A Direct Collaborative Network Intrusion Detection System for IoT Networks Integration

Carlos Pedroso[1], Agnaldo Batista[1], Samuel Brisio[2], Rodrigues S. R.[2], Aldri Santos[1,2]

[1]Núcleo de Redes Sem-Fio e Redes Avançadas (NR2) – UFPR

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

{capjunior, asbatista}@inf.ufpr.br, guilherme-sr@ufmg.br, {samuelbrisio, aldri}@dcc.ufmg.br

Abstract. *Integrating thousands of smart devices over the various IoT domains will require the devices to deliver services free of threats. Although intrusion detection systems (IDS) offer a multi-layer of protection to IoT networks, they commonly operate in isolation, thus restraining their application in integrated environments. In this context, collaboration among IDS emerges as an alternative to enhance intrusion detection, relying on their knowledge about faced threats. However, collaborative IDS (CIDS) generally exchange messages through centralized entities, disregarding direct communication among IDS. This work proposes a collaborative network IDS (C-NIDS) that integrates standalone NIDS for sharing information about detected and mitigated threats, improving overall intrusion detection. Evaluation results showed that C-NIDS achieved an attack detection rate of 99%, enhancing the attack mitigation by up to 50% compared to non-collaborative scenarios.*

1. Introduction

Intrusion detection systems (IDS) have usually been applied to prevent several classes of attacks. In general operating independently, they aim to detect and mitigate malicious activities surpassing the first security layer of the networks [Heidari and Jabraeil Jamali 2022, Hara and Shiomoto 2020]. However, mainly in Internet of Things (IoT), the growing number of devices in numerous application domains hampers their inter-operation and resilience in such environments [Abikoye et al. 2021, Tanwar et al. 2022]. Therefore, a seamless integration of such heterogeneous IoT networks claim for secure environments for device operation by robust and integrated approaches. In this regard, Collaborative Intrusion Detection Systems (CIDS) emerge as a possible response, standing out by enabling IDS to share knowledge and experience, like alarms and attack signatures. Such collaboration allows building a collective knowledge about faced threats and attacks, and increasing overall detection accuracy [Alkadi et al. 2020, Putra et al. 2021]. CIDS enables a secure environment for the convergence of IoT networks by strengthening threat defense and improving IoT interconnection in increasingly complex environments.

Since CIDS operation relies on exchanging messages among IDS, the knowledge of each IDS holds about threats faced during its operation naturally becomes pivotal to leverage the operation of others belonging to CIDS beyond a Zero-Knowledge condition [Feige et al. 1988]. Further, the sooner an IDS under attack shares its knowledge about a faced threat, the faster other IDS are ready to overwhelm similar threats, i.e., the age of attack-related information [Yates et al. 2021] is critical to overall CIDS performance. Although these IDS know each other previously, they establish connections

only when an IDS faces any threat. Hence, such a network performs as an opportunistic network [Lilien et al. 2006], where an IDS directly delivering [Spyropoulos et al. 2004, Sachdeva and Dev 2021] the available knowledge to other IDS enhances network protection and, hence, CIDS overall performance.

Since that communication between IDS is essential to a collaborative operation, several studies aim to enhance IDS interactions. In a layered structure, network IDS devices follow the network hierarchy to make decisions about attack detection [Nguyen et al. 2019, Kheddar et al. 2023]. Further, technologies, such as blockchain and cloud, offer a transparent layer for collaboration between IDS, enabling IoT devices to run as thin clients [Alkadi et al. 2020, Javadpour et al. 2023]. As CIDS operates decentralized, a cloud storage system can act as middleware, ensuring the availability of attack-related information for autonomous IDS [Putra et al. 2021]. In host-based approaches, machine learning classifiers analyze data traffic and collaborate in making decisions about attacks [Nguyen et al. 2022]. Transfer learning aids collaboration by enabling system training using a small scale of data from the target domain based on knowledge acquired from a source domain [Mehedi et al. 2022, Luo 2023]. These strategies promote collaboration between IDS, but they often restrict the direct communication of such devices. Hence, they increase the time required for attack detection and mitigation, jeopardizing network recovery. This constraint highlights communication barriers in CIDS to enhance the overall efficiency and responsiveness of intrusion detection and mitigation processes.

This work addresses a collaborative network intrusion detection system (C-NIDS) for IoT networks. NIDS devices communicate directly to share information about previously mitigated threats, like alarms, detection rules, and attack signatures, thus improving overall attack detection. Each NIDS device operates autonomously, protecting its local IoT network. They play collaboratively by exchanging such information in the face of a detected attack. Therefore, other NIDS devices can perform better against similar threats and improve their accuracy, detection, and response times. The proposed C-NIDS works in a distributed and collaborative manner, establishing a framework where direct communication among NIDS nodes reduces the damage caused by attacks aimed at communication among devices belonging to an IoT network. Evaluation results showed that our C-NIDS achieved a detection rate of 99%, with 0% false negatives and 100% true positive rate, and increased the attack mitigation by up to 50% compared to non-collaborative scenarios. Further, it achieved a collaboration time among NIDS of less than 16 seconds, highlighting the effectiveness of direct cooperation.

This paper proceeds as follows. Section 2 presents the related work. Section 3 details the proposed C-NIDS system. Section 4 discusses system performance evaluation, and Section 5 presents conclusions and future works.

2. Related Work

Collaboration among IDSs has enhanced anomaly detection by leveraging approaches like blockchain, trustworthy collaboration, and machine learning. The decentralized nature of blockchain is harnessed to enable IDSs to share detection signatures, enabling data exchange and ensuring IoT devices function as lightweight clients [Alkadi et al. 2020]. Trustworthy collaboration includes device trust assessment [Putra et al. 2021], contributing to detection of IoT botnets by machine learning classifiers that analyze data traffic [Nguyen et al. 2022]. The use of machine learning comprises transfer learn-

ing, applying gained knowledge to combat attacks, like DoS, DDoS, and man-in-the-middle [Mehedi et al. 2022, Luo 2023]. These studies, however, overlook direct communication among network IDS to facilitate real-time sharing of detection information.

In [Nguyen et al. 2019], IDS nodes run in a collaborative NIDS architecture for SDN-based IoT networks to detect anomalies through hierarchical layers. They formulate policies for gateway devices to block malicious traffic, including Edge-IDS, Fog-IDS, and Cloud-IDS. The strategy distributes traffic analysis, relieving edge nodes. Collaboration between IDS improves attack detection and mitigation. But dependence on IDS decisions at higher hierarchical levels compromises system performance. [Sarhan et al. 2023] present a distributed IDS for IoT network security using SDN and an optimized decision tree algorithm. The system divides the network into monitored sub-networks with controller nodes, optimizing accuracy through the black hole optimization (BHO) algorithm. IDS employs a collaborative decision-making approach, with controller nodes sharing results and determining attacks through majority voting. However, the approach does not employ direct collaboration among IDSs, increasing decision-making time. [Pandey et al. 2023] propose an IDS for a secure social network, employing soft and cooperative edge computing. The approach seeks to optimize resource allocation and improve data transmission, improving network security and performance in IoT environments. Despite being a promising approach, the authors fail to address the collaboration time among IDS, focusing exclusively on information distribution at the network's edge.

In [Alkadi et al. 2020], a deep blockchain framework provides security-based distributed intrusion detection and privacy-based blockchain in IoT networks. It employs a bidirectional long short-term memory (BiLSTM) deep learning algorithm for sequential network data and treats IDS alerts as blockchain transactions. Blockchain consensus ensures alert validity and privacy for attack detection and mitigation. Given that heavy processing takes place in blockchain, IoT devices can play as lightweight clients for verifying and disseminating alert correctness. However, deep learning depends on available datasets for LSTM training and supporting CIDS operation, disregarding training costs or collaboration time. Further, since collaboration primarily occurs at edge devices, it overlooks direct communication among NIDS. In [Javadpour et al. 2023], a distributed multi-agent intrusion detection and prevention system (DMAIDPS) performs on Cloud Internet of Things environments. But the cloud centralization restrains direct information exchange and collaboration among NIDS, compromising network operation. In [Quincozes et al. 2021], an intrusion detection approach to a network of specialized detectors, called counselors, collaborates to enhance the accuracy of intrusion detection in environments with heterogeneous data sources. However, such an approach lacks of information about resolving conflicts between classifiers, the absence of representatives in training data, the scarcity of labeled signatures, and a comprehensive evaluation to highlight its effectiveness and robustness. In [Nguyen et al. 2022], a collaborative approach for early detection of IoT botnets employs several machine learning classifiers to analyze data traffic. They collaborate in the decision-making by voting about traffic analysis. Although the applied strategy enables botnet detection, as a host-based solution, it operates centralized.

In [Mehedi et al. 2022], the knowledge of a source domain allows training an IDS using only a small scale of data from the target domain. According to the training data, such IDS faces attacks such like DoS, DDoS, and man-in-the-middle. However, the operation of IDS relies on training data. In [Luo 2023], a cyber threat intelligence shar-

ing scheme employs federated learning for network intrusion detection. Nevertheless, the decision-making time and the direct collaboration are hindered by training time. In [Putra et al. 2021], a decentralized and trustworthy CIDS for IoT comprises three categories of nodes: validator, contributors, and regular, each playing a distinct role in the system. Validator nodes endorse rules submitted by contributing nodes, whereas regular nodes utilize shared, validated rules. The collaborative strategy enables nodes to confront unknown attacks by rules provided by CIDS from other environments. However, trust evaluation depends on predefined rules for validators. Further, as CIDS collaborate through a distributed storage system, it increases the system's detection time.

Therefore, there is a demand for solutions capable of acting through direct communication and identifying and isolating malicious actions in IoT networks. By preserving communication security between devices and servers, solutions must promote the integration by allowing multiple networks to connect and converge securely and resiliently.

3. A Collaborative NIDS

In this section, we describe the system model for the collaborative NIDS to provide IoT networks seamless integration. We also present the system architecture and its operation, and we discuss NIDS interactions to achieve overall collaboration and knowledge sharing.

3.1. Environment and NIDS model

We take into account a network environment composed by a couple of IoT networks - Net_1, Net_2, ..., Net_n, each of them protected by a signature-based NIDS operating on the gateway, as shown in Figure 1, which illustrates a scenario with three IoT networks. These NIDS operate standalone and connect through the Internet or another network access control to form the collaborative NIDS (C-NIDS). Over the established network, all NIDS communicate with each other to exchange attack-related information. As signature-based devices, they are previously configured with rules to meet the network domain security requirements and operate on gateway to analyze all the data traffic traversing it.

Network model: Each IoT domain, named 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 to a given application, whereas the DMS on each Island frequently exchange data to support a complete view of the surveyed environments. Running on the gateway, a NIDS monitors all the data traffic traversing the device from/to the Island. Therefore, C-NIDS establishes an overlay with all NIDS nodes so that they can exchange warning messages to update their rules database whenever a NIDS detects an anomaly on the IoT island.

NIDS communication model: All NIDS belonging to C-NIDS can connect to each other. However, such connections take place only when a NIDS is under attack. They communicate through a secure and direct channel, and, for simplicity, we disregard any communication failures. Each NIDS keeps other NIDS updated about detected anomalies 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 anomaly; *AplRule* is the applied rule to mitigate it; and *FwdFlag* indicates to the receiver NIDS the need to forward such message to other NIDS. As a NIDS under attack may be overloaded during

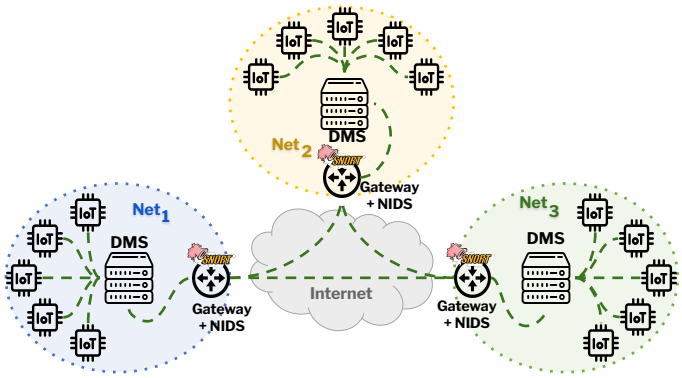


Figure 1. Collaborative NIDS

such period, which impairs its communication with other NIDS, we devised an opportunistic strategy to improve attack information delivery, where an attacked NIDS sends warning messages to other NIDS. Thus, information collaboration occurs in two stages: sending and forwarding, according to *FwdFlag* value. A NIDS under attack ends collaboration when it shares attack-related information with another NIDS, which corresponds to the sending stage. The first device that confirms receipt of the information incorporates the applied rule to its rules database and becomes responsible for forwarding it to others NIDS, which must acknowledge its reception. Therefore, the collaboration between a threatened NIDS and the others occurs in two steps, i.e., directly between a threatened NIDS and other NIDS, and between the later NIDS and the other NIDS not under attack.

NIDS model: Each NIDS operates 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, it mitigates the threat and stores the attack-related information. Next, it sends such information to other NIDS belonging to the C-NIDS.

Threat model: The main threat consists of attacks targeting the communication between IoT devices and the DMS, aiming to overload the channel to carry the server out of its normal state (i.e., its continuous and correct operation service). These attacks direct the data flow to the monitoring server, overwhelming it with a large volume of data, which leads it to deny service to IoT devices and servers on other networks.

3.2. C-NIDS architecture and operation

The architecture comprises a standalone NIDS operating on each island's gateway, as shown in Figure 1. Islands mean environments with physical IoT devices or emulate IoT environments with multiple devices; such devices interact and exchange information. Thus, each island can represent distinct application domains like smart homes, industries, and hospitals. A NIDS on the island gateway monitors the data traffic traversing it and mitigates detected anomalies through suitable countermeasures. Next, it shares information about anomaly detection, forming a collaborative system. Thus, C-NIDS' operation depends on direct communication among all NIDS to improve overall network security.

C-NIDS operation depends on all NIDS functioning, thus requiring their preconfiguration with specific rules according to the IoT application domain and its data traffic pattern. For example, supporting a *smart home* environment, a NIDS node should protect it from threats aiming to open a front door to interrupt the heating system, among

other unwanted actions. At the same time, a *smart industry* environment demands protection against attempts to interrupt an accumulation line to cut the energy supply, among other threats. Therefore, each NIDS can have a distinct rules database suitable to deal with the possible threats to its network environment.

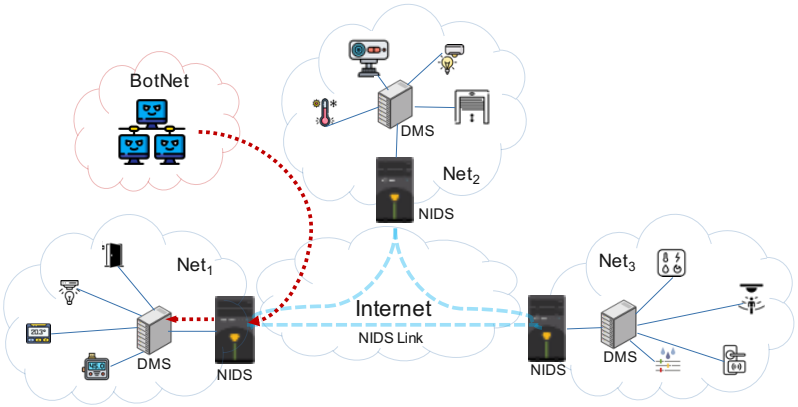


Figure 2. C-NIDS operation under attack

Figure 2 depicts a C-NIDS operation, where each NIDS protects an IoT network (island), and one island - Net_1 - is under attack from an external entity, like a botnet established through BoNeSi tool [Goldstein 2023]. For instance, the attack can target the transport layer in the communication between IoT devices and DMS, which occurs by UDP protocol. Such a threat leads DMS to a denial of service so that it cannot receive data from IoT devices while communication with other servers may be jeopardized. Another example is an attack threatening the network layer through a large data volume sent to DMS through ICMP protocol. In such a scenario, the communication between DMS through the TCP protocol can experience data losses, high delays, and latency. Therefore, considering a botnet attacking Net_1, as illustrated in Figure 2, its NIDS performs to detect the attack from the botnet. Upon detection, it employs some available preconfigured rules to mitigate the threat and sends a warning message to the other NIDS belonging to C-NIDS carrying the attack-related information. The NIDS under attack stops sending warning messages whenever another NIDS acknowledges the receipt of this message. Supposing the NIDS from Net_2 received the message, it keeps the information in its events database to update it and forward the warning message to the NIDS on Net_3, thus completing the sharing of information initiated by the NIDS on Net_1. Therefore, all the other NIDS can employ the acquired knowledge to tackle new threats within their network environment.

4. Evaluation and Analysis

We implemented the proposed C-NIDS in a virtual environment according settings presented in Table 1, and engaging a set of tools, as showed in Table 2, to emulate three distinct IoT networks and the DDoS attacks depicted in Figure 2. For this purpose, we employed Docker to build isolated environments called containers and KIND (Kubernetes in Docker) to make multiple Kubernetes nodes using containers. The plug-in Calico CNI implements the Kubernetes Container Network Interface (CNI), and assigns a fully routable IP address to each pod to establish a Layer 3 network, providing connectivity for containers and pods. The interaction with Kubernetes occurred by commands in the terminal through Kubectl to construct and remove clusters, pods, and services. Calicoctl enables us to assign IP policies for pods, manage security policies, and configure network

infrastructure and devices. Lastly, we emulated DDoS attacks targeting the monitoring servers through BoNeSi tool [Goldstein 2023], creating a botnet with 3,000 bots, which performed volumetric attacks of approximately 35,000 packets per second following the chronology presented in Table 3. During an emulation, each network was subject to two distinct attacks: one based on UDP protocol and one based on ICMP protocol.

Table 1. Emulation setup

Parameter	Value
Emulation duration	1200 s
IoT devices → DMS protocol	UDP
DMS ↔ DMS protocol	TCP
# IoT networks	3
# IoT devices per network	15
Data transmission frequency:	
- IoT devices	1 msg / s
- DMS	1 msg / 3 s

Table 2. Resources settings

Application	Tool	Version
Container orchestration	Kubernetes	1.25.3
Container management	Docker	24.0.2
Run local clusters	KIND	0.17.0
Container interface	Calico CNI	3.25
Clusters management	kubectl	1.27.2
Calico management	calicoctl	3.25.0
Botnet emulation	BoNeSi	0.3.1

As described in Table 4, we emulated the scenario depicted in Figure 2 in four distinct configurations to compare the performance achieved by the proposed C-NIDS. In BASE, networks operate regularly and are not subject to malicious threats, e.g., DDoS attacks. In the other three configurations, DDoS attacks took place, but NIDS were deactivated in BASE-NIDS, enabled in BASE+NIDS, and collaborated in COLLAB. This last configuration relies on rules previously available on each network NIDS: Net_1 NIDS holds a rule to UDP attacks, Net_2 NIDS keeps a rule to ICMP attacks, while Net_3 NIDS operates without rules to face attacks based on these two protocols. We considered a transient state ended at 60 s of each emulation, being the moment that all emulated devices reached their steady-state performance, i.e., when all nodes could send and receive messages. Hence, the presented evaluation considers the deletion of results obtained until 60 s of each emulation. Lastly, each emulation was run for 1200 s, and the applied metrics are averaged over 35 emulation runs to achieve a confidence interval of 95%. In the future, we intend to make all data public available on a git-based platform.

Table 3. Attacks chronology

Network	Attack protocol	
	UDP	ICMP
$\boldsymbol{Net}_1$	60 s – 180 s	840 s – 1020 s
$\boldsymbol{Net}_2$	240 s – 360 s	600 s – 780 s
$\boldsymbol{Net}_3$	420 s – 540 s	1080 s – 1200 s

Table 4. Scenario organization

Reference	Configuration
BASE	Operation without any threats
BASE-NIDS	BASE with DDoS attacks with disabled NIDS
BASE+NIDS	BASE with DDoS attacks with enabled NIDS
COLLAB	BASE+NIDS with NIDS sharing data

We evaluate C-NIDS taking into account *collaboration performance* and *security metrics*, as described in Table 5. *Collaboration performance metrics* measures the ability of C-NIDS to deal with the inflow of messages and how C-NIDS impacts network operation. *Collaboration security metrics* evaluate C-NIDS attack detection capabilities.

Table 5. Evaluation metrics

Metric description	Goal	Equation
Collaboration time (CT): The total time required to a NIDS to share the information about an attack with others NIDS belonging to the C-NIDS. CT equals the sum of sending time (ST) to one NIDS, the time to incorporate (IT) the received rules to NIDS rules database, and the time to forward (FT) the received message to other NIDS	P	CT = ST + IT + FT
Throughput (THR): The rate of message delivery over a communication channel. It equals the percentage of delivered messages (DM) in relation to total messages sent (TMS)	P	THR = (DM/TMS) x 100
Latency (LAT): The time taken for data to pass from one point to another on a network, i.e., the difference between the data sending time (DST) and data receiving time (DRT)	P	LAT = DRT - DST
Packet Loss rate (PLR): The percentage of non-received packets – difference between the quantity of sent packets (SP) and received packets (RP) – in relation to sent packets	P	PLR = ((SP - RP) / SP) x 100
Attack Detection Time (ADT): Indicates how fast a policy is conducted and implemented based on the analysis of the malicious traffic that generates an alert, i.e., the difference between the attack start time (ST) and attack detection alert time (AT)	S	ADT = AT - ST
Attack Mitigation Time (AMT): Measures how fast a policy is conducted and implemented after a detection alert is raised until its mitigation, i.e., the difference between the attack detection alert time (AT) and application of attack mitigation policy time (PT)	S	AMT = PT - AT
Detection rate (DR): Shows how C-NIDS correctly identify attacks	S	DR = (TP / (TP + FN)) x 100
True positive rate (TPR): The percentage of correctly labeled attacks	S	TPR = (TP / (TP + TN)) x 100
False negative rate (FNR): Indicates when C-NIDS fails to identify an anomaly and classifies it as normal and is represented by the percentage of attacks that are labeled as non-attacks	S	FNR = (FN / (TP + FN)) x 100

C: Performance metric; S: Security metric

4.1. Performance results

The collaboration among NIDS plays a crucial role in C-NIDS operation; hence, we start by examining how collaboration takes place to verify the impact on overall system performance and security under cyber attacks described in Table 3, as discussed next. According to scenarios configuration presented in Table 4, the collaboration occurs after DDoS attacks, from Net_1 NIDS after the first attack (UDP), and from Net_2 NIDS after the second attack (ICMP). In all scenarios, Net_3 NIDS operated without specific rules to face such attacks, thus depending on other NIDS collaborations to perform successfully. Therefore, in the COLLAB scenario, we measured the time to send (ST), incorporate (IT), and forward (FT) attack-related information to compute the *Collaboration time* (CT) each NIDS under attack takes to share its knowledge with others, as seen in Table 6.

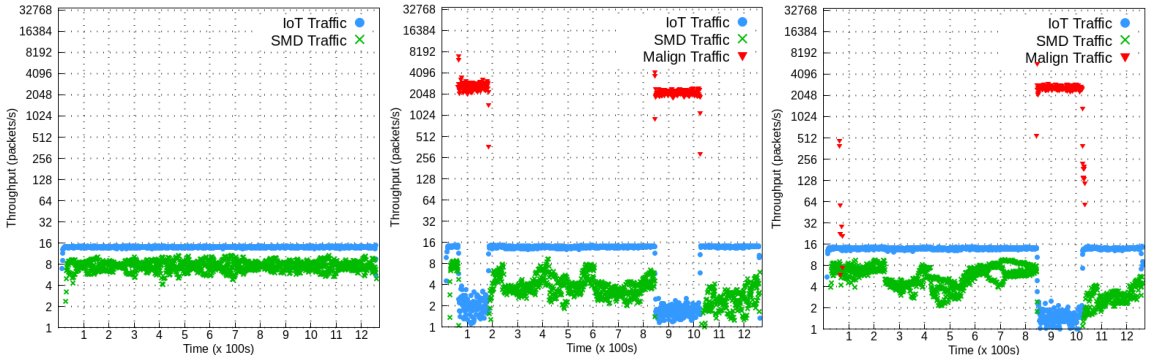
Table 6. Collaboration assessment

Network/Attack	Measured times			CT(s)
	ST(s)	IT(s)	FT(s)	
Net_1 - UDP attack	6.65	2.12	6.76	**15.53**
Net_2 - ICMP attack	0.54	1.29	0.52	**2.35**

The impact of attack type on CT is very distinct, as shown in the values in Table 6. It is worth noting that the first attack threatens the transport layer, whereas the

second menaces the network layer. Although both attacks target DMS communication, as it receives data from IoT devices through UDP protocol, the attack based on such protocol strongly jeopardizes its operation. Generally, a NIDS took 15.53 s to conclude the collaboration of attack-related information during the first attack – UDP-based, mainly because a NIDS under attack must probably be overloaded analyzing the traffic traversing the gateway into the IoT network. On the other hand, during the second attack – ICMP-based, the collaboration occurs much faster, generally concluding in about 2.35 s. In both situations, other NIDS are still ready to face a similar threat during the attack, highlighting the importance of all NIDS collaboration to the system's overall performance, as we will see in the following discussions.

The throughput assessment took communication between IoT devices and DMS via the UDP protocol and among DMS via the TCP protocol for each configured scenario. Due to space limitations, we present only the results from Net_1 for the BASE, BASE-NIDS, and BASE+NIDS scenarios; however, as all networks have similar characteristics, this does not affect the results. Figure 3 (a) exhibits the throughput results for the first three scenarios where BASE presents stable values, 15 messages/s for UDP traffic, and 20 messages/s for TCP traffic. We expected this behavior since networks operate regularly, without any threat, in the BASE configuration. Therefore, this conduct forms the basis for future comparisons and represents the best operating condition. On the other hand, BASE-NIDS is a type of attack without any network protection. In Figure 3 (b), we observe a substantial rise in the amount of malicious packets and a corresponding decrease in benign traffic during attack periods in both communications. The impact generated by attacks degrades the capacity data availability and communication among devices and servers. It is noteworthy that the network has no protection, allowing attacks to operate freely.

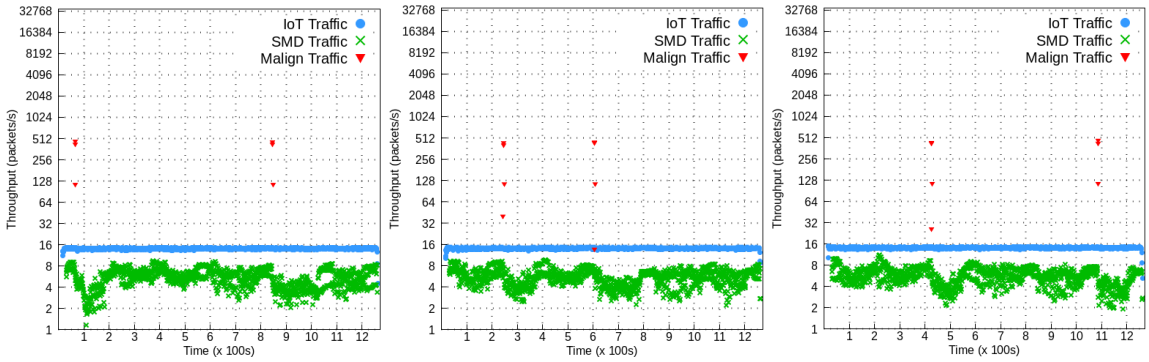


a) BASE b) BASE-NIDS c) BASE+NIDS

Figure 3. Network 1 data traffic

The BASE+NIDS scenario comprises both attacks under network protection provided by NIDS. Figure 3 (c) illustrates that network protection improved performance by 98% for both communications and maintained stable performance even under threats. However, NIDS achieved these results only against attacks for which it holds detection rules, emphasizing the importance of collaboration among NIDS. Figure 4 shows the throughput on the three networks in the COLLAB scenario, taking into account both attacks. All networks maintained stability, indicating a 99% improvement in attack mitigation compared to BASE-NIDS and BASE+NIDS. This result was achieved due to the effectiveness of C-NIDS, enabling interference-free communication among IoT devices

and DMS. This behavior underscores the efficacy of direct collaboration among NIDS in detecting and protecting networks against attacks, as it allows all NIDS to access the rules employed for attack detection.



a) Net_1 b) Net_2 c) Net_3

Figure 4. Network data traffic in COLLAB scenario

We conduct a complete latency assessment across various scenarios to examine the effects of device-to-server and server-to-server communication. The results allow us to quantify the effects of collaborative actions among NIDS on network security. We employed two approaches: the first targeted the latency of UDP traffic, while the second took into account TCP traffic, and both were considered during attack windows. Table 7 summarizes the latency values for the UDP protocol, categorized over the entire emulation time for all scenarios, and during the 1st and the 2nd attacks disregarding the BASE scenario. We observed stable values in the BASE scenario, with a variance of just 1.52 μs in communication among devices and servers across all networks. BASE-NIDS exhibited a latency variation of 3 μs and 1 μs for the 1st and 2nd attacks, respectively. Meanwhile, BASE+NIDS showed a variance of 10 μs for the 1st attack and 11 μs for the 2nd. However, the average latency time remained consistent at 94 μs for the 1st and 93.67 μs for the 2nd attack. Lastly, COLLAB presented a variance of 9 μs for the 1st attack and 3 μs for the 2nd. The mean across the networks for the 1st attack was 94.67 μs, and for the 2nd attack, it was 90.00 μs.

Table 7. UDP traffic latency

	LAT (μs)								
Window	**Emulation time**			**1st attack**			**2nd attack**		
Scenario	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3
BASE	149	150	147	-	-	-	-	-	-
BASE-NIDS	122	123	119	103	103	100	101	101	100
BASE+NIDS	105	105	108	100	90	92	89	100	92
COLLAB	96	97	93	98	97	89	91	91	88

Table 8 presents TCP traffic latency values for DMS communication. We observed a significant variation among the scenarios, particularly in the BASE-NIDS scenario. The server communication showed a variation of 55 μs during the 1st attack, and 1.0 μs during the 2nd attack. The BASE+NIDS scenario shows a 172 μs variation among all networks during the 1st and 11 μs during the 2nd attacks. In contrast, the COLLAB scenario showed an average latency variation of 132 μs for the 1st attack and 3.0 μs for the 2nd, indicating an improvement compared to the other scenarios. Furthermore, we observed

that the nature of volumetric attacks can lead to significant variations in latency. The results emphasize this latency behavior, given that UDP attack on device-server communication and ICMP attack on server-server communication accentuate values variation. It also supports the hypothesis that collaborative efforts increase the network's ability to recover quickly from damage caused by attacks. Besides, as a quality metric, ideal latency values vary for different communication types, subject to the influence of the protocols employed in data transmission.

Table 8. TCP traffic latency

	LAT (μs)								
Window	**Emulation time**			**1st attack**			**2nd attack**		
Scenario	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3
BASE	434	434	433	-	-	-	-	-	-
BASE-NIDS	390	378	379	511	566	520	101	101	100
BASE+NIDS	403	351	369	540	570	398	89	100	92
COLLAB	420	434	427	643	775	740	91	91	88

Table 9 highlights the results obtained regarding packet loss during the two attacks in different network scenarios. Organizing the data between the 1st and 2nd attacks allows a more detailed analysis of how packet loss impacts each protocol in different configurations. This strategy provides a comprehensive view of each network's vulnerabilities and identifies the scenarios most susceptible to each attack. As mentioned previously, the BASE-NIDS scenario revealed the highest losses, reaching up to 24% and 90% loss for the 1st (ICMP) and 2nd (UDP) attacks, respectively. These values were expected, considering the absence of specific security systems to prevent packet loss in communication among servers, depending exclusively on TCP control mechanisms. The BASE+NIDS scenario demonstrated a significant improvement compared to the previous scenario. In some cases, packet loss reached 0%, while in others it remained at 88%. This result occurs because only some NIDS have rules for identifying the 1st and 2nd attacks, while others do not. Notably, the COLLAB scenario showed the most promising results, recording 0% loss for the 1st and 2nd UDP attacks and ranging from 1% to 6% for ICMP attacks. These results highlight the effectiveness of collaboration among NIDS in protecting the network. The cooperation enables the direct exchange of information among systems, improving attack detection. When an attack is identified, NIDS shares the rule applied with others, strengthening the network's overall security.

Table 9. Packet Loss during attacks windows

	PLR											
Attack window	**1st attack**						**2nd attack**					
Attack protocol	**UDP**			**ICMP**			**UDP**			**ICMP**		
Network	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3
BASE-NIDS	83%	84%	83%	**24%**	29%	30%	**90%**	90%	90%	27%	25%	30%
BASE+NIDS	**0%**	84%	84%	4%	13%	33%	**88%**	0%	88%	26%	0%	23%
COLLAB	0%	0%	0%	**1%**	0%	2%	0%	0%	0%	4%	**6%**	0%

We also analyzed the full 1200 seconds of emulation, and the results revealed that the BASE scenario, without interference, showed no packet loss, serving as the baseline for subsequent scenarios. In the BASE-NIDS, an average of 21% packet loss was recorded across all networks, with a variation of 5%. Notably, this scenario lacked network protection. In the BASE+NIDS, the networks were individually protected by NIDS, operating in isolation, resulting in an average loss of 14%, with a variation of 9%. Finally, in the COLLAB, the average packet loss was 1% throughout the emulation.

4.2. Security results

The security assessment focused on deploying attack protection systems in the BASE+NIDS and COLLAB scenarios. Table 10 presents the results of the detection process, encompassing the time from the arrival of the first malicious packet to the DSM until the NIDS identifies this action. In the BASE+NIDS scenario, the absence of rules for all attacks results in Net_1 achieving the best detection time of 48 ms in the 1st attack and Net_2 recording 100 ms in the 2nd attack. In the COLLAB scenario, Net_3 stands out with the best detection time of 90 ms in the 1st attack and 32 ms in the 2nd attack. Averaging at 17 ms in critical moments attests to the system's detection effectiveness, which is attributed to the direct collaboration mechanism among the NIDS. These results emphasize the system's robustness, highlighting its substantial assistance to network security.

Table 10. Detection and Mitigation time

Metric	**ADT** (ms)						**AMT** (ms)					
Attack protocol	**UDP**			**ICMP**			**UDP**			**ICMP**		
Network	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3
BASE+NIDS	**48**	-	-	-	107	-	**47**	-	-	-	**78**	-
COLLAB	103	106	98	231	178	324	97	103	**90**	190	**123**	244

Table 10 summarizes values for the BASE+NIDS and COLLAB scenarios, specifying each network and type of attack regarding mitigation time, which involves interrupting the data malicious flow and source isolation after detection. In the BASE+NIDS scenario, Net_1 achieved the best mitigation time of 47 ms in the 1st attack, and Net_2 showed 78 ms in the 2nd attack. In the COLLAB scenario, Net_1 stands out with the best mitigation time of 90 ms in the 1st attack, and Net_2 records 123 ms in the 2nd attack. Comparing these values of detection times underscores C-NDIS's ability to take prompt action against threats. Furthermore, the immediate response to the threats expedites network recovery, guaranteeing a more secure communication environment among its participants. We highlight that direct collaboration increases the security of all network participants, thus ensuring greater communication availability.

Table 11. Detection, True positive and False negative rates

Attack	**1st attack**									**2nd attack**								
Metric	**DR (%)**			**TPR (%)**			**FNR (%)**			**DR (%)**			**TPR (%)**			**FNR (%)**		
Network	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3	Net_1	Net_2	Net_3
BASE-NIDS	**94.39**	0	0	100	0	0	**6**	100	100	0	**97.70**	0	0	100	0	100	0	100
COLLAB	**99.93**	**99.94**	**99.96**	100	100	100	0	0	0	99.97	99.85	99.96	100	100	100	0	0	0

Table 11 shows the security performance values for the BASE+NIDS and COLLAB scenarios under the 1st and 2nd attacks among Net_1, Net_2, and Net_3. Metrics include Detection Rate (DR), True Positive Rate (TPR), and False Negative Rate (FNR), expressed as a percentage (%). In the BASE+NIDS scenario, Net_1 achieved a high DR of 94.39% during the first attack. In comparison, Net_2 and Net_3 had 0% DR. These results were expected, as the NIDS of Net_2 and Net_3 did not have rules to identify the attack. TPR, representing the proportion of true positives from the total number of attacks, was 100% for Net_1 and Net_3, indicating complete detection. In contrast, Net_2 did not detect the attack. The FNR, meaning the proportion of false negatives about the total number of attacks, was 6% for Net_1, indicating a small number of undetected cases. In the second attack, Net_2 kept a high DR of 99.70%, while Net_1 and Net_3 failed to detect the attack. In the COLLAB scenario, all networks exhibited an impressive detection rate DR of around 99% for the first attack, indicating highly effective detection. TPR reached 100%, showing the

precise identification of all attacks. FNR remained at 0% for all networks, signaling that virtually no attacks went unnoticed. For the 2nd attack, the DR rates consistently hovered around 99%, and the TPR remained steadfast at 100%. The result points out that when detected, all NIDS accurately identify attacks. Similarly, FNR remained at 0%, showcasing the robustness of accurate identification, with the system rarely overlooking attacks.

Note that the DR, TPR, and FNR values may vary depending on the complexity and specific nature of the attacks since these attacks are volumetric, and NIDS are rule-based. Additionally, the adaptability of detection rules to new threats can influence the NIDS effectiveness. Also, in scenarios involving volumetric attacks, the traffic overload can affect the ability of NIDS to analyze and detect all instances of attacks. Thus, the variation in results can be attributed not only to the detection system's effectiveness but also to the specific characteristics of the attacks and the network dynamics during attack events.

5. Conclusion

This work presented a collaborative network intrusion detection system (C-NIDS) for dense IoT environments against volumetric DDoS attacks. C-NIDS aims to provide a resilient and integrated system among different networks to share threat-related information. For that, C-NIDS adopts direct communication among participating NIDS to reduce the time it takes to exchange information about threats and enable faster detection. The results demonstrate the effectiveness of C-NIDS in keeping networks operational in the face of volumetric attacks, consequently providing greater communication availability between devices and servers. Furthermore, C-NIDS improves detection time, data loss reduction, and network recovery time compared to scenarios without collaboration. As future work, we will make a C-NIDS based on anomalies, analyze its behavior in the same experiment and compare its performance against C-NIDS based on rules.

Acknowledgment

This work was supported by National Council for Scientific and Technological Development (CNPq/Brazil), grants #309129/2017-6 and #432204/2018-0, by São Paulo Research Foundation (FAPESP), grants #2022/06802-0 and #2022/06840-0, and CAPES, grant #88887.509309/2020-00.

References

Abikoye, O. C., Bajeh, A. O., Awotunde, J. B., Ameen, A. O., Mojeed, H. A., Abdulraheem, M., Oladipo, I. D., and Salihu, S. A. (2021). Application of Internet of Thing and Cyber Physical System in Industry 4.0 Smart Manufacturing. In *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*, pages 203–217. Springer.

Alkadi, O., Moustafa, N., Turnbull, B., and Choo, K.-K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. *IEEE Internet of Things Journal*, 8(12):9463–9472.

Feige, U., Fiat, A., and Shamir, A. (1988). Zero-knowledge proofs of identity. *Journal of cryptology*, 1(2):77–94.

Goldstein, M. (2023). BoNeSi - the DDoS Botnet Simulator. `https://github.com/Markus-Go/bonesi`.

Hara, K. and Shiomoto, K. (2020). Intrusion detection system using semi-supervised learning with adversarial auto-encoder. In *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, pages 1–8.

Heidari, A. and Jabraeil Jamali, M. A. (2022). Internet of things intrusion detection systems: a comprehensive review and future directions. *Cluster Computing*, pages 1–28.

Javadpour, A., Pinto, P., Ja'fari, F., and Zhang, W. (2023). DMAIDPS: a distributed multi-agent intrusion detection and prevention system for cloud IoT environments. *Cluster Computing*, 26(1):367–384.

Kheddar, H., Himeur, Y., and Awad, A. I. (2023). Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review. *Journal of Network and Computer Applications*, 220:103760.

Lilien, L., Kamal, Z., Bhuse, V., Gupta, A., et al. (2006). Opportunistic networks: The concept and research. In *the NSF International Workshop on Research Challenges in Security and Privacy for Mobile and Wireless Networks (WSPWN 2006), Miami, FL, USA*, pages 15–16.

Luo, K. (2023). A distributed SDN-based intrusion detection system for IoT using optimized forests. *Plos one*, 18(8):21.

Mehedi, S. T., Anwar, A., Rahman, Z., Ahmed, K., and Rafiqul, I. (2022). Dependable Intrusion Detection System for IoT: A Deep Transfer Learning-based Approach. *IEEE Transactions on Industrial Informatics*.

Nguyen, G. L., Dumba, B., Ngo, Q.-D., Le, H.-V., and Nguyen, T. N. (2022). A collaborative approach to early detection of IoT Botnet. *Computers & Electrical Engineering*, 97:107525.

Nguyen, T. G., Phan, T. V., Nguyen, B. T., So-In, C., Baig, Z. A., and Sanguanpong, S. (2019). Search: A collaborative and intelligent NIDS architecture for SDN-based cloud IoT networks. *IEEE access*, 7:107678–107694.

Pandey, B. K., Saxena, V., Barve, A., Bhagat, A. K., Devi, R., and Gupta, R. (2023). Evaluation of soft computing in intrusion detection for secure social Internet of Things based on collaborative edge computing. *Soft Computing*, pages 1–11.

Putra, G. D., Dedeoglu, V., Pathak, A., Kanhere, S. S., and Jurdak, R. (2021). Decentralised Trustworthy Collaborative Intrusion Detection System for IoT. In *2021 IEEE International Conference on Blockchain (Blockchain)*, pages 306–313. IEEE.

Quincozes, S. E., Raniery, C., Ceretta Nunes, R., Albuquerque, C., Passos, D., and Mossé, D. (2021). Counselors network for intrusion detection. *International Journal of Network Management*, 31(3):e2111.

Sachdeva, R. and Dev, A. (2021). Review of opportunistic network: Assessing past, present, and future. *International Journal of Communication Systems*, 34(11):e4860.

Sarhan, M., Layeghy, S., Moustafa, N., and Portmann, M. (2023). Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection. *Journal of Network and Systems Management*, 31(1):23.

Spyropoulos, T., Psounis, K., and Raghavendra, C. S. (2004). Single-copy routing in intermittently connected mobile networks. In *2004 IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.*, pages 235–244.

Tanwar, S., Gupta, N., Iwendi, C., Kumar, K., and Alenezi, M. (2022). Next Generation IoT and Blockchain Integration. *Journal of Sensors*, 2022.

Yates, R. D., Sun, Y., Brown, D. R., Kaul, S. K., Modiano, E., and Ulukus, S. (2021). Age of information: An introduction and survey. *IEEE Journal on Selected Areas in Communications*, 39(5):1183–1210.