

Real-time Network Cyber Situational Awareness in B5G networks

José Antonio Pastor*, Martin Husák[†], Jorge Bernal Bernabe*, Antonio Skarmeta *

*Department of Information and Communication Engineering, University of Murcia, Spain,

Email: {japv, jorgebernal, skarmeta}@um.es

[†]Institute of Computer Science, Masaryk University, Email: husakm@ics.muni.cz

Abstract—The dynamic nature of beyond 5G network (B5G) topologies imposes continuous and real-time cyber situational awareness (CSA) to make cognitive security orchestration according to the actual context. In this sense, security orchestration decisions such as virtual network security functions placement or (re)configuration of the system to counter cyberthreats can benefit of these kind of CSA models. Traditional infrastructure and service models for CSA such as CRUSOE capture the security posture, missions, networks and assets, that can be used as baseline for cognitive functions such as cyber asset attack surface management, risk-trust assessment as well as detection and mitigation of cyber-attacks. However, these infrastructure data models and tools have not been adapted to complex B5G domains and do not support real-time processing of 6G network traffic that, once supported, can boost context awareness and decision making. This paper describes the design, implementation and evaluation of the extension to the CRUSOE infrastructure model to enable the real-time modeling of 6G network flows, thereby increasing cyber security awareness capabilities in 6G Security Operation Centers (6G-SOC), that ultimately, can help to improve cognitive security management of 6G networks. The implementation and performance evaluation carried out shows promising results to capture and model in real time the dynamicity of 6G network topologies and traffic.

I. INTRODUCTION

Cyber situational awareness (CSA) is a concept describing the ability to perceive elements of cyber environment (e.g., hosts, service, data), comprehend their meaning, and predict future changes in the situation [1], [2]. Traditional approaches to achieve CSA usually started with mapping the networks and hosts in them and then proceeding to analyze their relationships or vulnerabilities. However, computer networks has become highly dynamic due to the wide spread of wireless networking (including 5G and beyond), the use of IoT and cloud, or containerized services. Thus, there is a need to dynamically update the information on the network, even to the point to acknowledging current network traffic flows.

Traditional CSA methods rely on static network mapping and predefined assessments, making them ineffective for highly dynamic B5G networks with virtualized, cloud-native, and IoT components. The key gap is the inability to integrate real-time traffic analysis with structured CSA models, limiting the ability to monitor and predict security threats in these environments. Overcoming this challenge requires a more adaptive approach that combines both perspectives for comprehensive situational awareness.

To fill the gap, we propose a design of a situational awareness system for B5G networks that combines the expressiveness and wide scope of CSA models known from traditional networks and the dynamic network traffic measurements used in B5G networks. Namely, our design combines the network traffic measurement tool Skydive and the ISIM data model (used in Resilmesh framework and based on earlier CRUSOE data model). Custom additions to the toolset as well as the data model are required for successful introduction of the concepts into the B5G domain. The design is also a part of wider framework known as 6G-SOC¹.

The proposed system aims to improve cyber situational awareness in B5G networks by integrating real-time traffic monitoring with structured CSA models. It is expected to improve responsiveness to network changes, scale efficiently with complex infrastructures, and improve threat detection while minimizing false positives. The system should maintain low overhead, ensure efficient data processing, and seamlessly integrate with the 6G SOC framework to enable continuous and adaptive situational awareness.

The remainder of this paper is structured as follows. Section II surveys the related work. The proposed approach is outlined in Section III, description of the implementation is presented in Section IV, and performance evaluation is presented in Section V. Section VI concludes the paper.

II. RELATED WORK

The issue of organizing the data on the network has been approached in the past in the context of network-wide situational awareness [1]. For example, M2D2 [3] correlates alerts and vulnerabilities and Virtual Terrain [4] allows modeling the network. The graph-based approaches to data modeling, together with the emergence of graph database enabled the design of data models like CyGraph [5], which was implemented in a tool by MITRE, or CRUSOE [6], which was implemented in an open-source toolset [2]. CRUSOE later evolved into ISIM model used in this work. However, this models do not integrate network flow monitoring metrics as proposed herein.

Research works on situational awareness in B5G networks [7] can consider advanced network metrics and topology information to make analytics and perform cognitive decisions,

¹<https://ants.inf.um.es/en/6g-soc>

including anomaly detection [8] leveraging the N5G NWDAF analytic function, however current works do not combine that information with cybersecurity oriented metrics and attributes (e.g. vulnerabilities), as proposed in this paper.

The importance of cyber situational awareness in future wireless technologies has been highlighted in the context of 5G and IoT deployments, where anomaly detection and security monitoring are recognized as key components for achieving leadership in next-generation networks [9]. In addition, domain-specific applications of situational awareness using 5G have been proposed, such as the Back Situation Awareness (BSA) service for public safety, which uses MEC-based orchestration to improve road safety through early notification of emergency vehicles [10].

Beyond public safety, the use of 5G communications to enhance situation awareness in active distribution networks has been explored, with resource-efficient frameworks proposed to support real-time data collection and emergency event handling [11]. Finally, focused efforts to integrate situational awareness models into large-scale 5G MIMO systems for safety assessment and prediction [12] demonstrate the importance of modeling and predicting complex networks behaviors. However, these approaches typically address either communication performance or security event prediction in isolation and do not comprehensively integrate network topology, flow monitoring, and cybersecurity vulnerability data into a unified situational awareness framework, which is one of the main focuses of this work.

III. DESIGN

The Infrastructure and Service Information Model (ISIM) is currently being integrated into a multilayer cybersecurity architecture designed for a 6G Security Operations Center (SOC), as shown in Figure 1. As part of the Data & Information layer, ISIM is being developed to interact with key security components in the Reaction Plane, Monitoring & Analytics, and Operations layers. This integration aims to improve CSA by enabling the structured aggregation of security-related data from multiple sources, including security information and event management (SIEM) systems, attack surface manager, data aggregation mechanisms, topology monitoring (TM) tools, and data network monitoring (DM). Once fully implemented, ISIM will contribute to a more comprehensive understanding of network security by facilitating event correlation, network topology analysis, and vulnerability detection in multiple domains.

Topology Monitoring (TM) is responsible for tracking and managing the structure of the network, including its devices, network ports, and their interconnections. TM tools continuously update network topology maps by discovering new devices and changes in the network infrastructure. This capability helps to understand how different network components interact and provides critical data for security monitoring, anomaly detection, and threat mitigation. Data Monitoring (DM) focuses on observing and analyzing the flow of data within the managed infrastructure. Shows insight into network

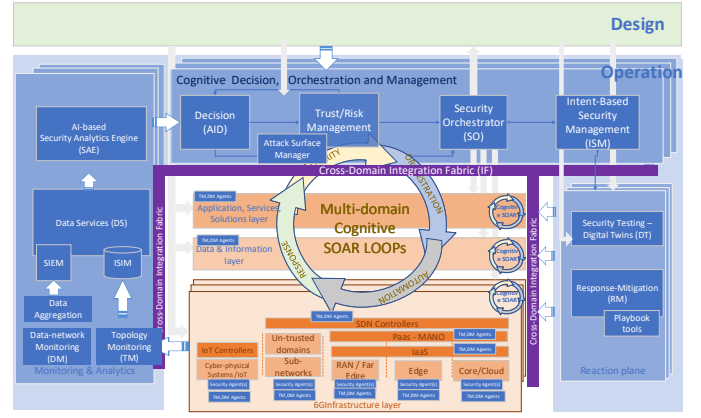


Fig. 1. 6G-SOC framework architecture.

behavior by detecting anomalies, collecting statistics on network activity, and identifying potential threats. By integrating with ISIM, DM improves the detection of suspicious patterns and facilitates proactive security measures.

In addition, a variety of connectors can be integrated to obtain infrastructure information and improve context awareness. These include active discovery tools such as Nmap² or Skydrive³. Passive monitoring solutions can collect telemetry from network devices, and network analysis tools can improve visibility into dynamic virtualized environments. Monitoring connectors, such as flow data connectors (e.g. Skydrive or Flowmon⁴), can be integrated to analyze traffic patterns and detect anomalies in real time.

ISIM acts as a central aggregator and processor of security-related data within the 6G-SOC framework. In addition, ISIM integrates with AI-driven analytics engines, such as the Security Analytics Engine (SAE) and AI-driven Decision (AID) components, to enhance security intelligence and enable proactive threat detection and response. These components (TM and DM) are distributed throughout the 6G network, ensuring broad coverage and real-time monitoring of the network. Beyond monitoring, dedicated components assess risk and confidence based on ISIM analytics and make informed decisions to dynamically act on the network. In addition, orchestrators and playbook tools enforce security actions across multiple enablers and controllers, automating responses and mitigation strategies across multiple domains.

As ISIM is further integrated into the 6G-SOC framework, its role in cyber situational awareness will become increasingly important, providing a unified view of network security and helping to build a more agile and resilient defense strategy.

A. ISIM Data Model

In this work, we use the ISIM data model that is designed for assessing network security situation in our Resilmesh EU

²<https://nmap.org/>

³<https://skydrive.network/>

⁴<https://www.progress.com/flowmon>

project⁵. ISIM data model is a direct successor to CRUSOE data model [6]. Both data models use nodes and edges to represent entities in the computer networks (e.g., devices, services, vulnerabilities) and their relationships (e.g., device hosts a service, service has a vulnerability). An excerpt from the data model can be seen in Figure 2.

ISIM is structured into seven layers, where each layer represents a certain area of cybersecurity and its entities and could be obtained by a dedicated tool. Relationships, however, can connect both entities within the same layer or across layers, thus interconnecting the data.

- Host layer models hosts (devices) in the network. Hosts are linked with nodes representing various pieces of software (Software version) discovered typically by fingerprinting the hosts [13].
- Network layer lists the IP addresses assigned to hosts and network services running on them, IP addresses' belonging to subnets, and resolved domain names.
- Threat layer models vulnerabilities and CVE (Common Vulnerabilities and Exposures) [14] records. Vulnerabilities are mapped to software version of the host layer, from which it can be traced which devices are running such software versions and, thus, being vulnerable [15].

The remaining layers are not used in this work and, thus, not discussed in detail. Access control layer covers user accounts and privileges, Detection and response layer cover intrusion detection and attack mitigation system, System layer models redundancies and dependencies between hosts, and Mission layer connect cyber assets to business missions. ISIM and CRUSOE further differs in several details. From the B5G perspective, the most interesting are the new layers representing hardware and physical location of devices, which are used namely in industrial robotics and other OT use cases. Further, ISIM adds a labeling attribute to distinguish types of network nodes based on MITRE D3FEND's Digital Artifact Ontology (DAO)⁶ and custom labels for internal purposes, e.g., which sensor provided a particular piece of information.

ISIM, implemented using Neo4j, provides GraphQL and REST APIs for Resilmesh interaction but does not collect data itself, relying instead on external tools such as CASM or Observe in CRUSOE [2]. A minimalist scenario includes a network scanner, such as Nmap, which enumerates active hosts and network services on the network, exporting CPE fingerprints [16]. The CPE is used in CVE to identify which versions of the software are affected by a vulnerability. For each CPE found, a list of CVEs relevant for them is downloaded from NVD⁷. All such elements (IP addresses, CPEs, CVEs) are stored in ISIM in the corresponding node types, optionally enriched by vulnerability scanners or host-based agents.

B. Extension of ISIM to model network flows

Although databases like CRUSOE or ISIM are rather static (i.e., their content does not change often), it might be advanta-

geous to provide them with more dynamicity, such as including recent network traffic between the nodes.

First, there is a need to define the nodes and edges. We start with the node representing a network flow. Such a node contains all the features of a network flow (e.g., start and end MAC address, IP address, and port, duration, number of packets and bytes transferred) stored as properties. Based on such properties, the node is then connected to other nodes in the graph that represent the entities mentioned in the properties. Therefore, the "Flow" node is connected to nodes representing IP addresses (type "IP address") or network services on end ports (type "Network Service").

5G represents a significant advancement over previous technologies, offering improvements in performance, multi-tenancy, mobility, and dynamic management. To support these features, 5G data packets have a nested structure, as shown in Figure 3. The first set of headers includes communication between physical machines, including MAC, IP, and UDP. The second set includes VXLAN, MAC, IP and UDP to isolate tenant traffic, especially for telecommunication operators that share the same physical 5G infrastructure as a tenant. The third set includes GTP, IP, and UDP to enable user mobility. Finally, the application header handles the data exchanged between end users. This study focuses on GTP for 5G mobile communications, using VXLAN for tenant isolation as an example, although other protocols can also be used to achieve the same goal.

C. Advanced Metrics for real-time contextual awareness

Our proposal will bring several benefits for cognitive network management. The knowledge of the specific flows that are continuously transversing every point in 6G network, can significantly increase the capabilities of detection of anomalies and cyberattacks. The information about the current status of the traffic when combined at the same time with the vulnerabilities and services in each node of the datapath of the flow can foster the capabilities of detection. This information can provide meaningful information for making decisions about possible prevention actions and countermeasures against ongoing attacks. Spatial network metrics, such as betweenness centrality [7] that computes the criticality of a node in the topology, that is traditionally based on static network topologies, can now be weighted by the number of flows in every particular point of the network, so that this new kind of metric can provide the evolving importance and criticality of each node in real time. These new sophisticated types of metrics will also influence the risk assessment component of the architecture in charge of computing risk per node and service.

IV. IMPLEMENTATION

This section covers ISIM's 5G network monitoring enhancements, including a Python connector that integrates Skydrive with Neo4j for topology and flow data storage, improving CSA. It also details Skydrive source code modifications to support GPRS Tunneling Protocol (GTP) [17] traffic analysis,

⁵<https://resilmesh.eu/>

⁶<https://d3fend.mitre.org/dao/>

⁷<https://nvd.nist.gov/>

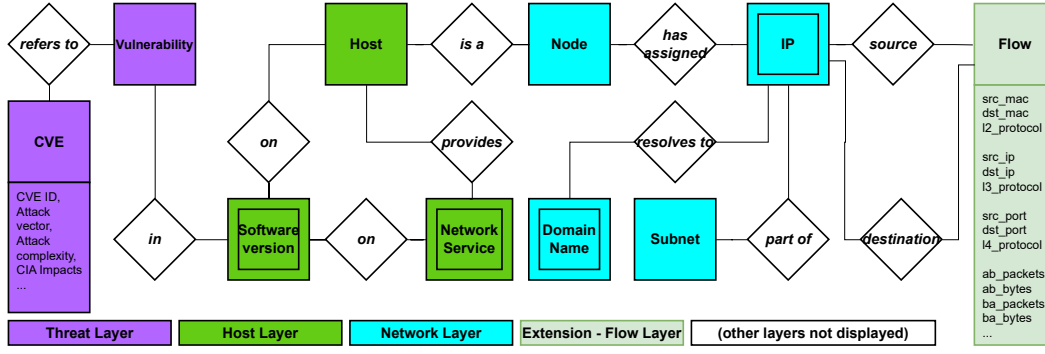


Fig. 2. An excerpt from enhanced ISIM data model: relevant entities and relationships from threat, network, and host layers and the new Flow entity.



Fig. 3. GTP packet header representation.

addressing a key limitation in existing encapsulation protocol support.

A. 5G network topology scanning

As part of the ISIM extension, a Python-based integration was developed to connect ISIM with the Skydive API. This integration consists of two main components: *SkydiveConnector*, which is responsible for retrieving network data from Skydive, and *SkydiveAdapter*, which processes and stores these data in the Neo4j database. By continuously scanning the network, this system improves CSA, allowing real-time monitoring of the attack surface, tracking of vulnerabilities, and identification of critical assets. The components involved in this integration and their interactions are illustrated in Figure 4.

The *SkydiveConnector* component interacts with the Skydive API using the **skydive-client** Python library to retrieve details about network hosts, including their addresses, neighbors, hardware, SO and kernel, etc., which are essential to build an accurate representation of the topology. Once the data is collected, *SkydiveConnector* forwards it to *SkydiveAdapter*, which processes the information and stores it in Neo4j. The database stores hosts as graph nodes and establishes relationships between them based on network connectivity.

In addition to topology data, *SkydiveConnector* collects network traffic flow information, capturing key attributes such as IP addresses of the source and destination, ports, protocols, and traffic volume metrics. This data is sent to *SkydiveAdapter*, which processes the flow information and inserts it into the graph database, linking flows to the relevant hosts and network entities.

Once topology and flows are collected, ISIM can leverage active fingerprinting techniques, such as Nmap scans, to iden-

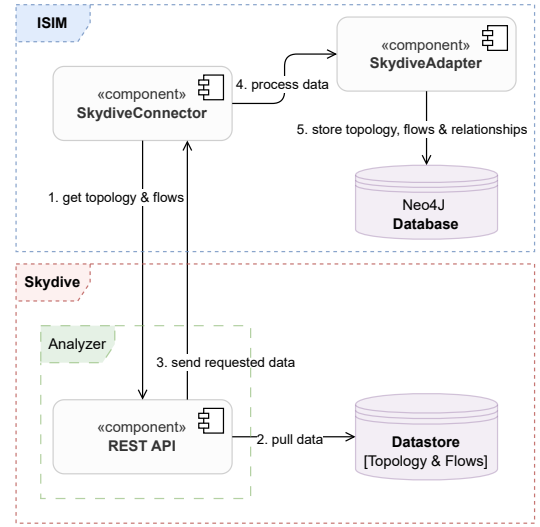


Fig. 4. SkydiveConnector and SkydiveAdapter components integration.

tify the services running on hosts and their associated software components (CPEs).

By continuously updating the network topology and flow information, *SkydiveConnector* and *SkydiveAdapter* ensure that ISIM maintains an up-to-date understanding of the network attack surface and helps identify vulnerabilities that could affect system security. The use of a graph database ensures that even as the volume of collected data increases, storage and querying operations remain efficient. The ability to correlate host relationships, network traffic, and vulnerability data enhances ISIM's capabilities for asset discovery, threat detection, and CSA.

B. 5G network flow traffic handling

Skydive is a network monitoring tool that provides real-time visibility into network traffic and topology. It supports multiple encapsulation protocols, such as Generic Routing Encapsulation (GRE) [18], Virtual eXtensible LAN (VXLAN) [19], Generic Network Virtualization Encapsulation (Geneve) [20] and Multiprotocol Label Switching (MPLS) [21], enabling flow analysis across tunnel-based communications. However,

it lacked support for the GPRS Tunneling Protocol (GTP), crucial for 5G network traffic analysis.

One of the biggest challenges in supporting GTP was ensuring that Skydive could correctly identify and differentiate GTP-encapsulated traffic. Since GTP encapsulates multiple subscriber sessions within a single UDP flow (typically over port 2152), an approach was needed to accurately track these individual sessions.

Modifications to the `TransportFlow` function enable the detection of GTP-U packets by identifying `layers.LayerTypeGTPv1U` as the last layer of the packet. Instead of using standard transport flow fields, the tunnel endpoint identifier (TEID) is extracted from the GTP header, similar to how VXLAN and Geneve use virtual network identifiers (VNI) to distinguish flows. This enhancement allows Skydive to track GTP flows per session rather than treating all GTP traffic as a single UDP flow.

Furthermore, modifications to Skydive’s `TransportFlow` and `networkID` functions ensure that GTP traffic is correctly identified and associated with sessions via the TEID field, similar to VXLAN’s VNI tracking.

The `PacketSeqFromGoPacket` function was extended to treat GTP as an encapsulation protocol, properly extracting inner payloads from tunneled packets, improving mobile network traffic analysis.

V. PERFORMANCE EVALUATION

This section evaluates the performance of ISIM, focusing on its scalability and efficiency. Experiments are conducted to assess its capacity to manage increasing network flows and storage overhead. The experimental design involves the examination of two key factors: the impact of batch size on Skydive flow retrieval times, and the efficiency of storing flows in a graph database. In addition, the assessment will include the latency in parsing 5G traffic.

A. Scalability test of increasing number of flows to stress ISIM

Figure 5 illustrates how the fetch time varies with different batch sizes, ranging from 1,000 to 10,000 flows. The trend suggests a roughly linear increase in the fetch time as the number of flows increases.

Since ISIM retrieves flows in batches of fixed size (typically 1,000 flows), this ensures that retrieval remains efficient and controlled, preventing excessive delays. Furthermore, given the speed at which ISIM retrieves flows from Skydive, it would be unusual for the network to generate traffic faster than ISIM can retrieve and process it.

Storing flows takes longer than fetching them, but not enough to impact performance. ISIM’s batch-based fetching and graph database allow for efficient scaling, ensuring high throughput even under heavy network traffic.

Figure 6 shows that storage time for flows in Neo4j increases steadily but remains under 3 seconds for 10,000 flows. Creating relationships between flows and entities adds minimal overhead while enhancing data modeling and query efficiency. Some outliers occurred due to cold starts when the database

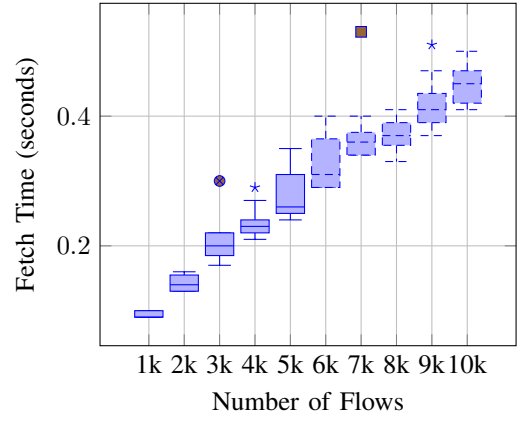


Fig. 5. Fetch times for batches of different sizes of Skydive flows from ISIM.

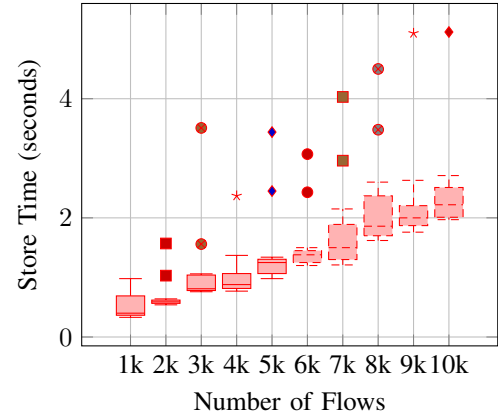


Fig. 6. Store times for batches of different sizes of flows in ISIM database.

lacked prior flow data, but performance improved as it warmed up.

B. Latency introduced for parsing 5G traffic

This section evaluates the latency introduced by Skydive when analyzing 5G traffic such as GTP, compared to TCP and UDP. Performance was measured by timing the processing of network packets within the `packetToFlow` function, which converts raw packets into flows. By dividing the total processing time (in microseconds) by the size of the packet (in bytes) including its headers and payload and excluding small synchronization packets that can be generated, such as in TCP communications, *time per byte in microseconds per byte* ($\mu\text{s}/\text{byte}$) was calculated.

Figure 7 shows the packet processing *time per byte* for the TCP, UDP, and GTP protocols. TCP has the lowest median processing time and the smallest interquartile range (IQR), indicating more consistent performance. UDP has a slightly higher median processing time than TCP, along with a wider IQR and several outliers, indicating greater variability in processing. GTP, an encapsulated protocol, has a median and distribution similar to UDP, indicating that the overhead introduced by its decapsulation is not significant. In general,

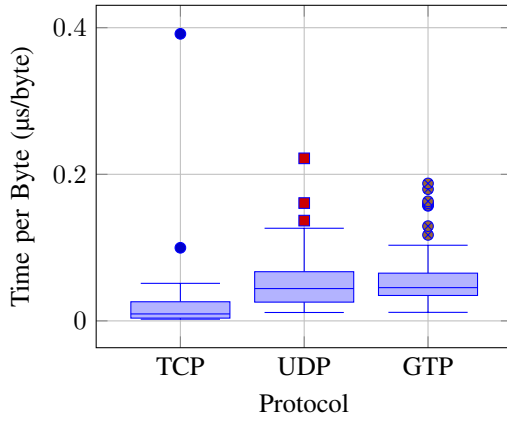


Fig. 7. Distribution of Skydive's processing time per byte ($\mu\text{s}/\text{byte}$) for TCP, UDP, compared with processing time of our GTP protocol implementation.

the results in Figure 7 suggest that, although encapsulation adds some complexity, its impact on *per-byte* processing time remains comparable to that of non-encapsulated protocols such as UDP.

VI. CONCLUSION

In this paper, we approached the issues of achieving cyber situational awareness in B5G networks. As a part of 6G-SOC framework, we designed and implemented the topology monitoring system that tracks the network structure. We also set up network traffic monitoring via the Skydive tool. Moreover, we enhanced the ISIM data model, which allows for mapping cyber assets and their fingerprints to vulnerabilities, and added the notion of network flows to it. In an experiment, we illustrated the performance of a system that stores network flows into the enhanced ISIM, thus enabling us to observe security situation of a network in close to real time and at the granularity of network flows. As future work, we plan to leverage on this model to perform CSA-based cognitive decisions to prevent and counter sophisticated cyberattacks in real-time.

ACKNOWLEDGMENT

This work has been funded by the European Union's NextGenerationEU, as part of the Recovery, Transformation, and Resilience Plan, supported by Spanish INCIBE (6G-SOC project). This work has been also funded by the RIGOUROUS project from the European Union's Research and Innovation Programme Horizon Europe under grant agreement no. 101095933. Besides, this research has been supported by the Resilmesh project funded by the European Union as part of the Horizon Europe Framework Program (HORIZON), under grant agreement no. 101119681.

REFERENCES

[1] N. Evancich, Z. Lu, J. Li, Y. Cheng, J. Tuttle, and P. Xie, "Network-wide awareness," in *Cyber Defense and Situational Awareness*. Springer, 2014, pp. 63–91.

[2] M. Husák, L. Sadlek, S. Špaček, M. Laštovička, M. Javorník, and J. Komárková, "CRUSOE: A toolset for cyber situational awareness and decision support in incident handling," *Computers & Security*, vol. 115, p. 102609, 2022.

[3] B. Morin, L. Mé, H. Debar, and M. Ducassé, "M2D2: A formal data model for IDS alert correlation," in *International Workshop on Recent Advances in Intrusion Detection*. Springer, 2002, pp. 115–137.

[4] J. Holsopple, S. J. Yang, and B. Argauer, "Virtual terrain: a security-based representation of a computer network," in *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security*, 2008, p. 69730E.

[5] S. Noel, E. Harley, K. H. Tam, M. Limiero, and M. Share, "CyGraph: Graph-Based Analytics and Visualization for Cybersecurity," *Handbook of Statistics*, vol. 35, pp. 117–167, 2016.

[6] J. Komárková, M. Husák, M. Laštovička, and D. Tovarňák, "CRUSOE: Data Model for Cyber Situational Awareness," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 36:1–36:10.

[7] I. Sanchez-Navarro, J. Bernal Bernabe, J. M. Alcaraz-Calero, and Q. Wang, "Advanced spatial network metrics for cognitive management of 5g networks," *Soft Computing*, vol. 25, no. 1, pp. 215–232, 2021.

[8] P. K. Gkonis, N. Nomikos, P. Trakadas, L. Sarakis, G. Xylouris, X. Masip-Bruin, and J. Martrat, "Leveraging network data analytics function and machine learning for data collection, resource optimization, security and privacy in 6g networks," *IEEE access*, vol. 12, pp. 21 320–21 336, 2024.

[9] E. Chang, F. Gottwalt, and Y. Zhang, "Cyber situational awareness for cps, 5g and iot," in *Frontiers in Electronic Technologies*, S. Prabaharan, N. M. Thalmann, and V. S. Kanchana Bhaaskaran, Eds. Singapore: Springer Singapore, 2017, pp. 147–161.

[10] N. Slamnik-Kriještorac, F. Z. Yousaf, G. M. Yilma, R. Halili, M. Liebsch, and J. M. Marquez-Barja, "Edge-aware cloud-native service for enhancing back situation awareness in 5g-based vehicular systems," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 660–677, 2024.

[11] Q. Li, H. Tang, Z. Liu, J. Li, X. Xu, and W. Sun, "Optimal resource allocation of 5g machine-type communications for situation awareness in active distribution networks," *IEEE Systems Journal*, vol. 16, no. 3, pp. 4187–4197, 2022.

[12] S. Yang, D. Yin, X. Song, X. Dong, G. Manogaran, G. Mastorakis, C. X. Mavromoustakis, and J. M. Batalla, "Security situation assessment for massive MIMO systems for 5G communications," *Future Generation Computer Systems*, vol. 98, pp. 25–34, 2019.

[13] M. Laštovička, M. Husák, P. Velan, T. Jirsík, and P. Čeleda, "Passive operating system fingerprinting revisited: Evaluation and current challenges," *Computer Networks*, vol. 229, p. 109782, 2023.

[14] L. A. B. Sanguino and R. Uetz, "Software vulnerability analysis using CPE and CVE," *CoRR*, vol. abs/1705.05347, 2017. [Online]. Available: <http://arxiv.org/abs/1705.05347>

[15] M. Laštovička, M. Husák, and L. Sadlek, "Network monitoring and enumerating vulnerabilities in large heterogeneous networks," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 2020.

[16] B. A. Cheikes, D. Waltermire, and K. Scarfone, "Common platform enumeration: Naming specification version 2.3," *NIST Interagency Report*, vol. 7695, no. 8, 2011.

[17] J. Collins, *GPRS Tunneling Protocol (GTP)*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 1–3. [Online]. Available: https://doi.org/10.1007/978-3-642-27739-9_1522-1

[18] T. Li, D. Farinacci, S. P. Hanks, D. Meyer, and P. S. Traina, "Generic Routing Encapsulation (GRE)," RFC 2784, Mar. 2000. [Online]. Available: <https://www.rfc-editor.org/info/rfc2784>

[19] M. Mahalingam, D. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell, and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks," RFC 7348, Aug. 2014. [Online]. Available: <https://www.rfc-editor.org/info/rfc7348>

[20] J. Gross, I. Ganga, and T. Sridhar, "Geneve: Generic Network Virtualization Encapsulation," RFC 8926, Nov. 2020. [Online]. Available: <https://www.rfc-editor.org/info/rfc8926>

[21] A. Viswanathan, E. C. Rosen, and R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031, Jan. 2001. [Online]. Available: <https://www.rfc-editor.org/info/rfc3031>