Enhancing trust and liability assisted mechanisms for ZSM 5G architectures

Noelia Pérez Palma,* Sara Nieves Matheu-García,* Alejandro Molina Zarca,* Jordi Ortiz,* Antonio Skarmeta*
noelia.perez3@um.es, saramieves.matheu@um.es, alejandro.mzarca@um.es, jordi.ortiz@um.es, skarmeta@um.es
* University of Murcia, Department of Information and Communication Engineering, Spain

Abstract—5G improves previous generations not only in terms of radio access but the whole infrastructure and services paradigm. Automation, dynamism and orchestration are now key features that allow modifying network behaviour, such as Virtual Network Functions (VNFs), and resource allocation reactively and on demand. However, such dynamic ecosystem must pay special attention to security while ensuring that the system actions are trustworthy and reliable. To this aim, this paper introduces the integration of the Manufacturer Usage Description (MUD) standard alongside a Trust and Reputation Manager (TRM) into the INSPIRE-5GPlus framework, enforcing security properties defined by MUD files while the whole infrastructure, virtual and physical, as well as security metrics are continuously audited to compute trust and reputation values. These values are later fed to enhance trustworthiness on the zero-touch decision making such as the ones orchestrating end-to-end security in a closed-loop.

I. INTRODUCTION

5G infrastructure offers multiple technology advancements at different levels such as significant speed upgrades in mobile broadband connectivity (up to a 100x increase compared to 4G), low latency communications (less than 5 milliseconds) as well as enhanced capacity capable of providing connectivity to a massive number of devices, something essential considering the Internet of Things (IoT) growth trend. Beyond radio access improvements, some of these advanced features can only be provided through dynamic capabilities such as dynamic deployment, configuration and management of the 5G infrastructure (e.g., by deploying services as near to the consumer as possible to decrease latency). Although it is a promising approach, its dynamic, extensible and evolutionary nature is accompanied by new challenges, specially in terms of trust and security. In fact, security will be of little value if the method or technology employed is not trustworthy.

The research community is making efforts to design frameworks capable of providing Artificial Intelligence (AI)-assisted automation and autonomous orchestration to manage the security aspects of the 5G infrastructure. For instance, Sun et. al. [1] presented a 5G security challenges analysis and introduced a framework towards 5G security. The framework is based on a hierarchical attack and defense graph considering entities, attributes and relationships. However, the solution only provides a high-level theoretical approach not aligned with the European Telecommunications Standards Institute (ETSI) Zero touch network and Service Management (ZSM), plus, trust and security management are not considered. In a more practical approach, Rathore et. al. [2] presented a security framework for 5G that relies on Deep Learning (DL) techniques for intelligent data analysis and on Blockchain (BC) for data security across cloud, fog and edge. The authors also provided an experimental evaluation by simulating the 5G network with WiFi equipment. In this case, the solution focused more on the detection part but did not provide trust mechanisms, automation, alignment with ZSM, neither a well defined security management process.

Unlike previous approaches, INSPIRE-5GPlus framework [3] provides a smart, trustworthy and liability-aware 5G security platform for 5G infrastructures and beyond. To this aim, it adopts emerging technologies such as ZSM, Software Defined Security (SD-SEC) models, AI and Machine Learning (ML) techniques and Trusted Execution Environment (TEE). Trust and security are, from design, also provided by novel mechanisms that ensure the correct behaviour and confidence across the 5G infrastructure. This paper tackles the latter mechanisms by integrating and instantiating MUD files and a TRM over the INSPIRE-5GPlus architecture. On the one hand, MUD files are intended to provide access control by specifying what kind of access and network functionalities must be available for different types of devices composing the infrastructure. This feature is in turn helpful to configure monitoring tools according to the MUD specifications as well as to learn about regular devices behaviours that will allow the identification of abnormal events on the 5G infrastructure. On the other hand, the TRM provides trust assessment from multiple values gathered from the rest of the components of the 5G infrastructure. These trust calculations will be essential during the orchestration of the MUD requirements to make better decisions to enforce them in a trustworthy way. That is, only security assets (pieces of hardware or software capable of enforcing security properties) that have a previous TRM assessment above a configurable threshold will be employed as part of the MUD security requirements orchestration.

The rest of the paper is organized as follows: Section II introduces the state of the art related to Trust and Liability. Section III provides the main objective of the solution inside the scope of the INSPIRE-5GPlus project. Section IV presents the security enablers, highlighting the ones that are instantiated as part of the proposed solution. Section V delves into the proposed solution for the TRM and MUD integration into the INSPIRE-5GPlus architecture. Finally, Section VI concludes the paper providing an analysis of the current efforts as well as presenting future research lines.
II. STATE OF THE ART ON TRUST AND MODEL BASED LIABILITY

Past works have included trust evaluation and management to their approaches. Authors in [4] identify the need for developing a trustworthy Service Legal Agreement (SLA) capability framework to establish assurance dimensions to preserve data confidentiality, integrity and availability in SLAs as trust-enhancing instruments. The study proposes the incorporation of security capabilities into SLA contexts to establish trust between the customer and service provider. Moreover, works like [5] describe how existing security concepts such as manifests and Security-by-Contract, root cause analysis, remote attestation, proof of transit, and trust and reputation models can be used to deal with security and liability management. A good example of trust and reputation models is introduced in [6] with their approach called COMITMENT. It uses information from previous direct and indirect fog node interactions to compute the trust level of the nodes within the fog computing environment. Additionally, works for vehicular networks are starting to emerge, like [7] which proposes a scheme that incorporates feedback from vehicles in Vehicular Edge Computing (VEC) servers to predict the average number of true messages. Then, VEC uses deep reinforcement learning to determine the optimum reputation update policy to stimulate vehicles to send true feedback.

For this work, we are not only considering the way of computing trust scores but also other two important concepts in which the implementation of the TRM relies on. These are Distributed Ledger Technologies (DLTs) and the process of computing a trust score of an entity. Both terms can be used together, as we can use the benefits DLT offers (as traceability and security) to obtain trust values in a guaranteed way. There are some approaches that use them, as analysed in [8]. In our case, we employ HyperLedger Fabric\(^1\) as DLT technology, a DLT platform that supports Smart Contracts. A Smart Contract\(^2\) is a piece of code (executable logic) whose results are added to the ledger as a new transaction. To the best of our knowledge, this paper comprises the first work tackling trustworthiness aspects of the network in such high dynamic scenarios.

Regarding model based liability, Polk et al. [9] from National Institute of Standards and Technology (NIST) provided a guide to use Internet Engineering Task Force (IETF) MUD for mitigating network-based attacks on small business and home IoT environments. To this aim, MUD file provides Access Control List (ACL) requirements for each device type so it is possible to identify a well-known regular behaviour for them. In fact, same authors in [10] remarked the potential Denial-of-service attack (DDoS) mitigation capabilities by exploiting this idea. Hamza et al. [11] also applied this approach for managing the Software Defined Network (SDN) network by translating MUD files into final SDN rules that are enforced in the SDN switches. Following the same approach, Ranganathan et. al., [12] presented a MUD implementation for OpenFlow-enabled devices. They used Dynamic Host Configuration Protocol (DHCP) in order to detect IoT interactions and to install MUD profile configurations in devices (e.g., open a device port).

Although there are several works that introduce MUD in IoT environments, new solutions to provide model based liability and behavioural profiles in next generation infrastructures are still missing. For instance, [13] provided a description to integrate MUD into 4G/5G core network by using Protocol Configuration Options (PCOs) within 4G/5G cellular signaling to share MUD Uniform Resource Identifiers (URIs) from devices to cellular core network elements, which can apply additional policies for IoT devices. However, whereas previous proposals provide valuable contributions, they are not integrated as a whole in a 5G security framework, besides, they are not aligned with ETSI ZSM so they do not provide essential capabilities for 5G ecosystems such as the automation and intelligent reaction. In this regard, our proposal, built on the top of INSPIRE-5GPlus ZSM-aligned architecture, does not only allow proactive and reactive (autonomously) multi-proposal MUD policy enforcement but also intelligent threat MUD enforcement.

Concerning threat information sharing, there is a high number of schemes aiming to model security information. The best known is the Extensible Markup Language (XML)-based Structured Threat Information Expression (STIX) [14] language used to exchange cyber threat intelligence (CTI) sponsored by MITRE. In line with STIX, the XML-based Incident Object Description Exchange Format (IODEF) [15] is an IETF standard format for representing computer security information in XML representation.

Despite the high flexibility offered by these models, the mechanisms for sharing such information are undefined, cumbersome, heavy or difficult to use, which limit its adoption in a such restricted but widespread context like the IoT. Moreover, there are no solutions that enable an automatic exchange of cyber threat information in IoT systems that allow for automatic implementation of defensive actions against novel cyber attacks. Dealing with the above and looking for a transparent mechanism for the user to effectively protect their connected devices, the NIST proposed a threat signalling mechanism using a threat MUD file [16] based on the existent MUD standard. While the MUD is associated with a device and is used to establish preventive configuration rules, the threat MUD is associated with a threat and is used to establish configuration rules that limit access to the domains compromised by it. This way, the combination of MUD and threat MUD represents a simple and transparent way to reduce vulnerabilities and potential network attacks on IoT devices.

However, the NIST proposal is still under development and has not yet been implemented. This work represents a pioneering effort not only to implement this mechanism, but also to adapt and integrate it into a broader context such as the 5G, where the IoT devices are quite present.

\(^1\)https://www.hyperledger.org/use/fabric
\(^2\)https://hyperledger-fabric.readthedocs.io/en/latest/smartcontract/smtracton.html
III. OBJECTIVE

INSPIRE-5GPlus is by design committed to bring Trust and Liability into the 5G and beyond ecosystem. In terms of Trust, it is mandatory to have the ability to judge the security framework trustworthiness at component and system level, including multi-tenancy, to determine whether the services required can be deployed on top of it. European regulations (EECC ³, NIST ⁴) and Industry 4.0 impose the delivery of evidence of data protection and local sovereignty compliance as examples of a longer list of restrictions that are addressed within INSPIRE-5GPlus via remote attestation and path proof mechanisms among others. These evidences are highly related to the slice concept that due to 5G softwarization implies the usage of TEE techniques which certify that the software and data have not been unlawfully altered.

IV. INSPIRE-5GPLUS TRUST ENABLERS

In Table I, we describe the trust enablers identified in the INSPIRE-5GPlus architecture. Trust and liability become specially relevant on 5G deployments since clients need to be able to know how reliable the infrastructure on which its services are being deployed is, and Cloud Service Providers (CSPs) must also be informed of the reliability of the services that will be deployed on it. However, these metrics are highly dynamic and described in assurance levels based on specific measures that identify when and how an entity, a relationship or a transaction can be relied upon. For that reason, we have also envisaged two novel mechanisms that also benefit from the existing enablers’ information, combining their knowledge to ensure the trust and reliability of both the underlying infrastructure and the services and applications deployed on it. These two new enablers are described next.

A. Trust Reputation Manager

Trust is defined by ETSI [17] as the confidence in the integrity of an entity for reliance on that entity to fulfill specific responsibilities. For 5G scenarios, the need emerges to develop a system capable of calculating, both from historical and live data, how reliable a cloud (or a service) is. Thus, in this section we introduce the TRM enabler, inside the Trust Management block, whose goal is to evaluate and assign trust and reputation values to the monitored 5G entities (for instance, VNFs like Access and Mobility Management Functions (AMFs), User Plane Functions (UPFs) or Authentication Server Function (AUSF), nodes, infrastructure, etc.) using historical data, monitoring data and combining a variety of assurance elements that include identity, attribution, attestation and non-repudiation. The TRM is also in charge of sharing the obtained values in a safe and trustable way. The main idea resides in the ability to offer the trust values regardless of the domain or tenant. That is, when an entity requires to use a different infrastructure, it must be able to know, in a liable way, the trust value of the infrastructure, without the need of further knowledge about the infrastructure itself. This simplifies the relationships between domains and third-parties infrastructures such as other operators, which are some of the basis of the 5G paradigm. In such way, every domain will implement a Trust Management Service, which will be in charge of calculating and storing the trust values in data services. Therefore, they will be available when required.

It is important to point out that the TRM job is not only to quantify the reliability but also to offer valuable and trustable information in a non-repudiated and auditible way. For that purpose, the trust computation process will be carried out inside Smart Contracts to ensure the liability of the resulting values. Besides, these values are envisioned to be used by Inspire-5GPlus’ security orchestration processes as a trigger to deploy countermeasures if an abnormal situation occurs and needs to be mitigated.

Decisions on trust are rarely made on a single parameter, and trust is always contextual, thus, the content and format in which the enablers publish data for the computation of the trust score has been defined complying with the ETSI recommendations [17]. Hence, a set of specific potential parameters provided by the enablers are listed in what follows: geographical location, jurisdiction/regulatory location (public/private), logical (network) location, hardware capabilities, hardware provenance and history, software capabilities, software provenance, execution instance history, chain of trust, time elapsed since last trust audit/check, date, time of day, ownership of hardware, ownership of software, security of network, appropriate use of encryption techniques, extent to which the software was initially hardened, measures in place to maintain the integrity of the software and, physical security of the various locations over which the entity components are deployed. The previous parameters, from which trust is calculated, can be retrieved from the below listed elements:

- Attestation of Virtual Machines (VMs), hypervisors, and network traffic. As well as the information coming from the entities dynamically deployed to enforce security policies, such as detections, decisions and reactions. This input comes from multiple monitoring services, deployed throughout the infrastructure, which offer the information

| Name                  | Functionality                                      |
|-----------------------|----------------------------------------------------|
| Systemic VNF          | Delivers code confidentiality and integrity and    |
|                       | licence infringement.                              |
| Proof Of Transit      | Guarantees that a given network packet has passed  |
|                       | through certain nodes in a given order.            |
| Component certification tool | Evaluates different components statically.          |
| e-reputation management | Expresses the global reputation of the domain.     |
| Network Slice Manager for trusted BC-based Network Slices | Enforces public visibility for the validation results of Network Slices and its components through the use of tests. |
| Risk Graphs Analysis  | Capture the topology of a system, vulnerabilities, |
|                       | accessibility between components, external         |
|                       | exposure, and evolution over time.                 |

³https://www.uems-cardio.eu/index.php/initiatives/eegc/83-logistics  
⁴https://www.nist.gov/
both in real-time and stored in a historic.

- System model/topology of the infrastructure, as well as Manifests and VNFs software execution evidence.
- Audits from Remote Verifiers which are entities in charge of analyzing the services of the underlying infrastructure.

The number of present Remote Verifiers might be variable and each one of them focuses on a specific security aspect. Remote Verifiers reports use a series of defined Smart Contracts supported by the Blockchain infrastructure, providing traceability and auditing. These reports determine the way attestations are performed to make them auditable.

- The Security policies and Security Service Level Agreements (SSLAs) defined on the environment, to ensure their compliance.

From the list of initial parameters, a JavaScript Object Notation (JSON) template is established in the first place for the involved enablers which will, in turn, fill and publish it via the Integration Fabric. This way, the TRM can rely on the same standard file for post-processing.

For trust calculation, a reputation approach is used, performing the evaluation across a set of different elements, as exemplified above, and leading to a calculation of "reputation". Additionally, a set of weight algorithms are applied, together with a Fuzzy Trust Evaluator, which uses weights and fuzzy logic (among others). Given that the trust score is calculated inside a Smart Contract, the processes and hence the scores obtained are auditable and provide non-repudiation, give that the reference to these values are added to the Blockchain.

### B. Threat Manufacturer Usage Description

The MUD\(^5\) was standardized in 2019 within the scope of the IETF. The MUD specification’s major goal is to limit the threat and attack surface of a certain IoT device by allowing manufacturers to establish network behavior profiles for their devices. Each profile is built around a set of policies, or ACLs, that specify the communication’s endpoints. MUD represents a scalable and flexible approach to the definition of network access policies beyond the use of IP addresses to enable communications with other services. A manufacturer could, for example, declare that the access to particular cloud services, as well as connections with other manufacturers’ devices, should be permitted.

Based on this idea, the NIST [16] proposed a threat signaling mechanism using a threat MUD. This MUD follows a similar structure than the MUD standard format. However, unlike MUD standard, it is designed as a mitigation mechanism, listing those external sites to and from which traffic should be prohibited, because the sites are associated with a given threat. It is not in the threat MUD scope to list sites with which communication should be permitted, nor provide any rule regarding local network traffic. Therefore, the threat MUD is intended to be created by a threat intelligence provider rather than the manufacturer, and its model contains certain fields to identify both the threat intelligence provider and the name of the threat that the file is associated with.

One of the main advantages of the threat MUD is that this mechanism allows to alert about a new threat in a very dynamic way to all the clients of a compromised domain, providing mitigation faster than a usual update or patch. Moreover, it represents a way to obtain information about the trustworthiness of a domain, since the reception of a threat MUD file represents the discovery of a new threat in that domain, affecting to its reputation.

### V. TRM AND MUD INTEGRATION INTO INSPIRE5G-PLUS ARCHITECTURE

INSPIRE5G-Plus’ architecture is trust aware by design defining components to integrate enablers that enhance that property of the system. We are going to describe how the TRM is integrated in such components while the MUD is employed as input for Security Orchestration processes. The proposed integration is shown in Fig. 1 and is further explained in detail below.

The workflow related to the TRM is illustrated with red numbers in Fig. 1 matching the following enumeration:

1. To provide the resulting trust scores to security management entities and end users in 5G virtualized networks, enablers should first publish relevant information held through the Integration Fabric, also depicted in Fig. 1, using a publication/subscription mechanism that allows the TRM to subscribe to its publications. These parameters are related to specific entities in the

---

\(^5\)https://datatracker.ietf.org/doc/html/rfc8520
deployment for which we are interested in computing their trust/reputation score.

2) The TRM receives the subscribed data through the Fabric. In order to support this pub/sub mechanism, we have implemented two modules for the integration of the TRM. The first one corresponds to the publishing module to simplify the integration of the enablers providing the data while the second one is the subscription module integrated as part of the TRM.

3) All this gathered information is fed into the defined Smart Contracts, whose output includes the trust value (score obtained in a quantitative way) of VNFs and services or the Virtualized Infrastructure Manager (VIM), as well as the SLA and SSLA compliance (if applicable) and the Security Policies verification.

4) The enablers’ obtained values, together with the computed trust scores are stored in Data Services (as Trustable Data Collection) for further historical post-processing.

5) Once the TRM has populated the databases of the entities trust information, interested enablers may request the value of trust of a given 5G entity. For that end, the TRM relies on an Application Programming Interface (API) also provided through the Integration Fabric.

Secondly, the workflow for the MUD enabler is illustrated with blue numbers in Fig. 1 which correspond to the following explanation points:

1) In the first place, we start by integrating the step required to collect the standard MUD file. Here, we assume that an external device willing to access the network has previously sent its associated MUD Uniform Resource Locator (URL), which has been in turn received at the MUD Manager (as part of the security orchestrator) to restrict the device communications. The MUD Manager asks through the Integration Fabric for both the MUD file and the MUD file signature to the MUD File Server using the MUD URL. Note that, the MUD File Server is in charge of storing and delivering MUD files of a specific manufacturer.

2) In the second step, we address threat signalling using the threat MUD file which extends the typical MUD architecture introduced in step 1. In this case, the external device sends Domain Name System (DNS) requests to access certain domain, these requests are forwarded to the Threat Agent to restrict the device communications. The Threat Agent monitors DNS traffic from/to devices to the DNS service and detects if any DNS request is not solved. If that is the case, it returns a null value informed by the DNS service. The DNS service also serves as information collector from threat intelligence providers about compromised domains.

3) In case a null value is received, meaning that the domain is possibly compromised, the Threat Agent asks for confirmation to the Threat API and alerts the Threat MUD Manager about this domain. If so, the Threat API replies with information about the Threat Intelligence provider that marked that domain as compromised.

4) Finally, the Threat MUD Manager which has a similar role to the usual MUD Manger, uses the compromised domain name and asks for the associated Threat MUD file (and its signature) to the Threat MUD file Server. Note that, the Threat MUD, which is associated to a threat, contains all the domains affected by this threat as well as the filtering rules to limit the access to them. At this point, the Threat MUD Manager parses and enforces the filtering rules through the Security Orchestrator.

A. Use Case: Attack mitigation

The TRM enabler is integrated in the workflow of a test case whose main objective is to deploy security mechanisms like Internet Protocol security (IPsec) tunnelling and to detect/mitigate attacks such as non-legit VNF creation and manipulation. In this context, the TRM will maintain the trustability of each component updated in the virtualized infrastructure, including the trust calculation of the behaviour of IPsec tunnel, the Malicious VNF deployed, and the Monitoring System. In Fig. 2, in blue, we can observe how the IPsec tunneling is deployed (1.a, 1.b, 1.c) and, based on Security Data Collector information (2), how the TRM updates the trust calculation and sends it to the Security Orchestrator (3) and to the End-to-End (E2E) TRM (4). Additionally, in orange, we represent how
the TRM participates in the monitoring and attack mitigation procedure. In this flow, after a malicious event has been detected by the corresponding entities at domain level (1.a/b and 2.a/b), the TRM receives the attack mitigation data from the Security Data Collector (3.a/b) and updates the trust score of the monitored components/domains, lowering its values in case of abnormal behaviour detection. Then, the computed values are received at both the Security Orchestrator (4.a/b) and the E2E TRM (5.a/b) so the Decision Engine can select the most suitable solution for each involved domain.

### B. Use Case: vOBU deployment

In Fig. 3, we show a second use case workflow. Here, the TRM calculates the reputation value of the Virtual Domain where a virtual On-board Unit (vOBU) is to be deployed.

When an On-board Unit (OBU) moves between different domains (0), a new vOBU nearer to its new position needs to be deployed. Taking profit of the signalling from the gNB to the 5G core (1), the Security Orchestrator (2) of the visited domain notifies the E2E level (3), which triggers the deployment of the new vOBU (6). Previously, the trust score for the whole visited domain has been retrieved (5) to help deciding whether to trust the visited domain. Steps 6 and 7 depict the inter-domain policy enforcement of the vOBU deployment which, also at the visited domain level, will check the trust score (8) of the deployed vOBU VNF. At this point, the OBU traffic is rerouted to the new vOBU (9, 10, and 11) where the same DTLS proxy crypto material is present. Finally, the Edge Virtual Domain instantiates and releases the new vOBU (12) and its corresponding OBU traffic is forwarded through it (13).

### VI. Conclusion and Future Work

As 5G is expected to be such a flexible and dynamic network fulfilling multiple use cases with extremely diverse requirements, the potential attack surface will inevitably increase. Thus, our approach addresses the challenge of establishing the infrastructure and tools necessary for achieving trust management in dynamic environments. For doing so, in this paper we have introduced two novel mechanisms envisioned for the integration with the INSPIRE-5GPlus project.

We have described how each of these enablers contribute to different trust dimensions, devoting special efforts to the integration of these enablers together with the existing ones, in order to provide a higher level of trust information.

Future lines of research will focus on ensuring, at each domain level, powerful tools of trust which can be easily combined afterwards to provide a whole trust framework at multi-domain level.

**ACKNOWLEDGMENT**

The research is supported by the H2020 EU project INSPIRE-5Gplus project, Grant Agreement N 871808.

**REFERENCES**

[1] Y. Sun, Z. Tian, M. Li, C. Zhu, and N. Guizani, “Automated attack and defense framework toward 5g security,” IEEE Network, vol. 34, no. 5, pp. 247–253, 2020.
[2] S. Rathore, J. H. Park, and H. Chang, “Deep learning and blockchain-empowered security framework for intelligent 5g-enabled iot,” IEEE Access, vol. 9, pp. 90075–90103, 2021.
[3] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alenmy, R. Muñoz, R. Vilalta, C. Gaber et al., “Inspire-5gplus: Intelligent security and pervasive trust for 5g and beyond networks,” in Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020, pp. 1–10.
[4] Y. Nugraha and A. Martin, “Understanding trustworthy service level agreements: Open problems and existing solutions,” in International Workshop on Open Problems in Network Security (iNetSec), 2017, pp. 54–70.
[5] C. Gaber, J. S. Vilchez, G. Gür, M. Chopin, N. Perrot, J.-L. Grimault, and J.-P. Wary, “Liability-aware security management for 5G,” in 2020 IEEE 3rd 5G World Forum (5GWF), IEEE, 2020, pp. 133–138.
[6] M. Al-Khafajiy, T. Baker, M. Asim, Z. Guo, R. Ranjan, A. Longo, D. Puthal, and M. Taylor, “Comitment: a fog computing trust management approach,” Journal of Parallel and Distributed Computing, vol. 137, pp. 1–16, 2020.
[7] S. Gyawali, Y. Qian, and R. Q. Hu, “Deep reinforcement learning based dynamic reputation policy in 5g based vehicular communication networks,” IEEE Transactions on Vehicular Technology, 2021.
[8] E. Bellini, Y. Iraqi, and E. Damiani, “Blockchain-based distributed trust and reputation management systems: A survey,” IEEE Access, vol. 8, pp. 21127–21151, 2020.
[9] M. Souppaya, D. Montgomery, W. Polk, M. Ranganathan, D. Dodson, W. Baker, S. Johnson, A. Kadam, C. Pratt, D. Thakore et al., “Securing small-business and home internet of things (iot) devices: Mitigating network-based attacks using manufacturer usage description (mud),” Special Publication (NIST SP) - 1800-15, 2021.
[10] T. Polk, M. Souppaya, B. Haag, and W. C. Barker, “Mitigating iot-based distributed denial of service (ddos),” US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, 2017.
[11] A. Hamza, H. H. Gharakheli, and V. Sivaraman, “Combining mud policies with sdn for iot intrusion detection,” in Proceedings of the 2018 Workshop on Iot Security and Privacy, 2018, pp. 1–7.
[12] M. Ranganathan, D. Montgomery, and O. El Mimouni, “Implementing manufacturer usage descriptions on openflow sdn switches,” tspapps.nist.gov, 2019.
[13] S. Patil, M. Grayson, B. Pularikkal, S. Anantha, and S. Chakraborty, “IoT device policy management framework in 5g/4g cellular networks,” Technical Disclosure Commons, 2018.
[14] OASIS, “Cyber Threat Intelligence - STIX and TAXII,” 2017. [Online]. Available: https://www.oasis-open.org/news/announcements/stix-v2-0-and-taxii-v2-0-are-now-oasis-committee-specifications
[15] R. Danyliw, “RFC 7070 - The Incident Object Description Exchange Format,” 2016. [Online]. Available: https://tools.ietf.org/html/rfc7070
[16] NIST, “Securing Small-Business and Home Internet of Things Devices: NIST SP 1800-15,” 2021.
[17] ETSI, “Network function virtualisation (nfv); nfv security; security and trust guidance,” ETSI GS NFV-SEC 003 V1.1.1, 2014. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/nfv-sec/001_099/003/01.01.01_60/gs_nfv-sec003v010101p.pdf