute domain
  - WAN Infrastructure Manager (WIM) – network domain

Implementation

- **Network traffic management**
  - Two-layer mechanism
    - WIMs – decide how to use the resources on each link
    - Central SDN controller – finds the best path across the network
  - Monitored data
    - Link resources – ATR and OWD
    - Flow-related statistics
  - Quality of Experience
    - Traffic priority
    - Prediction
    - Real-time QoE feedback

Implementation

- **Network traffic management**



Implementation

- **Network security**
  - Secure data transfer
    - Legacy solution – TLS
  - Secure data storage
    - FHE – distributed database system
  - Processing on encrypted data
    - Personal records
    - Flow and link-related information
    - Prediction

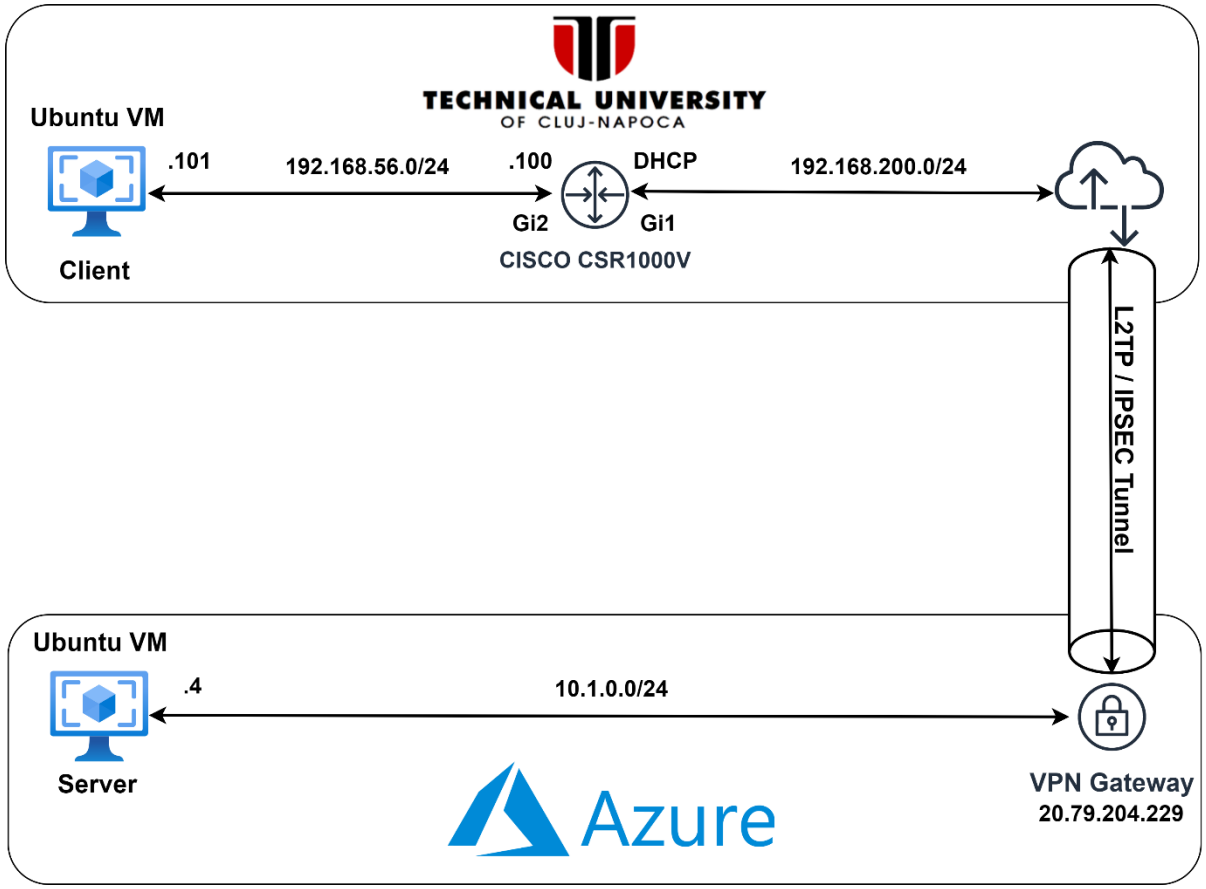
Experimental Results

- **Solution tested in the TUCN MAN**

University	Number of students
Technical University of Sofia (Bulgaria)	20,000
Cyprus University of Technology (Cyprus)	3,000
University of Technology of Troyes (France)	3,000
Hochschule Darmstadt - University of Applied Sciences (Germany)	15,000
Technological University Dublin (Ireland)	28,500
Riga Technical University (Latvia)	14,000
Technical University of Cluj-Napoca (Romania)	22,000
Polytechnic University of Cartagena (Spain)	6,500

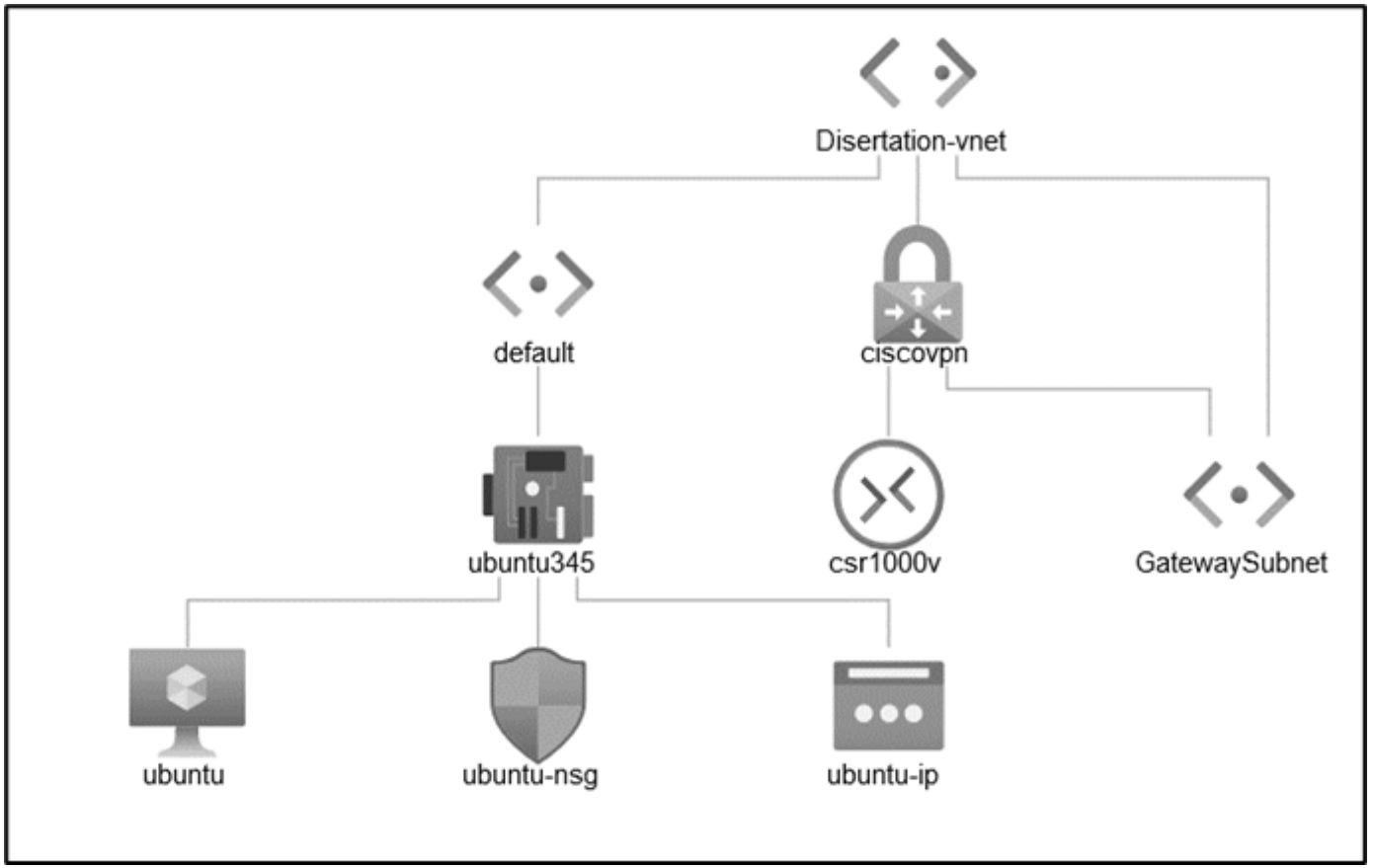
Experimental Results

- **Evaluate the SD-WAN proposed architecture**



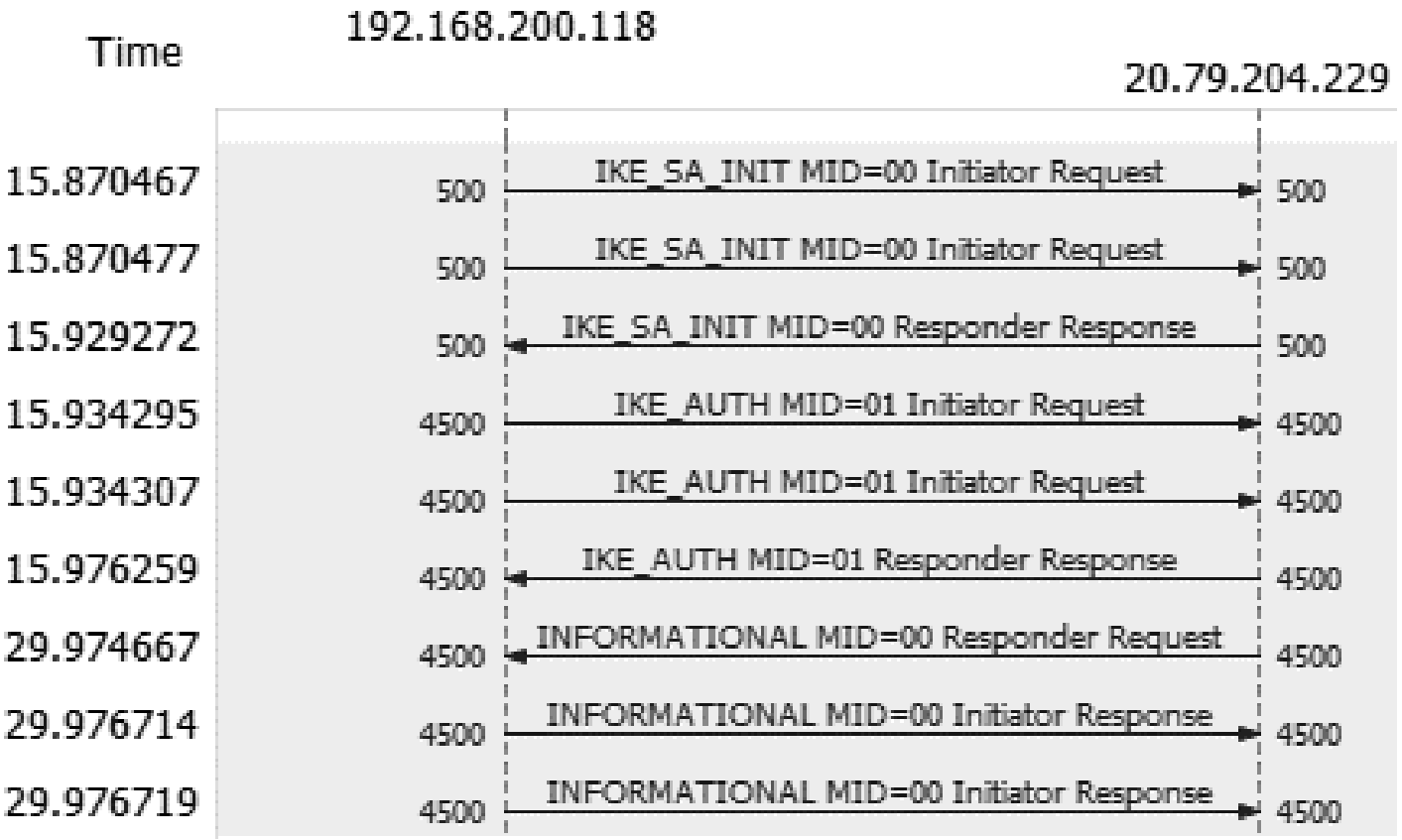
Experimental Results

- **Network topology in Azure**



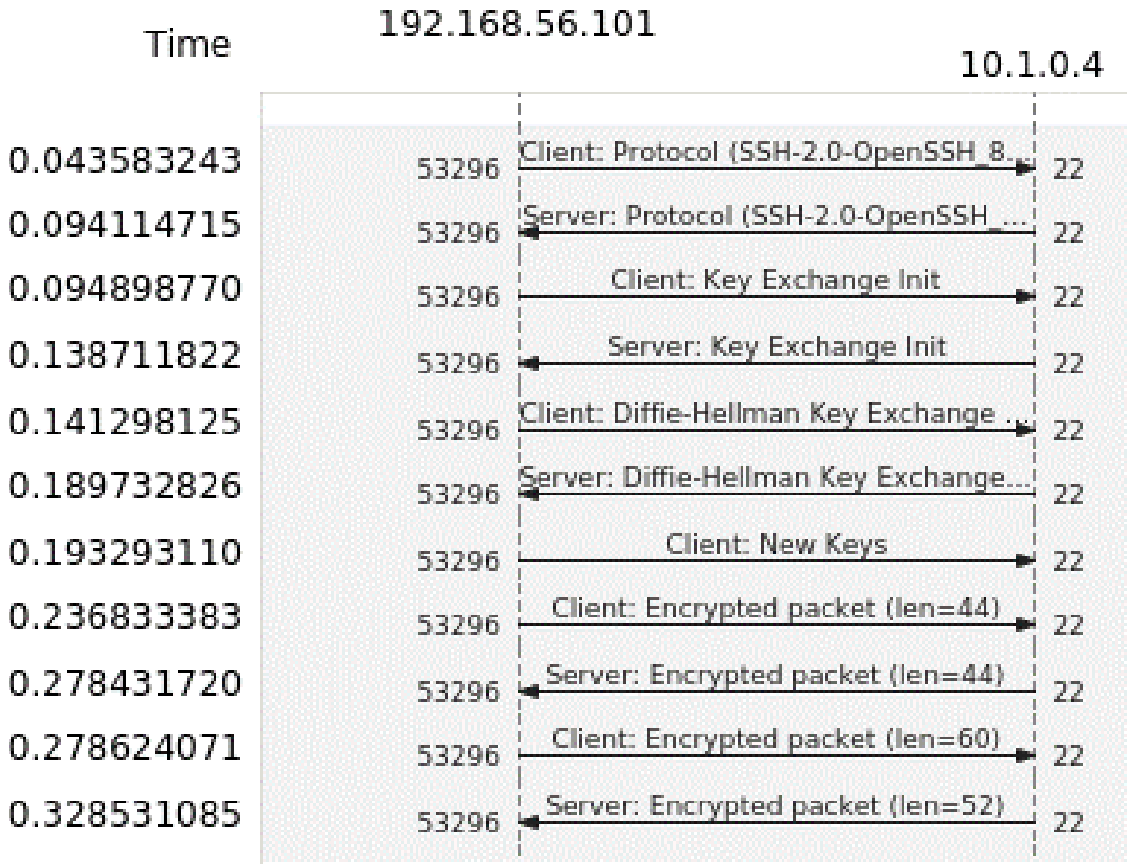
Experimental Results

- **IPSec tunnel creation**



Experimental Results

- **Client-server SSH connectivity**



Conclusions and Future Work

- **Conclusions**
  - Framework for EUt+
  - Physical and virtual mobility
  - Quality of Experience
  - Data privacy
  - Proof-of-work SD-WAN secure solution
- **Future work**
  - Include SD-WAN controller
  - Extend to multiple domains

Acknowledgement

This paper was financially supported by the Project **Entrepreneurial competences and excellence research in doctoral and postdoctoral programs "ANTREDOC",** project co-funded by the European Social Fund financing agreement no. 56437/24.07.2019

References

1. European University of Technology (EUt+), 2021, Available: https://www.univ-tech.eu.
2. Z. Yang, Y. Cui, B. Li, Y. Liu and Y. Xu, "Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities," 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 2019, pp. 1-9, doi: 10.1109/ICCCN.2019.8847124.
3. G. Yilma, Z. Yousaf, V. Sciancalepore and X. Costa-Perez, "Benchmarking open source NFV MANO systems: OSM and ONAP," Computer Communications, vol. 161, pp. 86-98, 2020, doi: 10.1016/j.comcom.2020.07.013.
4. A. Chatterjee and K. M. M. Aung, "Fully Homomorphic Encryption in Real World Applications", Singapore:Springer, 2019.
5. H. Yousuf, M. Lahzi, S. Salloum and K. Shaalan, "Systematic Review on Fully Homomorphic Encryption Scheme and Its Application", Studies in Systems, Decision and Control, pp. 537-551, 2020, doi: 10.1007/978-3-030-47411-9_29.
6. X. Yi, R. Paulet and E. Bertino, "Homomorphic Encryption and Applications" in Springer Briefs in Computer Science, Springer, 2014, ISBN 978-3-319-12228-1.
7. R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978, doi:

References

8. C. Gentry, "Fully homomorphic encryption using ideal lattices", Proceedings of the 41st annual ACM symposium on Symposium on theory of computing - STOC '09, 2009, doi: 10.1145/1536414.1536440.
9. C. Hong et al., "B4 and after", Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication, 2018, doi: 10.1145/3230543.3230545.
10. C. Hong et al., "Achieving high utilization with software-driven WAN", Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, 2013, doi: 10.1145/2486001.2486012.
11. P. Berde et al., "ONOS: towards an open, distributed SDN OS", Proceedings of the third workshop on Hot topics in software defined networking, 2014, doi: 10.1145/2620728.2620744.
12. A. Tootoonchian, Y. Ganjali, “Hyperflow: A distributed control plane for openflow,” in Proc. of the 2010 internet network management conference on Research on enterprise networking, https://static.usenix.org/event/inm10/tech/full_papers/Tootoonchian.pdf.
13. T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama et al., “Onix: A distributed control platform for large-scale production networks.” in USENIX OSDI (2010), Available: https://static.usenix.org/events/osdi10/tech/full_papers/Koponen.pdf.
14. N. McKeown, et al., “Openflow: enabling innovation in campus networks,” ACM SIGCOMM Computer Communication Review, 2008, Available: https://dl.acm.org/doi/abs/10.1145/1355734.1355746.

References

15. S. R. Chowdhury, M. F. Bari, R. Ahmed and R. Boutaba, "PayLess: A low cost network monitoring framework for Software Defined Networks," 2014 IEEE Network Operations and Management Symposium (NOMS), Krakow, Poland, 2014, pp. 1-9, doi: 10.1109/NOMS.2014.6838227.
16. P. Karamichailidis, K. Choumas and T. Korakis, "Enabling Multi-Domain Orchestration using Open Source MANO, OpenStack and OpenDaylight," 2019 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), Paris, France, 2019, pp. 1-6, doi: 10.1109/LANMAN.2019.8847036.
17. I.A. Ivanciu, "Active Measurements for Routing in Cloud-Based Networks", Technical University of Cluj-Napoca, Romania, 2016, https://rei.gov.ro//teza-doctorat, Cod dosar: F-CA-4044/03.01.2017.
18. A. Taut, I.A. Ivanciu, E. Luchian, and V. Dobrota, "Active Measurement of the Latency in Cloud-Based Networks", ACTA TECHNICA NAPOCENSIS, Electronics and Telecommunications, ISSN 1221-6542, Vol.58, No.1, 2017, pp.22-30.
19. I. Ellawindy and S. Heydari, "Crowdsourcing Framework for QoE-Aware SD-WAN", 2020. Available: 10.21203/rs.3.rs-31021/v2 [Accessed 8 April 2021].
20. Y. Gahi, M. Guennoun and K. El-Khatib, "A secure database system using homomorphic encryption schemes", Computer Science, pp. 54-58, 2015.
21. R. Shrestha and S. Kim, "Integration of IoT with blockchain and homomorphic encryption: Challenging issues and opportunities", Advances in Computers, pp. 293-331, 2019, doi:: 10.1016/bs.adcom.2019.06.002.

References

22. M. Rahman, I. Khalil, M. Atiquzzaman and X. Yi, "Towards privacy preserving AI based composition framework in edge networks using fully homomorphic encryption", Engineering Applications of Artificial Intelligence, vol. 94, p. 103737, 2020, doi: 10.1016/j.engappai.2020.103737.
23. GÉANT - Pan-European data network for the research and education community, 2021, Available: https://www.geant.org/
24. R. Botez, J. Costa-Requena, I.A. Ivanciu, V. Strautiu and V. Dobrota, "SDN-Based Network Slicing Mechanism for a Scalable 4G/5G Core Network: A Kubernetes Approach", Sensors, vol. 21, p. 3773, 2021, doi: https://doi.org/10.3390/s21113773.
25. C. Gheorghe, C. Iurian, E. Luchian, I. Ivanciu and V. Dobrota, "Applications of the Cisco APIC-EM software-defined networking controller for a virtualized testbed," 2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2017, pp. 1-6, doi: 10.1109/ROEDUNET.2017.8123731.