Security Orchestration Framework for Federated Network Slicing

Shalitha Wijethilaka*, Madhusanka Liyanage†
*†School of Computer Science, University College Dublin, Ireland
†Centre for Wireless Communications, University of Oulu, Finland
Email: *mahadurage.wijethilaka@ucdconnect.ie, †madhusanka@ucd.ie, †madhusanka.liyanage@oulu.fi

***Abstract*—Network slicing is a utilitarian technology in future mobile networks that can facilitate heterogeneous network requirements of a plethora of applications over a shared physical network cost-effectively. Federated slicing, an extension of conventional network slicing, allows network services across multiple administrative domains in a seamless manner. Management of security operations in such a system is a cumbersome activity. This paper proposes a framework to simplify the security orchestration in a federated network slicing system to support efficient security management in 5G and beyond networks. Probable advantages and the potential implementation challenges of the proposed framework are discussed in the paper.**

***Index Terms*—Network Slicing, Security**

I. Introduction

The "One size fits all" concept does not fit with future mobile networks due to the diverse network requirements of heterogeneous applications [1]. Along with the advent of the Fifth Generation (5G) architecture, telecommunication networks tend to have a myriad of new features. Among those, network slicing is becoming one of the predominant technologies in future mobile networks that eliminate the static nature of traditional networks [2]. Allocation of dedicated logical networks, known as "network slices", for each application on top of the shared physical network, can be defined as the concept of network slicing [3]. Diverse network characteristics can be provided to various applications by altering the network function arrangement of the slices.

Network slices allocated to different applications may stretch over large geographical areas that can't be covered by a single Mobile Network Operator (MNO) [4]. Hence allocated network slices are required to be expandable over multiple administrative domains. Moreover, users are demanding global connectivity to have a unified service experience, even when roaming across different operators globally. Federated Network Slicing facilitates this requirement by seamless platform sharing between operators to ensure a better user experience. Moreover, the necessity of having individual agreements with different operators is eliminated in this concept by allowing operators to provide the network service globally [5].

Mobile networks are vulnerable to several security challenges such as Distributed Denial of Service, botnets, Man in The Middle (MITM), and zero-days [6]. When considering a network slicing ecosystem, the attack space is even more significant. Moreover, the facilitation of diverse security requirements of different applications is a convoluted operation. Along with the augmentation of network slices within a single MNO, managing the security operations within the slicing ecosystem becomes complex. Security management of federated slicing is even more challenging due to the scattering nature of the security functions across multiple domains.

II. Proposed architecture

The proposed framework mainly introduces two entities to a federated network slicing ecosystem: A local Security Orchestrator (LSO) and a Global Security Orchestrator (GSO). Figure 1 illustrates theses two proposed elements that span over three administrative domains in the federated slicing system to create a single Network Slice Instance (NSI). The upper section of the figure 1 illustrates the modular level diagrams of the proposed orchestrators. Each orchestrator contains a set of modules, and the primary operations of each module are as follows.

- **Slice Security Monitoring Element (SLME):** monitor performance and operation of the slice.
- **Data Evaluation Element (DEE):** perform all the decision taking activities.
- **Security Life-Cycle Management Element (SLCME):** manage the life-cycle of security functions.
- **Security Policy Management Element (SPME):** translate the security requirements in to configurations.
- **Security Information Repository (SIR)**: store all the security related information.
- **Security Solution Deployment Element (SSDE):** trigger NSM to perform security configurations.

The LSO is responsible for managing security operations within a single MNO. When considering a federated slicing system, the number of LSOs is equal to the number of domains in the system. It monitors the network slices within the local environment. According to the monitored information, it can identify ongoing security attacks. Deciding the required security function to mitigate the security attack in the local environment, alerting the relevant parties regarding the attack, and triggering the GSO about the ongoing attack, are the other functionalities of the LSO. Furthermore, life-cycle management (acceptance, installation, deployment, evaluation, maintenance, and disposal) of the security functions within the slices is also performed by the LSO.

The GSO is responsible for managing the security operations within the federated system. It receives the security

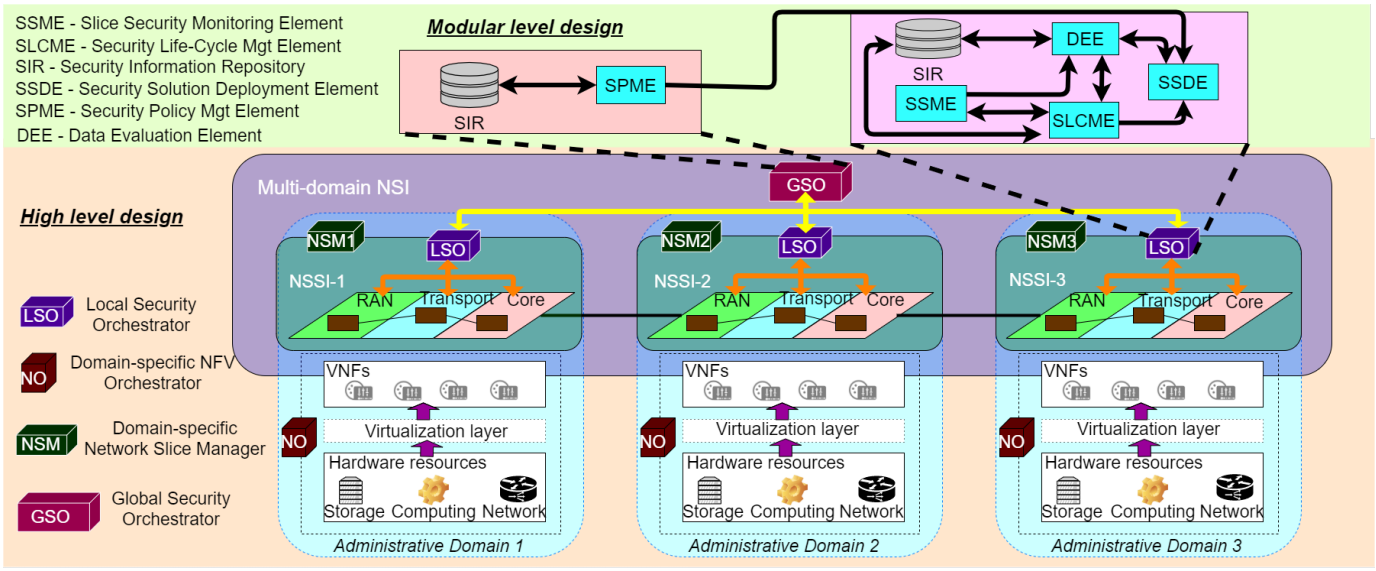

Fig. 1: The architecture of the security orchestration framework

requirements from tenants at the time of slice creation. The accepted security requirements are converted into security configurations. Then, derived security configurations are sent to each LSO. Each LSO performs the received security configurations within their local environments. If MNO specific security configurations exist, they can be directed to the LSO. The LSO executes them within the relevant local slice.

III. Discussion

A. Expected Benefits

The number of MNOs that combine to create a slice is not static, and sometimes the slices are required to be extended across new administrative domains. The proposed architecture is designed to be horizontally scalable to facilitate this requirement. While re-active security mechanisms can be performed within each domain via the proposed solution, pro-active security mechanisms can be deployed over multiple domains straightforwardly. Modularised designs of the proposed entities simplify the management operations in the framework. Resources are scarce in telecommunication networks. Hence, allocating a dedicated amount of resources for security operations is not efficient. The proposed framework offers the capability to allocate resources for security operations when needed. Moreover, the ability to manage the life-cycle of security functions according to the severity of the attack further improves resource utilisation efficiency.

B. Implementation Challenges and Solutions

When the number of administrative domains increases, the workload that is expected to be handled by the GSO increases. Hence the GSO becomes a resource starving element, and it can be a bottleneck of the system. For the optimal operation of the framework, the connectivity between the LSOs and the GSO is mandatory. The connectivity issues between them may disrupt the overall functionality of the system. Therefore standard algorithms and protocols need to be developed to facilitate re-active and pro-active security mechanisms. Minimizing human intervention is also an essential requirement in future mobile networks. Developing novel Artificial Intelligence/ Machine Learning (AI/ML) methods and aligning the framework with ETSI's Zero-touch network & Service Management (ZSM) framework are the possible courses of action to automate the functionality of the orchestration framework.

IV. Conclusion

Network slicing is an indispensable technology in future mobile networks. Federated slicing enables the stretching of network slices among multiple MNOs to provide network services for various applications. Security orchestration is a key requirement for a federated slicing system. The proposed framework can perform security orchestration in such a system with added advantages. The identified weaknesses of the proposed framework are potential future research directions.

References

[1] C. de Alwis, A. Kalla, Q. V. Pham, P. Kumar, K. Dev, W. J. Hwang, and M. Liyanage, "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," *IEEE Open Journal of the Communications Society*, pp. 1–1, 2021.

[2] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," *IEEE Communications Surveys & Tutorials*, 2021.

[3] N. Alliance, "Description of network slicing concept," *NGMN 5G P*, vol. 1, no. 1, 2016.

[4] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, "On multi-domain network slicing orchestration architecture and federated resource control," *IEEE Network*, vol. 33, no. 5, pp. 242–252, 2019.

[5] (2017) World's first 5g federated network slicing grants global reach. [Online]. Available: https://www.prnewswire.com/in/news-releases/worlds-first-5g-federated-network-slicing-grants-global-reach-613826083.html

[6] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements and future directions," *IEEE Communications Surveys & Tutorials*, 2019.