Securing Multi-Agent Systems for Near Real-Time Control of 6G Services

L. Velasco[*], M. Ruiz and P. González
Universitat Politècnica de Catalunya
Barcelona, Spain
[*]luis.velasco@upc.edu

V. Lefebvre
TAGES SARL
Le Cannet, France

C. J. Bernardos
Universidad Carlos III de Madrid
Madrid, Spain

A. Muñiz
Telefónica I+D
Madrid, Spain

Abstract—**Multi-agent systems (MAS) have been proposed as an alternative to traditional centralized control for near real-time service control. However, MAS also show a distributed attack surface. To overcome their software higher security exposure, we combine a set of scalable techniques fostering enhanced security applied on individual agents and their communications. Specifically, the proposed solution combines: *i*) binary hardening with secure execution monitoring; *ii*) distributed ledger technologies for non-real-time MAS management; and *iii*) VXLAN and encrypted communications for near real-time MAS operation. The solution is designed not only to provide strong security to the MAS, but also to minimize any functional overhead.**

Keywords—Secure multi-agent systems; Near real-time control; 6G services

I. Introduction

Autonomous network operation is required to deal with the expected large traffic dynamicity and provide the stringent performance required by beyond 5G and 6G services. Solutions for autonomous operation running in a centralized controller have the potential to greatly reduce costs, but they might lead to inefficient resource utilization because of their long response times. To minimize response time, control algorithms might be executed as close as possible to the data sources.

In our previous work in [1], we proposed a distributed autonomous flow routing running in the packet nodes, following the concept of multi-agent systems (MAS) [2]. MAS can be defined as a set of individual agents that share knowledge and communicate with each other in order to solve a problem that is beyond the scope of a single agent. In the field of networking, we proposed agent nodes making autonomous decisions near real-time, based on guidelines received from the centralized controller/orchestrator. However, such solution presents several security issues due to its distributed nature.

In this paper, we carry out a systematic thread analysis of the MAS solution and propose a set of complementary solutions to secure both agents' execution and inter-agent communications.

II. Requirements

Agents are software entities controlling the operation of different types of network nodes (e.g., radio access network elements, and packet switches and routers). Their monitoring and control abilities augment their exposure to all types of software attacks, typically spawning denial of service. Agent security is a multi-pronged activity, covering confidentiality, integrity and availability preservation over the different life cycles (e.g., deployment, execution). Complementary to individual agent security assurances, MAS collaborative processing implies to foster a trust relationship between agents. Trustworthiness shall be timely established as it evolves over time. E.g., a trustworthy agent can evolve to corrupted or suspicious as it was targeted by an attacker during its operation.

To meet the goal of maintaining trustworthiness over time, a runtime monitoring of the agent's *healthy* condition shall be set. More precisely, agents shall be able to monitor their current execution conditions, provided that the measurements themselves and the periodicity used to deliver these measurements should not impact on agents' performance. Note that such dynamic healthy condition is a security increment as compared to a classical competing implementation without health measures.

MAS communications should be secured. In this regard, distributed ledger technologies (DLT) have recently attracted attention, as they avoid the need of a centralized authority for transaction information among peers, which fits very well with the concept of MAS. In brief, a distributed ledger is just a distributed database capable of recording all transactions between anonymous peers in a secure and time-stamped way. These transactions can contain any type of data. To add new data, these must be validated by the participant nodes though the use of a *consensus* mechanism. There are different consensus mechanisms that provide different levels of security, trust, and privacy. Several applications of DLT in the context of 5G services have been proposed [3] and showed that the consensus mechanism is key for the overall performance. However, even with the simplest consensus mechanism, data exchange can be slow for near real-time applications.

III. Proposed Solution

In view of the requirements revealed in the previous section, we propose the solution sketched in Fig. 1 for securing MAS based on the following ingredients: *i*) secure execution monitoring; *ii*) non-real-time MAS management; and *iii*) near real-time MAS operation.

A. Secure Execution Monitoring

Agents need to be hardened for higher resilience against various attacks and monitored to establish trust in a timely manner. To that end, we consider the initial set of measures made of proven evidences related to: *i*) the effectiveness of agents' actual execution; *ii*) the validity of the authentication of the agent at its start-up phase; and *iii*) the agent last runtime integrity measurement check passed. Further healthy measurement can be considered typically through an accurate tracing of the software control flow during execution, a method to infer any type of software attacks including vulnerability exploitation. This method can also be used to explicitly notify that the agent control flow does not deviate from the normal. A few changes on the agents' software need to be carried out.

The research leading to these results has received funding from the European Commission thought the HORIZON SNS JU DESIRE6G (G.A. 101096466) and the MICINN IBON (PID2020-114135RB-I00) projects, and from ICREA.

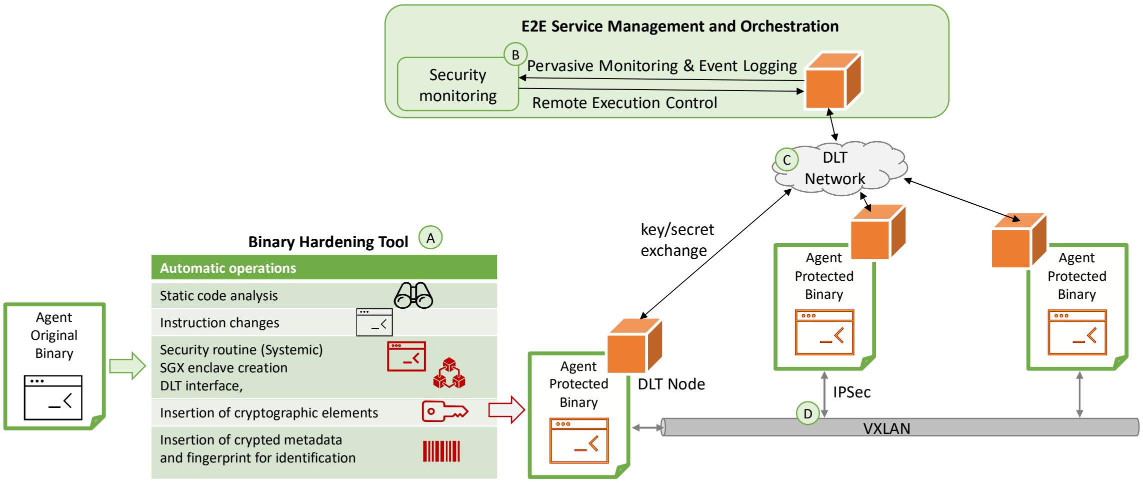

Fig. 1 - Proposed solution for Secure MAS: binary hardening tool (A), integrity monitoring (B), DLT (C) and IPSec + VXLAN (D)

These changes can either result from source level changes or be applied directly on the agent executable file, prior to deployment. Fig. 1(A) shows how original agents are loaded into the binary hardening tool and transformed into protected variants, which are both hardened against the confidentiality and integrity loss attempts and monitored by interfacing with the ledger. The global agent's integrity consists of checking that the agent has not been tampered by interception before being loaded, has not been tampered by local memory introspection during its execution, and that the agent is effectively running. The last criterion enables to infer denial of service attacks on the agent or on its platform by resource attrition. The monitoring delivers periodic integrity and activity status to an application running in the service orchestrator (labeled B in Fig. 1).

B. *DLT for Non-Real-Time Secure MAS Management*

We rely on a lightweight application-based DLT overlay for maintaining the highest level of trust between agents, ingesting and processing new trustworthiness software marks as delivered by the binary hardening tool and reflecting the healthy condition of the agents. DLTs' characteristics make them a great candidate to be an enabler for dynamic multi-agent association and key/secret exchange. Together with the service orchestrator, agents can dynamically register into the DLT (labeled C in Fig. 1), and smart contracts can be used to regulate and monitor each dynamic association between agents. A service level agreement can be defined for each association, thus monitoring the required level of service for the communication. An agent enrollment-retirement in the set of consensus-validated agents is initiated at discovery of a newly created agent. Moreover, its retirement and any change of any of the agent trustworthiness elements is done in a de-synchronized way to prevent latency at the establishment of inter-agent communication link.

C. *Near Real-Time Secure MAS Operation*

Using a DLT-based solution for inter-agent communication would add delay message exchange, which would prevent service operation near real-time. For this very reason, we propose combining DLT and extended VLANs (VXLAN) [4] to bring any added delay to a minimum; DLT exchange is kept offline, while VXLANs are used for near real-time communication among the agents (labeled D in Fig. 1). VXLAN is a network encapsulation technology that allows creating an overlay over a physical network to provide a service abstraction layer in virtualized environments. This solution provides quick set up and enables creating millions of networks in parallel (simultaneous segments). At the same time, VXLAN presents some security concerns, such as the possibility for *rogue devices* to join one or more multicast groups and inject fake traffic. Encryption protocols, such as IPsec, encrypt both the content and the inner headers, which reduces rogue risk, as compared to other real-time encryption protocols at the application level.

In addition, to reduce the delay added for encryption and to allow other MAS agents to verify and trace communications, in our implementation we use pre-shared secrets. Then, such solution needs from an authentication infrastructure for authorized agents to obtain and distribute such secrets. We rely on DLT for that purpose. In particular, the security intrinsic features of DLTs can be used to, once the association between agents is agreed, securely manage VXLANs as communication channels among the agents. Note that the impact of the consensus mechanism used is limited to the set-up phase of the dynamic associations between agents and does not have an impact on the actual exchanges between them once the associations are established.

IV. CONCLUSIONS

A multi-technique solution is proposed for securing multi-agent systems controlling 6G services. First, binary hardening is applied to the original agents' binaries. A DLT is deployed to submit asynchronous evidences and to share keys/secrets. Finally, securitized VXLAN is used for inter-agent communications. We claim that such combination will provide strong security to the MAS without impeding its performance.

REFERENCES

[1] S. Barzegar, M. Ruiz, and L. Velasco, "Distributed and Autonomous Flow Routing Based on Deep Reinforcement Learning," in Proc. PSC, 2022.

[2] M. Wooldridge, *An introduction to multiagent systems*, John Wiley & Sons, 2009.

[3] K. Antevski and C. J. Bernardos, "Federation of 5G services using distributed ledger technologies," Internet Techn. Letters, vol. 3, 2020.

[4] M. Mahalingam *et al.* (Eds.) "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks," IETF RFC 7348, 2014.