Joint opportunistic approaches for building resilient information sharing toward heterogeneous networks integration*

Agnaldo de Souza Batista[1], Aldri Luiz dos Santos[1,2] (Advisor)

[1]Departamento de Informática – Universidade Federal do Paraná (UFPR)

[2]Departamento de Ciência da Computação – Universidade Federal de Minas Gerais (UFMG)

asbatista@inf.ufrgs.br, aldri@dcc.ufmg.br

Abstract. *Massive networks demand resilient critical infrastructures as a means to achieve a safe operation against threats to their continuous and correct functioning. As a novelty, this thesis argues that the application of multi-opportunistic approaches can aid more robust information sharing on networks in the face of anomalies, and time- and space-sensitive data, thus enhancing overall resilience. To validate the hypothesis, we applied two opportunistic approaches jointly in a fixed environment on a collaborative network intrusion detection system (C-NIDS) for IoT networks against distributed denial-of-service (DDoS) attacks. Next, we employed two approaches on a location service in a network of unmanned aerial vehicles (UAVs) against false data injection (FDI) attacks. Thus, we evinced that a number of opportunistic approaches when employed jointly has great potential to provide resilient services across various network critical structures.*

1. Introduction

The environments of massive networks pursue to meet user and system needs by properties like high coverage extension, intense connectivity, higher data rates, lower latency, and higher reliability [Mohsan et al. 2022]. The demand for robust infrastructure services, particularly in handling anomalies, time- and space-sensitive data, and to support computationally intensive applications depends on resilient and safety network operation that makes up those integrated environments. Thus, ahead of fault tolerance due to attacks, the property of resilience emerges as an essential requirement for seamless network integration. In this thesis, we assume the concept of resilience as "*The ability to preserve the dependability of a system in the face of disruptions, thus absorbing, adapting, or recovering from damages"*.

Robust critical infrastructure services require the application of dependability techniques to attain resilient control information exchange in order to meet the need for a fast, adaptive, and low-energy-consumption response time. These infrastructure services rely on information sharing, many of them real time, to support networks operation, while their exchanged control data are vulnerable to several threats, whether malicious or stemming from the regular network functioning. Lately, applied strategies target data protection [Song et al. 2023, Pang et al. 2022] and reliability

*This study was financed by CAPES, Finance Code 001, and by FAPESP, grant #2018/23098-0.

[Shen et al. 2013, Li and Shen 2009, Liu et al. 2022, Firdaus and Rhee 2021], but they are often unsuited to deal with the constraints of massive network environments and its low delay response time. Thus, the adoption of jointly opportunistic approaches (OPPAPPS) to provide resilience to information sharing emerge as a promising way to deal with the pervasive operation of modern and future network environments.

Problem statement: Critical network infrastructure services are inherently vulnerable to several threats, whether malicious or originating from node and link failures. Further, issues like device connectivity, mobility, and energy depletion can reduce or even compromise network performance. Faced with these challenges, the countermeasures focused on resilience generally pursue to apply techniques like data replication, redundancy, and aggregation. Nevertheless, the approaches commonly disregard the instant of node interactions to enhance data exchanges. Therefore, they become unsuitable for addressing the dynamic nature of modern networks. Thus, the problem statement can be summarized as "*How to achieve resilient information sharing in networks against disturbances in their continuous and correct operation, thus supporting the seamless integration of heterogeneous networks into massive networks"*.

From the issues above and the challenges to provide resilience to information sharing on current networks, *the hypothesis investigated in this work is that combining OPPAPPS to support information sharing on networks enhances overall resilience and contributes to the seamless integration of heterogeneous networks into massive networks*. These approaches aim to establish network connectivity even without prior knowledge of existing contacts and in an infrastructure-less environment [Spyropoulos et al. 2010]. OPPAPPS have been applied over the time to build network infrastructure, enable routing services, and address mobility issues, among other applications. However, the lone application of these techniques is often unsuitable to achieve resilience in information sharing in current networks. This hypothesis relies on the premise that information sharing is crucial to network operation and enables the integration of networks by a resilient information exchange. Hence, these issues and challenges raise these research questions: **RQ 1:** *Which opportunistic approaches provide resilience to information sharing on dynamic networks?*; **RQ 2:** *How opportunistic approaches can face disturbances on dynamic networks functioning to achieve resilient information sharing?*; and, **RQ 3:** *How opportunistic approaches can work jointly to provide resilience in dynamic networks?*.

Objectives and contributions: The main objective of the thesis was to investigate, classify, and propose the adoption of OPPAPPS jointly to achieve resilient information sharing on dynamic networks to aid seamless heterogeneous network integration. In this way, we defined the following specific objectives: (i) Investigate existing approaches that have been applied to attain resilience in information sharing on dynamic networks; (ii) Classify those approaches and propose a taxonomy taking in account the faced threats, network disruptions and performance issues; (iii) Identify the OPPAPPS suitable to dynamic networks functioning, which may promote to resilient information sharing on dynamic networks; and (iv) Analyze and design the adoption of OPPAPPS for critical infrastructure services in fixed and mobile networks to provide resilience to information sharing.

The development of the thesis resulted in the following scientific contributions in the area of network security and communication, particularly on resilience to information

sharing in dynamic networks towards massive network integration [1].

- ***A survey on resilience in information sharing on networks***. This study presents a taxonomy of the existing approaches capable of fostering resilience to information sharing on networks, particularly according to the faced threats, network disruptions, and performance issues. These techniques benefit society by enabling the establishment of new resilient solutions for current and future networks. Furthermore, network integration paves the way for building and maintaining increasingly massive networks while meeting the decision-making requirements for secure, constant, accurate, and fast operations [Batista and Santos 2024].
- ***A resilient IoT NIDS-information sharing service***. This study investigated applying jointly OPPAPPS in a fixed IoT network environment to foster information sharing in an accurate and freshness way among NIDS belonging to a resilient collaborative NIDS against threats such as distributed denial-of-service attacks (DDoS). Besides improving overall security, such approaches enable the seamless integration of networks [Batista et al. 2025, Pedroso et al. 2024][2].
- ***A resilient UAVs location sharing service***. This study investigated engaging OPPAPPS in a mobile Flying Ad Hoc Network (FANET) to improve information sharing in an accurate and freshness way among UAVs against threats like Black hole and false data injection (FDI) attacks. In addition to boosting the spatial awareness of UAVs, these approaches advance to safe operation and network security [Batista and Santos 2026, Batista and Santos 2025][2].

2. A Resilient NIDS in IoT networks

As the identification and mitigation of malicious actions on structural traffic services in massive networks, such as a number of IoT networks, depend on greater resilience, we developed the C-NIDS (Collaborative-Network IDS) system for IoT data traffic analysis against DDoS attacks[3]. Unlike the approaches recently applied in the literature, C-NIDS exploits first contact and direct delivery between NIDSs, and freshness and age of the warning messages about existing attacks.

2.1. Environment model

We suppose a network environment composed of a couple of IoT networks – Net_1, Net_2, ..., Net_n. Figure 1 illustrates a scenario of an environment with three IoT networks, where a signature-based NIDS keeps rules to meet the security requirements of the IoT network domain. This NIDS runs on the gateway to analyze all the data traffic traversing it and protect the network. The NIDSs work standalone and connect through the Internet or another access control network to form the C-NIDS. Over the established network, NIDSs

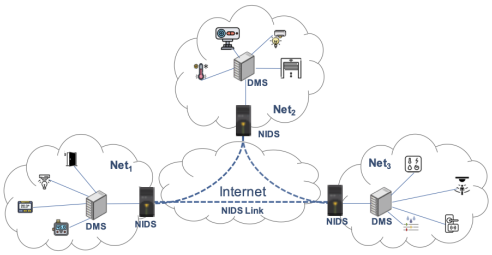

Figure 1. Collaborative NIDS

[1]Scientific production and citations are available on Google Scholar.
[2]The in-depth assessment can be found in the thesis.
[3]Source code found at https://github.com/mentoredproject/WP3-IEEE-LAT-2025

communicate with each other to exchange warning messages about the attacks, hereinafter referred to as *attack information*.

Network model: Each IoT domain, referred to as an island model, corresponds to a set of IoT devices, one data monitoring server (DMS), one NIDS, and one gateway. IoT devices collect environmental data and send them to DMS for a given application, whereas the DMS on each island frequently exchanges data to keep a complete view of the surveyed environments. The NIDS runs on the gateway to monitor the data traffic traversing devices from/to the island. Hence, C-NIDS establishes an overlay with NIDSs nodes to exchange warning messages and update their rules database whenever a NIDS detects an intrusion.

NIDS model: Each NIDS runs standalone on an island gateway to monitor, detect, and mitigate threats to this environment. It analyzes the traffic traversing the gateway and, whenever it detects an attack, mitigates the threat while storing the attack information. Next, it sends such information to other NIDS within the C-NIDS.

NIDS communication model: NIDSs within C-NIDS connect through a secure and direct channel only when a NIDS is under attack. Each NIDS keeps other NIDS updated about detected intrusions by warning messages, which carry a tuple $\langle Id, Anomaly, AplRule, FwdFlag \rangle$, where *Id* is the NIDS identification; *Anomaly* indicates the type of detected intrusion; *AplRule* is the applied rule to mitigate the threat; and, *FwdFlag* indicates to the receiver NIDS the need to forward such message to other NIDS. As a NIDS under a DDoS attack may be overloaded, such a menace impairs its communication with others, so we devised an opportunistic strategy to improve attack information delivery to help a NIDS under attack sends warning messages to others. Thus, it shares attack information in two stages: *sending* and *forwarding*, according to the value of *FwdFlag*. A NIDS under the DDoS attack ends collaboration when it shares attack information with another NIDS, i.e., the *sending* stage. The first device that confirms receipt of the information incorporates the applied rule into its rules database and becomes responsible for *forwarding* it to other NIDS, whose reception acknowledge is required. Therefore, the collaboration occurs in two steps, i.e., directly between the threatened NIDS and another NIDS within C-NIDS, and between the latter NIDS and the other NIDSs not under attack.

Threat model: We focus on external threats like DDoS attacks aiming to compromise the reliability and availability of DMS functioning. These attacks intend to overload the communication channels between IoT devices and DMS, as well as among DMS, for damaging the DMS operational state. We specially focused on volumetric DDoS attacks performed by botnets that send a high volume of data traffic to the DMS of an IoT network. They occur over UDP and ICMP protocols to target the transport and network layers, respectively. Over the UDP protocol, the attack menaces communication between IoT devices and DMS, while over the ICMP protocol, it significantly compromises communication among DMSs.

2.2. Architecture

The C-NIDS architecture comprises a set of a standalone NIDS operating on the gateway of each island, as shown in Figure 1. Each island can represent distinct application domains, such as smart homes, industries, and hospitals. The NIDS monitors and analyzes the data traffic traversing the gateway to mitigate detected attacks through suitable countermeasures. Next, it shares with other NIDSs within C-NIDS the information about

intrusion detection to form a collaborative system. Thus, the C-NIDS' operation depends on direct communication among NIDSs to improve overall network security.

The C-NIDS encompasses signature-based NIDSs connected through the Internet or another access control network, as seen in Figure 1. Each NIDS protects a given IoT network environment, named Net_1, Net_2, and Net_3, by monitoring the data traffic traversing the gateway. These NIDSs keep preconfigured rules to meet the network domain security requirements. They establish connections to communicate and exchange attack information, such as the time of the attack, its signature, and the applied rule. The communication occurs when a NIDS is under DDoS attack and does not impact communication among IoT devices and DMSs. The operation of the C-NIDS relies on NIDSs configuration with specific rules according to the IoT application domain and its data traffic pattern. Thus, each NIDS must have a distinct rules database suitable for addressing potential threats to its network environment. Adding new NIDSs to C-NIDS means increasing the base of rules available for the system as a whole, which enables C-NIDS to face new threats and system scalability.

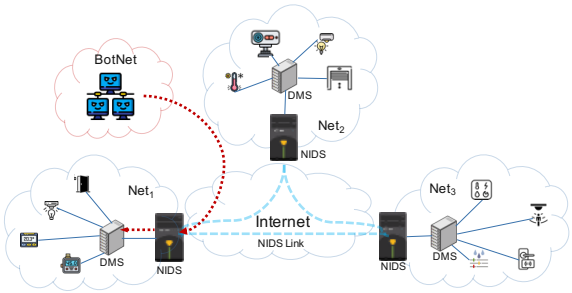

Figure 2. C-NIDS under DDoS attack

C-NIDS operation carries out as illustrated in Figure 2, where one island – Net_1 – is under a DDoS attack from an external entity, i.e., a botnet. For instance, the attack over UDP protocol target the transport layer in the communication between IoT devices and DMS. Such a threat causes DMS to deny receiving data from IoT devices and jeopardizes communication with other servers. Thus, the NIDS from Net_1 ($NIDS_1$) performs to detect attacks from the botnet, and upon detection, it takes configured rules to mitigate the threat. Next, it sends a warning message to the other NIDS within the C-NIDS carrying the attack information. The NIDS under the DDoS attack stops sending warning messages whenever another NIDS acknowledges the receipt of this message. Supposing $NIDS_2$ received the message, it updates its events database with such information. Next, it forwards the warning message to the NIDS on Net_3 to finish information sharing started by $NIDS_1$. As a result, other NIDSs can apply the shared knowledge to address new threats within their network environment.

Evaluation methodology and outcomes: We analyzed the C-NIDS system by emulation in a virtualized environment. The achieved results pointed out that jointly OPPAPPS support warning messages exchanges and fosters collaboration among NIDSs, thereby enabling a C-NIDS resilient operation, which answers RQ 2. Moreover, the orderly employment of the OPPAPPS proved to be essential to lead network operation to a resilient state, enhancing overall security against malicious disturbances, such as DDoS attacks, thereby answering RQ 3.

3. A resilient location service in UAV networks

Mobile networks, as UAV ones, also make up the massive networks, and present greater challenges due to the vulnerabilities raised by vehicles mobility and energy limitations,

compromising the provision of critical structural services. We present a resilient UAV location-sharing service – FlySafe[4] – to make UAVs aware of others in their coverage area to conduct proper flight coordination and avoid collisions. Unlike approaches often adopted, FlySafe relies on opportunistic interactions between UAVs, their mobility, and freshness and age of location information.

3.1. Setting model

FlySafe runs between network and application layers to enable UAVs to share their location with others. Hence, they make distributed and autonomous decisions to report their presence and mobility behavior. They operate in two phases: *Neighbor discovery* and *Neighbor maintenance*. A network discovery protocol combined with OPPAPPS epidemic and direct delivery perform for UAVs throughout both phases so that UAVs can identify their neighborhood and keep them updated. UAVs dynamically adjust their sensing scheme based on their mobility behavior to obtain accurate location information from others. Therefore, vehicle sensing capabilities and interactions support epidemic and direct delivery approaches, which carry out to the overall reliability and efficiency of location sharing among UAVs. UAVs compute their location by GPS and proactively interact with others to exchange such information. Thus, information exchange aids a seamless neighbor discovery while disregard previous vehicle interactions to reduce location perception errors. Direct delivery improves location-sharing efficiency since UAVs already know their neighbors and can interact directly with them. Further, the operation of the joined approaches enables resilient location information sharing and leads UAVs to achieve spatial awareness.

FlySafe runs over a set of UAVs interconnected by a wireless communication network, as depicted in Figure 3, denoted by $\mathcal{U} = \{u_1, u_2, u_3, ..., u_j\}$, where $u_j \in \mathcal{U}$. We take all UAVs have communication and processing resources to disseminate data, and each one owns a unique address (Id) to identify it in all time slots t. The neighborhood information of a UAV u in a slot t, $\mathcal{W}_u^t$, for instance, encompasses information of others by a set of distinct tuples $\langle Id, t, L^t, q^t, h^t, a^t, d^t, s^t \rangle$. Thus, $\mathcal{W}_u^t = \{\langle Id_1, t, L_1^t, q_1^t, h_1^t, a_1^t, d_1^t, s_1^t \rangle, \langle Id_2^t, t, L_2^t, q_2^t, h_2^t, a_2^t, d_2^t, s_2^t \rangle, ..., \langle Id_j, t, L_j^t, q_j^t, h_j^t, a_j^t, d_j^t, s_j^t \rangle\}$.

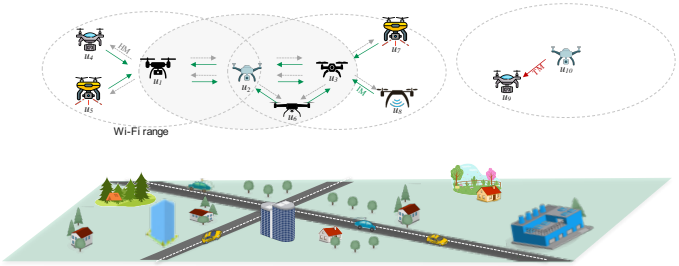

Figure 3. UAVs Environment

We denote the location of each UAV u, L_u^t, as a tuple $\langle x_u^t, y_u^t, z_u^t \rangle$, meaning its position in a 3D space. The *quality flag* q_u value shows how fresh is the neighbor location kept in a UAV u neighbor list (NL), i.e., it points out the update frequency of such information. q_u holds an integer value between 0 and 3, so that it compels *NL* updates in a maximum of three time slots, thus ensuring UAVs maintain their spatial awareness. The *hop flag* h_u value indicates whether the neighbor is within a coverage area of a UAV, $h_u = 1$, or beyond it, $h_u > 1$. Hence, it helps to extend UAV's spatial awareness by enabling knowledge about others outside the coverage area. The *attitude flag* a_u value

[4]Source code found at https://github.com/agnaldosb/flysafe-fdi

represents a neighbor mobility behavior relative to a UAV, i.e., inbound, 1; outbound, 2; or a static position, 0. The *distance* d_u equals the Euclidean distance between a UAV and one neighbor. The *state* s_u value means whether the neighbor UAV is ordinary, 0, or malicious, 1. We assume that a turned-off or a stationary UAV on the ground is out of the network. Further, any UAV can act maliciously and make an FDI attack by sharing false location to jeopardize the FlySafe operation.

As all UAVs move in time and space, they can simultaneously be a neighbor of one or more UAVs according to their location. Each UAV operation starts with neighbor discovery and shifts to neighborhood maintenance. Hence, it can establish *ad hoc* network connections with others to exchange messages. Whenever a neighbor moves outbound from a UAV coverage area, it eventually interrupts established connections. As displayed in Figure 3, UAV u_1 can establish *ad hoc* networks to connect with various neighbors, like u_2, u_4, u_5, whereas u_2 also belongs to u_6 neighborhood, $\mathcal{W}_6 = \{u_2, u_3\}$.

3.2. Malicious neighbors sensing

Whenever a UAV receives a message, it checks the coordinates sent by the neighbor UAV and computes the distance between them. Whether the obtained distance is greater than the coverage radius of the embedded communication technology, the component recognizes the neighbor UAV injects false location data in the network, i.e., it performs an FDI attack. In this sense, all UAVs start operating and create their Suspect List (SL) to hold information about malicious UAVs. Whenever a UAV *u* receives a message, its provenance is first assessed to avoid processing messages from malicious UAVs already blocked by the system. In the case of a false location received from an honest neighbor *n*, UAV *u* turns it suspicious and puts it in SL. Next, UAV *u* notifies all its neighbors about *n* and processes the received message. When the received message comes from a known malicious UAV *n*, *u* increases this *n* recurrence by 1. Whether *n* achieves a threshold of 3 false locations sent in a row, *u* blocks *n* in the SL and removes it from NL. Next, it notifies others about the blocked UAV and drops the received message.

Wether a UAV *n* sends a false location due to a GPS failure, for instance, it becomes suspicious to its neighbors. Case *n* sends a true location in a row, the receiver UAV decreases its recurrence by 1. When *n* recurrence reaches 0, it means *n* became honest. Hence, the receiver UAV *u* changes the *n* state to honest and removes it from SL. Then, the UAV *u* notifies others about *n* and processes the received message.

Evaluation methodology and outcomes: We analyzed the FlySafe system through simulations. The achieved results show that jointly OPPAPPS enable UAVs to share location information in a secure, accurate, and fast way, leading them to keep spatial awareness almost during the entire flight, thereby answering RQ 2. Further, the ordered application of the OPPAPPS verified pivotal to bring resilience to network regular operation, enhancing security against malicious disturbances like FDI attacks, which answers RQ 3.

4. Conclusion

The thesis addressed resilience and security on networks from the application of opportunistic approaches jointly and orderly for the sake of their seamless integration toward

building massive networks. We have studied and classified the resilience techniques identified through a systematic literature review and establish a taxonomy on resilience. To enhance resilience to an IoT-NIDS information sharing service, we employed jointly two OPPAPPS on a collaborative network intrusion detection system (C-NIDS) that share warning alerts even in the face of disturbances, such as DDoS attacks. We also applied combined OPPAPPS to bring resilience to a location service for UAV networks, thereby overcoming the dynamic characteristics of such network environments. UAVs actively share their location information with others to improve their spatial awareness even in the face of FDI attacks. The achieved results showed the adoption of jointly OPPAPPS improved information sharing resilience.

References

Batista, A., Pedroso, C., Brísio, S., Rodrigues, G., and Santos, A. (2025). Evaluating Robustness and Reliability of a C-NIDS for IoT Networks in Virtualized Environments. IEEE Latin America Transactions, 23(5):363–370.

Batista, A. and Santos, A. (2026). Analyzing The FlySafe System Face to Malicious UAVs Playing Black Hole Attacks. In Simpósio Brasileiro de Cibersegurança, SBSeg 2026, Porto Alegre, RS, Brazil. SBC.

Batista, A. S. and Santos, A. L. (2024). A Survey on Resilience in Information Sharing on Networks: Taxonomy and Applied Techniques. ACM Computing Surveys, 56(12):1–36.

Batista, A. S. and Santos, A. L. (2025). Resilient UAVs location sharing service based on information freshness and opportunistic deliveries. Pervasive and Mobile Computing, 111:102066.

Firdaus, M. and Rhee, K.-H. (2021). On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks. Applied Sciences, 11(1):414.

Li, Z. and Shen, H. (2009). A mobility and congestion resilient data management system for distributed mobile networks. In Proceedings of the 6th International Conference on Mobile Adhoc and Sensor Systems, MOBHOC, pages 60–69, New Jersey, USA. IEEE.

Liu, Y., Dong, Y., Wang, H., Jiang, H., and Xu, Q. (2022). Distributed Fog Computing and Federated-Learning-Enabled Secure Aggregation for IoT Devices. IEEE Internet of Things Journal, 9(21):21025–21037.

Mohsan, S. A. H., Khan, M. A., Alsharif, M. H., Uthansakul, P., and Solyman, A. A. A. (2022). Intelligent Reflecting Surfaces Assisted UAV Communications for Massive Networks: Current Trends, Challenges, and Research Directions. Sensors, 22(14).

Pang, Z., Yao, Y., Li, Q., Zhang, X., and Zhang, J. (2022). Electronic Health Records Sharing Model Based on Blockchain With Checkable State PBFT Consensus Algorithm. IEEE Access, 10:87803–87815.

Pedroso, C., Batista, A., Brisio, S., Rodrigues, G., and Santos, A. (2024). A Direct Collaborative Network Intrusion Detection System for IoT Networks Integration. In Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, SBRC 2024, pages 309–322, Porto Alegre, RS, Brazil. SBC.

Shen, H., Li, Z., and Chen, K. (2013). A Scalable and Mobility-Resilient Data Search System for Large-Scale Mobile Wireless Networks. IEEE Transactions on Parallel and Distributed Systems, 25(5):1124–1134.

Song, Z., Zhou, T., Zhong, W., Chen, D., Liu, L., and Yang, X. (2023). Fault-Tolerant Data Aggregation Scheme Supporting Fine-Grained Linear Operation in Smart Grid. IEEE Access, 11:2169–3536.

Spyropoulos, T., Rais, R. N. B., Turletti, T., Obraczka, K., and Vasilakos, A. (2010). Routing for disruption tolerant networks: Taxonomy and design. Wireless networks, 16(8):2349–2370.