Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2023.0322000

Reconciling Efficiency and Security of the Internet of Things: A Recursive InterNetwork Architecture (RINA) Approach

PEYMAN TEYMOORI[1,3], TOKTAM RAMEZANIFARKHANI[2,3]
[1]School of Business, University of South-Eastern Norway (e-mail: peyman.teymoori@usn.no)
[2]School of Economics, Innovation and Technology, Kristiania University College, Norway (e-mail: toktam.ramezanifarkhani@kristiania.no)
[3]Department of Informatics, University of Oslo, Norway (e-mail: {peymant | toktamr}@ifi.uio.no)

Corresponding author: Peyman Teymoori (e-mail: peyman.teymoori@usn.no).

.

ABSTRACT The Internet of Things (IoT) has revolutionized our lives by connecting devices to the internet, enabling automation and simplifying daily routines. However, as IoT is built upon the foundation of older network architectures and protocols, such as the Internet, its integration has brought forth significant challenges, particularly in achieving both transport layer efficiency and security at the same time. This paper presents a comprehensive overview of the current network stacks used in IoT and highlights the issues they face in this regard. We propose a novel architectural approach leveraging the Recursive InterNetwork Architecture (RINA) to address these challenges. We thoroughly evaluate how RINA's unique combination of recursion and networking can effectively reconcile the efficiency-security trade-off inherent in IoT networks; this has the potential to overcome the limitations of existing architectures and resolving the long-standing issue with Performance Enhancing Proxies (PEPs) that cannot operate on encrypted connections. We demonstrate the practical application of RINA through two use cases: a smart home environment, where RINA provides a unified networking framework, reducing the complexities of integrating diverse systems, and a healthcare patient monitoring scenario, where RINA ensures seamless integration of legacy devices while maintaining the advantages of the RINA architecture, including security and efficient data transmission. The paper concludes with a comprehensive discussion on potential future research topics, paving the way for an efficient and secure IoT ecosystem.

INDEX TERMS Efficiency, Internet of Things, Multicast, Recursive InterNetwork Architecture, Security.

I. INTRODUCTION

The Internet of Things (IoT) aims to provide a communication network infrastructure with inter-operable protocols and software for physical/virtual sensors, personal computers (PCs), smart devices, automobiles, and other items, such as a refrigerator, dishwasher, microwave oven, food, and medicines, anytime and on any network. Since IoT embraces many different technologies, services, and standards, it is widely perceived as a main pillar of the ICT market in the next ten years [1]. Many new applications such as health-care (e.g. remote patient/elderly people monitoring) and home automation (e.g. heating and lightning control) have been developed so far. This has led to efforts conducted by standardization bodies such as the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF) [2], towards the design of communication and security technologies for the IoT. Given the availability of wireless communication technologies, the number of developed things is expected to rapidly increase: this also raises serious challenges: the network can be easily targeted by attacks and malicious users. What IoT needs is a well-established *efficient* communication platform across different domains, capable of ensuring the *security* of information.

While the Internet has faced and tried to address many similar challenges, the Internet of Things (IoT) continues to grapple with comparable issues. This is primarily due to the unique characteristics and requirements of IoT networks. To enhance the efficiency at the transport layer, several performance enhancement methods have been proposed, such as Performance Enhancing Proxies (PEPs) [3] and Constrained Application Protocol (CoAP) gateways [4].

To tackle the security challenges inherent in IoT, Datagram

Transport Layer Security (DTLS) [5], a protocol based on Transport Layer Security (TLS) but designed to operate on datagrams, has been widely adopted. Many IoT protocols, including Message Queuing Telemetry Transport (MQTT) [6] and CoAP, utilize either TLS or DTLS to ensure secure communication.

However, it is important to note that the addition of security features, particularly at the transport layer, can inversely affect the performance of CoAP proxies. The main reasons include [7]

1) limitations of the DTLS Handshake Protocol with large messages,
2) complications of using DTLS with CoAP, and
3) not supporting multicast communications by DTLS.

In other words, adding (security) functionalities to one layer might interfere proper (and mostly performance) operations at the other layers [8]. The problem worsens when an IoT application is supposed to operate over multiple cross-domain nodes and heterogeneous environments; this is the cause of diversity of protocols and policies and their communication, especially from the security point of view.

To address these challenges, we propose the Recursive InterNetwork Architecture (RINA) as a novel solution. RINA's unique combination of recursion and networking can effectively reconcile the efficiency-security trade-off inherent in IoT networks. By separating security concerns at different layers, embedding security within each layer of the communication stack, and arbitrary stacking these layers, RINA effectively addresses the traditional trade-off between security and efficiency. Our methodology in this paper includes a detailed analysis of current IoT network stacks and their limitations, followed by a theoretical and practical exploration of the benefits of RINA.

RINA was first introduced in [9] and then, implemented and evaluated by a number of international projects. Recursion in RINA is performed by defining a layer as a foundation with basic *mechanisms* to provide Inter Process Communication (IPC) between two IPC Processes (IPCP). This layer is called Distributed IPC Facility (DIF). DIFs (the *mechanisms* inside DIFs) can be customized through adopting different *policies*. Then, DIFs can be recursively arranged to form different topologies [10].

RINA's approach to transport layer security is particularly advantageous. By separating security concerns at different layers, embedding security within each layer of the communication stack, and arbitrary stacking these layers, RINA effectively reconciles the traditional trade-off between security and efficiency. This is also confirmed by RINA's inherent support for secure multicast, a critical feature for IoT networks that is often overlooked in conventional network protocols.

To validate RINA's benefits to IoT, the paper also presents two distinct use cases: a smart home environment and healthcare patient monitoring. The first use case, the smart home, comprises various devices from different vendors, each with its own operational and security requirements.

The second use case focuses on the healthcare sector, where IoT devices have become crucial in patient monitoring and care. In this scenario, wearable IoT devices, which might not inherently support RINA, are incorporated into a RINA network using an IoT sub-manager, a special type of gateway. Our exploration results of these two use cases indicate that RINA has the potential to significantly improve both the efficiency and security of IoT networks.

The primary contributions of this paper are:

- A comprehensive overview of the current network stacks used in IoT and the issues they face.
- Presenting a novel architectural approach that leverages RINA to address significant challenges in IoT, particularly in achieving both transport layer efficiency and security, and offering practical examples of its application through two use cases.
- A comprehensive discussion on potential future research topics, identifying areas where further exploration could yield significant insights.

The remainder of this paper is organized as follows: In Section II, we delve into the current security challenges confronting IoT, particularly within its transport layer, providing a comprehensive overview of the issues at hand. Section III introduces RINA, detailing its transport features and their relevance to IoT. Sections IV and V illustrate how RINA could effectively address these IoT challenges, providing a thorough analysis of its potential benefits.

In Section VI, we explore RINA's unique features that can mitigate the persistent trade-off between efficiency and security in IoT, presenting a compelling argument for its adoption. Section VII presents three distinct use cases where RINA can be effectively employed in IoT environments, offering practical examples of its application. In Section VIII, we discuss potential future research topics, identifying areas where further exploration could yield significant insights. Finally, Section IX summarizes our findings and conclusions, encapsulating the key points of our discussion and highlighting the potential of RINA in the context of IoT.

II. ISSUES OF CURRENT IOT NETWORK STACKS

What IoT needs is an efficient communication platform across different domains, which is capable of ensuring security. We argue that IoT security challenges mostly stem from the architectural design of the IoT network stack. There are mainly two tracks of efforts on improving the security in IoT. One of them utilizes the current Internet design (i.e. TCP/IP) as the base, and the other adopts new frameworks such as Information-Centric Networking (ICN).

A. IP-BASED STACK

As IoT envisions a future Internet in which everyday objects possessing sensing and actuating capabilities cooperate with computer systems, IP-based communication protocols have been aligned with IoT devices to form a communications stack. Fig. 1 illustrates a typical network stack of IoT with

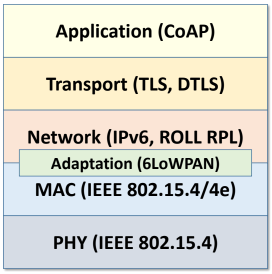


FIGURE 1. A typical IP-based IoT network stack with common protocols.

common protocols in each layer; up to the MAC layer, IEEE 802.15.4 [11] is usually supported; the 6LoWPAN protocol [12] enables the transmission of IPv6 over IEEE 802.15.4; RPL [13] provides routing over 6LoWPAN; TLS [14] and DTLS [5] represent transport layer security using TCP and UDP, respectively; and CoAP [4] provides web transfer at the application layer over UDP (DTLS) with some limited congestion control features. Since we focus on the network stack of IoT devices, we do not discuss *perception* (to perceive the environment with technologies such as RFIS and GPS) which is usually categorized as a layer.

A typical network stack of IoT with common protocols in each layer resembles the TCP/IP stack with some commonalities, especially in the design. However, the large-scale deployment of IP-based IoT solutions is still challenging [15].

In [16], it has shown that IoT security challenges of IP-based IoT frameworks mostly stem from the architectural design of the IoT network stack. In addition, comprehensive studies such as [17] on IoT security have confirmed that many issues stem from the currently-employed network stack protocols of IoT devices and their interoperability issues with the Internet. There are some major flaws with IP: the concept of scope of a layer is not used correctly [18], as it has been diluted by gradual updates. Although some research work (e.g. [19]) focused on presenting a secure IoT architecture, it usually operates at higher layers regardless of what the network stack is. On the contrary, in this paper, we fundamentally look at the lower layers, and especially the network stack and its protocols.

At the transport/application layer, DTLS, as the common protocol, have been in use to ensure end-to-end security using CoAP. As its limitations were mentioned by [7], [8], DTLS does not support multicast communication which is highly required in IoT networks. Due to its end-to-end security, DTLS also complicates operations of CoAP proxies in the path. This problem has led to securing CoAP communications and object security rather than the transport security provided by DTLS. However, this approach is not mature yet. Although most of these issues have been found and tried to be addressed before in the Internet, however, IoT still faces almost the same issues.

B. ICN-BASED STACK

Contrary to IP networks, Information-Centric Networking (ICN) adopts a unique approach by assigning distinct identifiers to content, independent of its originating location or application. This approach facilitates in-network caching/replication and content-based security [15]. Although the original architects of ICN did not specifically design it with IoT in mind, ICN has been repurposed and adapted to cater to the unique requirements of IoT.

However, the multifaceted and complex nature of IoT demands presents unique challenges to the design and implementation of ICN [15]. Even with ongoing standardization efforts for ICN-IoT deployments within the ICN Research Group (ICNRG) [20], there exists a considerable debate within the ICN community. The concerns center around potential security and performance issues that ICN could encounter in the IoT context [15], [21].

This is primarily due to the fact that ICN-IoT not only connects a significantly higher number of devices compared to most other networks, but it also assigns unique names to the content generated by these devices. This combination of vast connectivity and content-specific naming imposes considerable challenges in terms of managing security protocols and optimizing performance in an IoT environment.

C. SUMMARY OF IOT NETWORKING CHALLENGES

Although there has been much research work on securing IoT, there are still open issues regarding the layers, protocols, and their vulnerabilities; these issues are thoroughly discussed by [8], [17].

We argue that IoT security challenges mostly stem from the architectural design of IoT. The challenges are as follow[1]:

1) IoT Network Stack Challenges

Despite the lessons learned from the Internet, the IoT network stack has similar security issues. Referring to Fig. 1, the 6LoWPAN protocol does not define any security mechanism, but it makes the use of IPsec available to provide security between two communication end points. However, no specific method has been adopted yet for 6LoWPAN [8]. Since the 6LoWPAN Border Router typically does not perform any authentication, IoT networks are still vulnerable [17]. Moreover, encryption at the routing layer hides all the necessary information of the upper layers; this is one of the main problems that Performance Enhancing Proxies (PEPs) [3] are facing in wireless networks because they cannot break the end-to-end congestion control loop to start a new one matching the environment properties (e.g. wired, wireless) [22]. Although there have been proposals on smart gateways (e.g. [23], [24]) to connect *things* to the Internet, the same problem still exists [8].

At the routing layer, RPL [25] is commonly used, which does not define how to protect RPL communications and

[1] These challenges were originally published in [16] in a much shorter form.

operations from internal attackers, and it also lacks some key security features [8].

At the transport/application layer, DTLS, as the common protocol, have been in use to ensure end-to-end security using CoAP. As its limitations were mentioned by [8], DTLS does not support multicast communication which is highly required in IoT networks. Due to its end-to-end security, DTLS also complicates operations of CoAP proxies in the path. This problem has led to securing CoAP communications and object security rather than the transport security provided by DTLS. However, this approach is not mature yet.

2) Repeated Functionality in Layers/Protocols

As observed, similar security functionalities are often redundantly implemented across different layers within multiple protocols. This repetition not only reflects an inefficient use of resources but also an unnecessary complexity that contradicts the principle of ‘‘no need to reinvent the wheel’’ across several layers.

Each time a function is reimplemented, there’s a risk of introducing new vulnerabilities into the system. This is particularly relevant in the context of security functions, where a minor oversight can result in significant security breaches. Furthermore, the multiplication of similar functions in different layers often complicates the process of patching and updating security protocols, thereby increasing the system’s vulnerability to threats over time.

Moreover, this redundancy impedes the degree of reusability for future extensions. A more modular design, where functions are implemented as independent, reusable modules, could significantly enhance the scalability and adaptability of the system. This modularity not only allows for more efficient resource utilization but also enables faster development and deployment of new functionalities.

3) Global, Public, and Large Address Space

Given the overwhelming number of IoT devices, or ‘‘things’’, IPv6 was adopted to cater to the expansive address space requirement. However, the implementation of IPv6 introduces its own set of challenges, one of the most significant being the management of large, public addresses [26].

In an IPv6 environment, every IoT device requires a unique, globally addressable IP, which inherently increases the exposure and vulnerability of these devices. This high visibility leads to heightened security risks as potential attackers can easily identify and target specific devices. While providing each device with a unique, publicly accessible address facilitates communication, it simultaneously unveils a plethora of devices to potential cyber threats.

Furthermore, the adoption of IPv6 addresses presents practical difficulties due to their large size. Managing and maintaining such an extensive addressing space necessitates robust and efficient networking infrastructure, which can be resource-intensive and challenging to implement, particularly on a global scale.

Moreover, the current approach of exposing every device to the widest scope – the Internet – isn’t always necessary or ideal. Not every IoT device needs to be globally addressable; many can function effectively within local or private networks. Employing a more nuanced, scope-dependent addressing strategy can significantly mitigate the security risks associated with global, public addressing.

4) Security and Performance Enhancement Conflict

Performance enhancement techniques, such as Performance Enhancing Proxies (PEPs) and gateways, play a critical role in ensuring the smooth functioning of IoT networks. However, these techniques often encounter an inverse relationship with the implementation of security measures, particularly at the transport layer [10], [27].

The deployment of security features at one layer can disrupt the operations at other layers or devices on the path towards the destination. An example can be observed in the context of Transport Layer Security (TLS), where encryption at the transport layer can potentially interfere with the efficiency-enhancing operations of PEPs. This issue arises because the encrypted data packets are opaque to the PEPs, preventing them from performing their intended optimization tasks, such as protocol-specific acceleration [8].

5) Attack Repetition

The current landscape of IoT security functionalities presents a recurring and escalating issue: the reemergence of historical attacks in stronger forms. IoT protocols, despite their advancements, still reveal significant vulnerabilities, necessitating ongoing extensions and enhancements for effective security [17].

The rise of Distributed Denial of Service (DDoS) attacks exemplifies this cycle of attack repetition. As IoT devices increase, they form a vast landscape of potential targets, and unfortunately, unwitting participants in botnet activities. DDoS attacks traditionally overwhelm target systems with an excessive volume of requests, rendering them unable to provide services to legitimate users. In the context of IoT, these attacks have found a renewed form, leveraging the ubiquitous presence and often not enough security of IoT devices to build extensive botnets, amplifying the scale and impact of these attacks.

However, DDoS attacks are just one facet of the problem. The pervasive issue of attack repetition also extends to other forms of security threats, such as eavesdropping, man-in-the-middle attacks, and device spoofing. These age-old attack methodologies are constantly being rehashed, tailored, and optimized to exploit the unique vulnerabilities of IoT environments.

6) Future Extensions

The future of IoT promises an expansion of capabilities and functionalities, as well as a broadening of application domains. However, these advancements also imply potential security challenges that need to be thoroughly addressed.

While significant strides have been made in securing individual protocols or layers within the IoT architecture, this does not automatically translate into comprehensive security coverage, especially considering interlayer compatibility and future extensions [28] [1].

Consider, for instance, the increasing prevalence of mobile devices within the IoT ecosystem. The unique characteristics of these devices—such as their portability, variable connectivity, and resource constraints—pose novel security challenges that are yet to be comprehensively addressed. Moreover, the rise of 5G/6G and beyond technologies, with their emphasis on high-speed, low-latency communication, will only accentuate these concerns.

Future extensions of IoT technologies, such as mobility, multicast, and Quality of Service (QoS), further complicate this security landscape. Mobility brings about dynamic changes in network topology and demands secure, seamless handovers. Multicast communication, on the other hand, requires the secure distribution of data to multiple recipients, a task that becomes increasingly complex as the size and diversity of IoT networks grow. Finally, QoS, which is critical in time-sensitive applications such as autonomous vehicles and telemedicine, demands that security measures do not impede the timely delivery of data.

7) Cross-Domain Synergy

IoT applications are increasingly spanning across diverse domains, each with their unique requirements, protocols, and security policies [29]. This cross-domain nature of IoT applications and the ensuing heterogeneity in the environment poses significant challenges, especially from a security perspective.

Consider the scenario where an IoT network is composed of devices from healthcare, industrial automation, smart home, and automotive sectors. Each of these domains has its unique protocols, data formats, and security requirements. For instance, healthcare devices require strict adherence to privacy regulations, while industrial IoT may prioritize integrity and availability. Smart home devices might need to balance user convenience with security, and automotive IoT demands real-time guarantees to ensure safety. Thus, harmonizing these disparate needs is a nontrivial task.

Cross-domain communication further compounds this issue. When devices from different domains need to interact, they must do so through a common set of protocols and policies. However, designing such universal protocols is challenging due to the need to cater to diverse requirements. Moreover, these protocols should also be robust against potential security threats, as an adversary could exploit the weakest link in the cross-domain communication chain to compromise the entire network.

Beyond the technical issues, there is also the challenge of policy harmonization [30]. Different domains often operate under different regulatory frameworks, and reconciling these could be a significant hurdle. For instance, data privacy regulations could vary drastically between healthcare and consumer electronics domains.

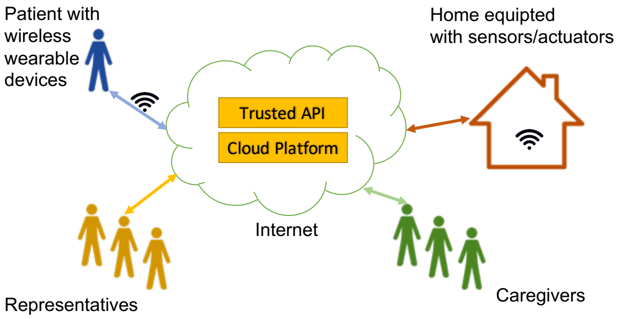

Patient with wireless wearable devices
Home equipted with sensors/actuators
Trusted API
Cloud Platform
Internet
Representatives
Caregivers

FIGURE 2. An example of domain synergy for two different IoT domains: health and home.

D. CHALLENGES OF BEING BOTH EFFICIENT AND SECURE

As we examine the complexities of IoT architectures, an inherent trade-off between transport layer efficiency and security in IoT becomes apparent, particularly within the previously discussed network stacks. To elucidate this issue, let's take the case of interconnected IoT applications in the realms of home monitoring and e-health, as depicted in Fig. 2.

These applications are designed with the objective of patient or elderly health monitoring within a residential setting, with the potential for emergency intervention [31]. Trust levels and privacy requirements vary significantly across the spectrum of interactions – between the patient or elderly monitoring IoT devices, the healthcare center, and the home monitoring system. For example, in emergency situations, caregivers should be granted access to the home, yet the trust dynamics within and between the home monitoring and e-health systems are contingent upon various factors, often transient in nature.

Further complications arise when considering that IoT devices often require the support of CoAP proxies to interface with the IoT cloud and other systems via an HTTP-like protocol. These proxies may need to break an end-to-end connection or even translate the protocol to a different one at the cloud side to optimize resource utilization. This dichotomy – ensuring efficient communication while maintaining stringent security – poses significant challenges.

The problem is accentuated by the essential requirement for multicast protocols in IoT. While there have been proposals specifically addressing multicast in IoT, such as the work in [32], the current landscape lacks the ability to secure multicast through DTLS [7]. This gap further emphasizes the challenges in securing communications in the IoT while maintaining efficient performance.

Having discussed the challenges of current IoT network stacks, we now introduce the Recursive InterNetwork Architecture (RINA) as a potential solution to these issues.

III. RECURSIVE INTERNETWORK ARCHITECTURE (RINA)

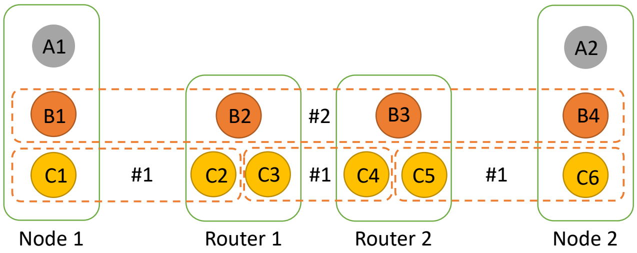


FIGURE 3. A sample network topology represented by DIFs.

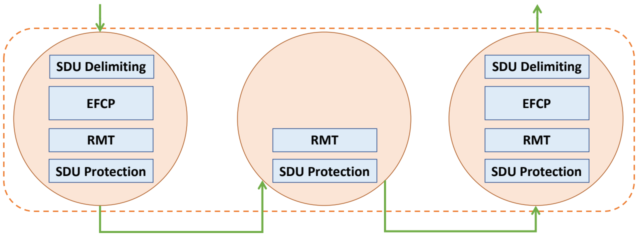


FIGURE 4. Data transfer modules of three IPCPs inside one DIF.

A. INTRODUCTION

The Recursive InterNetwork Architecture (RINA), presented by John Day in "Patterns in Network Architecture: A return to Fundamentals" [9], is a novel approach in networking architecture trying to avoid architectural problems of TCP/IP and other technologies. Through evaluating it in different use cases (e.g. see (e.g. [10], [18], [33]–[36])), this is shown that RINA can provide significant benefits to networking by removing architectural obstacles[2] [3].

As shown in Fig. 3, RINA is based on a single type of layer (represented by dashed boxes in the figure), which is repeated as many times as required by the network designer. The layer is called a Distributed IPC Facility (DIF), which is a distributed application that provides IPC services over a given scope to the distributed applications above (which can be other DIFs or regular applications). These IPC services are defined by the DIF API. All DIFs offer the same services through their API and have the same components and structure. However, not all the DIFs operate over the same scope and environment nor do they have to provide the same level of services.

In Fig. 3, there are four devices: Node 1 and Node 2 are two end-hosts that are connected via two routers. A1 and A2 are two application processes willing to communicate, and the circles in the DIFs are called IPC Processes (IPCPs). IPCPs have the same structure that can join DIFs. DIF #2 spans the whole network, allowing packets to be routed and congestion-controlled from A1 to A2 via routers. There are also three DIFs #1 (could be assumed as the link layer) connecting devices together (doing mostly flow control). However, the structure of the DIFs are the same, and just the scope of the DIFs is different. This solves the problem of inventing new layers (as those presented by MPLS, VLAN, tunneling, etc.) and their deployment; the same layer can be customized via policies and instantiated to operate over different scopes.

In RINA, a Distributed Application is a set of two or more Application Processes (APs) that cooperate to do some function. The set of these APs is called a Distributed Application Facility (DAF). DAFs use DIFs when IPC between the APs in DAF is not possible via shared memory.

In RINA, invariant parts (*mechanisms*) and variant parts (*policies*) are separated in different components of the architecture. This makes it possible to customize the behavior of a DIF to optimally operate in a certain environment with a set of policies for that environment instead of the traditional "one size fits all" approach or having to re-implement mechanisms over and over again.

Fig. 4 illustrates the data transfer modules inside IPCPs in a DIF. These modules show in each DIF, there is one (EFCP) sender and one (EFPC) receiver. The IPCP in the middle routes Protocol Data Units (PDUs) received from the left IPCP to the right one via its corresponding port. This scheme repeats at different DIFs, with the difference that it could be longer or as short as a point-to-point link without the routing IPCP. In [10], we evaluated the performance of a recursion of two layers of congestion controllers using a TCP Reno-like controller; we showed that the recursion can improve throughput while decreasing queuing delay compared to an end-to-end TCP Reno and Split TCP (or PEP), where a connection is broken at routers.

The main difference between RINA and other stacks is that RINA recurses the same layer, called DIF numbered from 1 (e.g. 1-DIF, 2-DIF) as the lowest one, and (N)-DIF as the current one we are focusing on. At the lowest layer, *shim* DIF operates over the physical layer, but it has the deployment possibility of operating on other protocols such as UDP.

B. IPCP'S MECHANISMS

A node joins a DIF through an IPC Process (IPCP), which is an instance of the same code handling IPC. IPCPs have the same structure consisting of the following mechanisms that operate at different timescales (ordered from faster to slower):

1) Data Transfer

This is the most fundamental mechanism of the IPCP, and it is responsible for the actual movement of data. It involves a series of functions:

- *Delimiting*: This function encodes Service Data Units (SDUs) that arrive from the upper DIF within Protocol Data Units (PDUs).
- *Error and Flow-Control Protocol (EFCP)*: This protocol ensures reliable data transmission using its two sub-protocols: Data Transfer Protocol (DTP) and Data Transfer Control Protocol (DTCP). DTP primarily concerns with the transmission and segmentation of data, while

[2] See [37] for a list of publications on RINA.

[3] A comprehensive yet easy-to-read text on RINA can be found in [38]

DTCP provides additional control functions, such as congestion control and error checking.

- *Relaying and Multiplexing Task (RMT)*: This task performs routing of PDUs to output ports of the DIF or upwards. It utilizes the routing information provided by the layer management to determine the optimal path for data transmission.
- *SDU Protection*: This mechanism performs encryption, compression, error-code calculation, and Time-To-Live (TTL) setting.

2) Data Transfer Control

This mechanism supervises the data transmission process to ensure it runs smoothly and effectively. It includes several sub-components:

- *Error Control*: This component keeps track of any errors that may occur during data transmission. It uses a variety of error detection and correction techniques to maintain data integrity throughout the transmission process.
- *Flow Control*: This component manages the rate of data transmission ensuring that the receiver is not overwhelmed with data and can process incoming data effectively.
- *Retransmission Control*: This component monitors for lost or corrupted data packets. In the event of packet loss or corruption, it initiates a retransmission request, ensuring reliable data delivery.
- *Congestion Control*: This component monitors network congestion and implements measures to alleviate it. This can include reducing the data transmission rate.

3) Layer Management

The layer management mechanism includes a variety of functions:

- *Resource Allocation:* The Resource Allocator (RA) manages resource allocation and monitors the resources in the DIF by sharing information with other DIF IPC Processes and the performance of supporting DIFs.
- *Routing:* Routing performs the analysis of the information maintained by the RIB to provide connectivity input to the creation of a forwarding function. The choice of routing algorithms in a particular DIF is a matter of policy.
- *Security Coordination:* Security coordination is responsible for implementing a consistent security profile for the IPC Process, coordinating all the security-related functions (authentication, access control, confidentiality, integrity) and also executing some of them (auditing, credential management).
- *Namespace Management:* The Name Space Manager (NSM) embedded in the DIF is responsible for mapping application names to IPC Process addresses. The NSM maintains a mapping between external application names and IPC Process addresses where there is the potential for a binding within the same processing system.
- *Flow Allocation:* The Flow Allocator is responsible for creating and managing an instance of IPC, i.e., a flow. The Flow Allocator-Instance (FAI) determines what policies will be utilized to provide the characteristics requested in the Allocate.
- *Enrollment:* The Enrollment process involves a new member joining the DIF. This process includes address assignment, information exchange about operational parameters, and updating the RIB with the latest information on routing, directory, resource allocation, etc. The new member then becomes a full member of the DIF.

C. ERROR AND FLOW-CONTROL PROTOCOL (EFCP)

EFCP is the only data transfer protocol in RINA, which is based on Richard Watson's fundamental results on synchronization for reliable data transfer [39]. Its main functions are sequencing, flow control, and retransmission control. EFCP provides an inter-process communication service to upper processes that might be an (N+1)-IPCP or and application process. The upper process is connected to (can write to/read from) the EFCP in the (N)-DIF via the (N)-port-id.

EFCP has two logical components operating at different time scales: 1) Data Transfer Protocol (DTP) that is the mandatory part of EFCP and includes tightly bound mechanisms, and 2) Data Transfer Control Protocol (DTCP), which include loosely bound mechanisms. DTP is instantiated every time a flow is created. It is roughly similar to the UDP protocol. However, depending on the QoS requirements, DTCP might be also instantiated to provide retransmission and flow control.

Watson's result imply that the necessary and sufficient condition for synchronization to have a reliable data transfer is to set an upper bound on only these times: Maximum Packet Lifetime (MPL), maximum time to wait before sending an Ack, A, and the maximum time to exhaust retries, R [39]. This decouples port allocation and synchronization.

EFCP can be customized via several policies. A simple example is that the behavior of different TCP flavors can be imitated by writing different policies. The mechanisms operating on PDUs and policies are the same.

As shown in Fig. 5 , when a PDU is written to an (N)-port-id, the delimiting module, associated to the port, processes the PDU by possible fragmentation or concatenation. The result is passed to the EFCP instance associated to that port. As a result, generated PDUs are passed to the RMT for multiplexing. The RMT sends PDUs to one or more (N-1) ports. When the RMT reads a PDU from an (N-1)-port, if the PDU's destination address is not in another node, it passes the PDU to the relevant EFCP instance for further processing. EFCP instances of (N)-DIF are managed by the module Flow Allocator (FA) in that DIF. FA can create a new EFCP instance, replace an old instance by a new one, or delete the instances.

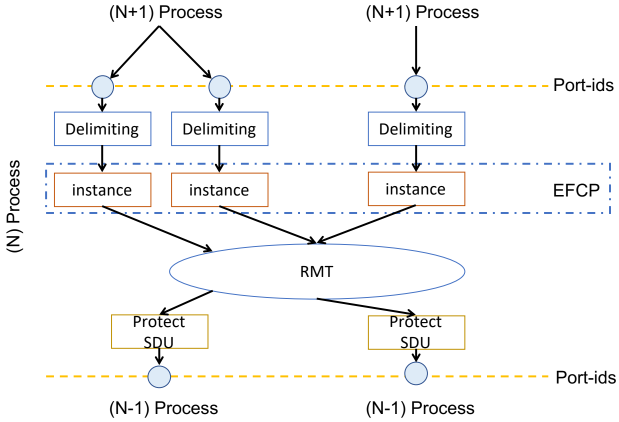


FIGURE 5. A sample of data transfer modules. Some (N+1) IPCPs are connected to an N-DIF, which is connected to some (N-1)-DIFs.

IV. RINA'S TRANSPORT SECURITY FEATURES

How RINA connects IPCPs and how their EFCP is connected to each other in different DIFs can provide other benefits than just performance. A complete evaluation is found in [16], [36]. Here, we summarize the security features related to EFCP:

A. SECURE DIFS

"DIF is a securable container" [33]. This is the main feature that RINA secures layers instead of protocols. This means that all the packets leaving an (N)-DIF are protected via the SDU Protection module. Hence, IPCPs in (N-1)-DIF cannot inspect the arriving packet, and this can continue downwards in lower DIFs, which also depends on the policy of those DIFs. However, every IPCP in the same DIF can inspect the packet, and in case of performing enhancements or protocol conversion in CoAP proxies, packets are not obscured. This also implies that in RINA, IPCPs should be enrolled first before joining a DIF, and their access rights are validated. This also implies that an outsider cannot attack the DIF. In case an attacker can compromise the enrollment or if the DIF communication is not encrypted, RINA's typical field lengths in packets are still long enough to make attacks harder to succeed, e.g. 2^{48} possibilities to guess the connection information in RINA compared with 2^{29} possibilities in TCP during data transfer [33].

B. HIDDEN ADDRESSES

RINA introduces a unique addressing scheme where IPCPs in each DIF have their own addresses. Unlike the traditional IP addressing system, where IP addresses are globally visible and can be targeted by malicious actors, in RINA, the addresses are confined to their respective DIFs and are not publicly visible.

This "hidden address" feature effectively mitigates a major security concern in traditional IP-based networks, where IP addresses are publicly accessible without any form of authentication. Publicly visible IP addresses expose the network to a variety of threats, such as Denial of Service (DoS) attacks, IP spoofing, and other forms of unauthorized access or data interception.

In an IoT context, where networks are typically composed of a large number of interconnected devices with varying levels of security capabilities, this feature of hidden addresses can offer substantial security benefits:

- *Enhanced Privacy*: By keeping the addresses hidden within each DIF, RINA effectively reduces the attack surface, making it more difficult for malicious actors to target specific devices within the network.
- *Scalability*: The RINA recursive nature allows for highly scalable networks without compromising security, essential for large-scale IoT deployments.

C. SYNCHRONIZATION-INDEPENDENT PORT ALLOCATION

In TCP, synchronization and port allocation processes are coupled. A potential vulnerability arises from this coupling because it becomes easier for an attacker to predict or ascertain a connection's state and launch attacks, such as SYN flood attacks, which are a type of Denial of Service (DoS) attack.

However, RINA introduces a novel design where synchronization and port allocation are decoupled, which significantly enhances the security posture of IoT networks. This decoupling makes it more difficult for attackers to predict or understand the state of a connection, hence reducing the chances of intercepting a connection or launching successful attacks.

D. PORT-INDEPENDENT COMMUNICATION

In most traditional network architectures, including the Internet Protocol (IP) suite, services are associated with well-known ports. For example, web servers typically listen on port 80 for HTTP and port 443 for HTTPS. These well-known ports can be targeted by attackers, who scan them for vulnerabilities or attempt to overwhelm them with traffic in Denial-of-Service (DoS) attacks.

However, RINA adopts a fundamentally different approach. Instead of relying on well-known ports, applications request services through their application names. This means there are no standard ports for attackers to listen to or target, significantly reducing the attack surface [36].

E. SOFT-STATE CONNECTION MANAGEMENT

In RINA, the management of connections is handled differently from traditional network architectures. RINA adopts Watson's method for managing connections in a soft-state manner. This means that instead of using explicit control messages to establish or close a connection, RINA relies on timers. After a period of time equal to twice the Maximum Packet Lifetime (2∗MPL), the receiver deletes the connection state. This unique feature of RINA offers several significant security benefits for IoT networks:

- *Reduction of Connection Misuse*: With the absence of explicit control messages for connection establishment and termination, the risk of connection misuse is significantly reduced. Misuse can occur when malicious actors manipulate control messages to illegitimately establish, hijack, or disrupt connections. By eliminating these messages, RINA reduces the opportunities for such attacks [33].

- *Mitigation of Denial of Service (DoS) Attacks*: Many DoS attacks, such as SYN flood attacks, exploit the control messages used to establish connections in traditional network architectures. RINA's soft-state connection management approach effectively mitigates this type of attack by eliminating the targeted control messages.
- *Improved Resource Management*: By automatically deleting connection states after 2∗MPL, RINA ensures efficient use of resources. This feature is particularly important in IoT networks, where devices often have limited computational resources. Efficient resource management also reduces the risk of resource exhaustion attacks.
- *Enhanced Privacy*: By not maintaining long-lived connection states, RINA also improves privacy. In traditional networks, persistent connection states could potentially be used to track and monitor user activities. In RINA, the transient nature of connection states makes such tracking more difficult.

F. CONNECTION MANAGEMENT INDEPENDENT AUTHENTICATION

RINA implements a unique architectural design where the authentication process is separate from connection management. Instead of performing authentication during connection establishment as in traditional network architectures, IPCPs in RINA are authenticated when they first enroll in a DIF.

This decoupling of authentication from connection management brings about several significant security benefits for IoT networks:

- *Enhanced Security*: By performing authentication at the enrollment stage, RINA ensures that only authenticated IPCPs can participate in the network. This measure significantly reduces the risk of unauthorized access or impersonation attacks.
- *Minimized Attack Surface*: Traditional network architectures often couple authentication with connection management, which can expose them to a variety of attacks such as man-in-the-middle (MitM) attacks. By decoupling these processes, RINA minimizes the attack surface and makes it harder for attackers to exploit the connection management process.
- *Robust Access Control*: With the separation of authentication from connection management, RINA can implement more robust access control mechanisms. This allows for more granular control over who can access what in the network, which is critical in IoT environments where devices with varying security capabilities are interconnected.
- *Efficient Resource Management*: By handling authentication during enrollment, RINA can also prevent resource exhaustion attacks aimed at overwhelming the authentication process during connection establishment.

G. VARIABLE ADDRESS SPACE

In traditional network architectures, addresses are usually fixed in size. For instance, IPv4 addresses are always 32 bits, and IPv6 addresses are 128 bits. These fixed-sized addresses can be predictable and therefore potentially exploitable by attackers.

RINA, on the other hand, introduces the concept of variable address space. The size of addresses in a DIF can vary, and it depends on the number of nodes in that DIF. This approach not only saves space in the packet header but also introduces a significant layer of unpredictability, making it harder for attackers to predict or manipulate addresses.

Here are some of the security benefits provided by the variable address space feature in RINA:

- *Enhanced Unpredictability*: The variability in address size makes it difficult for attackers to predict the address space, thereby making address-based attacks such as IP spoofing and reconnaissance more difficult.
- *Increased Difficulty for Eavesdroppers*: The variability in address size also makes it harder for eavesdroppers to understand the network's structure or to track specific devices, thus enhancing the privacy of the network.
- *Efficient Use of Address Space*: By adjusting the address size according to the number of nodes in a DIF, RINA ensures efficient use of the address space. This is particularly beneficial in IoT networks, where the number of devices can vary significantly.
- *Improved Scalability*: The ability to vary address size provides RINA with superior scalability, ensuring that the network can effectively support both small-scale and large-scale IoT deployments.

V. OTHER PERFORMANCE/SECURITY FEATURES OF RINA

A. RINA'S DAFS

In RINA, the application-layer component is encapsulated in what is known as the Distributed Application Facility (DAF). The DAF is responsible for providing services to applications and managing application-level communication. From a security standpoint, the DAF in RINA embodies the principle of end-to-end security. Unlike other networking architectures where security is often implemented as an afterthought, RINA incorporates security as an integral part of the DAF design. This means that applications using a DAF can rely on a built-in security model that protects their communication from eavesdropping, tampering, or message forgery.

When a DAF encrypts all communication, it indeed provides a robust layer of security for the application data, essentially rendering the information within the DIFs secure. This approach aligns with the principle of data protection at rest and in transit, one of the cornerstones of information security [40]. However, it's essential to understand that within a RINA network, each DIF still plays a crucial role in maintaining the overall system's security. For instance, the top DIF might employ Payment Card Industry (PCI) encryption [41] to prevent traffic analysis, a form of network surveillance that threatens privacy. This layer-specific encryption is a proactive measure to counteract any potential security breaches.

It can be argued that that link-layer encryption becomes redundant in this context, as it introduces an overhead of encrypting and decrypting at every hop, especially when the addresses used at this layer are not usually of interest to potential attackers.

B. RINA'S CDAP

RINA's architectural design emphasizes the importance of a unified application protocol and the flexibility of object models. One of the significant advantages of RINA is its Common Distributed Application Protocol (CDAP). It provides the necessary framework for creating a wide range of distributed applications, with the DIF being a notable instance of such an application.

Unlike the traditional approach of having different application protocols, which often results in protocol inconsistencies, RINA's CDAP establishes a common language for all applications, simplifying communication across varied applications.

The CDAP's generic nature provides a platform for diverse applications to exchange information using a unified protocol. This consistency removes the need for multiple application-specific protocols, such as the Constrained Application Protocol (CoAP), thereby reducing the complexity and overhead associated with maintaining numerous protocols. The elimination of CoAPs altogether aids in streamlining the intercommunication between IoT devices and servers, enhancing both the efficiency and reliability of data exchange.

C. MULTI-LAYER SECURITY

RINA embraces the "Divide and Conquer" principle by using DIFs and recursion. Instead of trying to secure a broad scope, such as an entire IoT network at once (which could be as vast as the Internet), security is enforced within smaller, more manageable scopes defined by DIFs.

This approach yields several significant advantages:

- *Containment of Attacks*: By dividing the network into smaller scopes (DIFs), the impact of a compromise can be contained within a single DIF. This means that even if some DIFs are compromised, the integrity of the whole network remains intact. This is a critical benefit in IoT networks where a vast number of diverse devices, each with their own potential vulnerabilities, are interconnected [18].
- *Enhanced Scalability*: The recursive nature of DIFs means that the same security mechanisms can be applied at different scales, from small local networks to large-scale global networks. This scalability is crucial for IoT networks, which can range from a few devices in a home network to millions of devices in a city-wide infrastructure.
- *Improved Manageability*: Securing smaller scopes (DIFs) is more manageable than securing a wide network as a whole. This allows for more targeted security measures and makes it easier to monitor and respond to security incidents.
- *Tailored Security Policies*: Each DIF can have its own security policies tailored to the specific needs and characteristics of the devices within it. This allows for a more fine-grained and effective approach to security compared to one-size-fits-all policies.

D. COMMUNICATION VIA A COMMON DIF

In RINA, two applications can only communicate if they share a DIF. If they do not have a DIF in common, they must either join an existing common DIF or create a new one. This is a departure from traditional Internet protocols, where any two nodes with Internet connectivity can attempt to communicate.

This feature offers several significant advantages for IoT network security:

- *Restriction of Unwanted Communication*: By requiring a common DIF for communication, RINA effectively restricts the ability of arbitrary nodes to communicate with each other. This can significantly reduce the risk of unwanted communication, such as those originating from malicious actors or compromised devices.
- *Enhanced Access Control*: The requirement of a common DIF also provides a mechanism for fine-grained access control. Only devices that are part of a given DIF can communicate, enabling network administrators to effectively control which devices can interact with each other.
- *Reduced Attack Surface*: By limiting communication to devices within a common DIF, RINA effectively reduces the attack surface of an IoT network. Attackers cannot directly reach devices outside of their DIF, which can help protect vulnerable devices from attacks.
- *Improved Privacy*: Since a device can only communicate with other devices within its DIF, the visibility of device communication is limited. This can help enhance the privacy of device interactions within an IoT network.

E. AUTHENTICATION

In RINA, every IPCP must be authenticated before joining a DIF. This authentication is performed during the enrollment process, prior to connection management. Notably, the enrollment process also includes access control measures.

These security mechanisms have several significant implications for IoT network security:

- *Enhanced Access Control*: Requiring IPCP authentication before joining a DIF ensures that only trusted entities can become part of the network. This measure effectively prevents unauthorized entities from joining the network, thereby reducing the risk of insider threats and unauthorized access.

- *Mitigation of Address Spoofing Attacks*: Since attackers must join a DIF (which requires authentication) to address IPCPs within that DIF, RINA's architecture inherently mitigates the risk of address spoofing attacks.
- *Improved Network Integrity*: By enforcing authentication and access control during the enrollment process, RINA enhances the overall integrity of the network.
- *Prevention of Unauthorized Data Access*: With strict authentication and access control, unauthorized entities are prevented from accessing or manipulating sensitive data within the network. This is crucial in IoT networks, where vast amounts of potentially sensitive data are regularly transmitted.

F. BUILT-IN FIREWALL

In RINA, every router inherently serves as a firewall. This is due to the security modules present within each IPCP. These security modules can provide firewall functionalities, thus enhancing the security of data transiting through the network.

This feature offers several significant advantages for IoT network security:

- *Enhanced Network Security*: The inherent firewall functionality in each router allows for enhanced protection against various network attacks. This includes protection against unauthorized access, data breaches, and various forms of cyber threats.
- *Simplified Network Architecture*: RINA simplifies the network architecture by having only three types of nodes: *end-nodes*, *border routers*, and *interior routers*. This streamlined architecture simplifies the implementation of security policies and reduces the potential attack surface.
- *Distributed Security*: Rather than relying on a centralized security solution, RINA's approach distributes security functionalities across all routers in the network. This can help to prevent single points of failure and distribute the load of handling security functions.
- *Granular Security Control*: The presence of security modules within each IPCP enables granular control over security policies. This means that different routers can implement different levels of firewall protection based on the specific needs and risk levels of their respective network segments.

G. PROGRAMMABLE DIFS

RINA enables DIFs to be programmable. This means that any new functionality, including those addressing security, privacy, or performance issues, can be developed as a policy and plugged into the existing mechanisms.

The implications of programmable DIFs for IoT network security are substantial:

- *Flexibility in Security Policy Implementation*: By allowing new functionalities to be developed as policies, RINA offers a high degree of flexibility in implementing and updating security measures. This can be especially beneficial in the rapidly evolving landscape of IoT security, where new threats and vulnerabilities often emerge [42].
- *Reduction of Functional Redundancies*: The ability to plug in policies into existing mechanisms can help reduce functional redundancies in protocols. This not only streamlines the network's operation but also eliminates potential security loopholes that might arise from redundant functionalities [43].
- *Mitigation of New Vulnerabilities*: By reducing the effort required to implement new functionalities, RINA lowers the risk of introducing new vulnerabilities during the implementation process. This is crucial because even minor errors in implementing security measures can lead to significant vulnerabilities.
- *Adaptable Security Measures*: The programmable nature of DIFs in RINA allows the security measures to be readily adaptable to the specific needs and threat landscape of an IoT network. This means that the security measures can be rapidly adjusted in response to evolving threats and vulnerabilities.

H. ACCESS CONTROL

In RINA, access control is enforced by the Access Control module within the IPCP, using CDAP as the signaling protocol. This mechanism determines whether a requesting entity is permitted to access a given resource.

The implications of RINA's access control mechanism for IoT network security are considerable:

- *Authorization*: By using the Access Control module, RINA ensures that every entity requesting access to a resource must be authorized. This adds an extra layer of protection, effectively reducing the risk of unauthorized access to network resources.
- *Fine-Grained Access Control*: Given that the access control is enforced at the IPCP level, this allows for fine-grained access control. Different resources can have different access control policies, thus providing a high level of granularity in controlling access to network resources.
- *Protection Against Insider Threats*: As the access control is enforced for each resource access request, this can effectively mitigate the risk of insider threats. Even if an entity is authenticated, it must still be authorized to access a resource, preventing misuse of access privileges.
- *Robust Signaling Protocol*: The use of CDAP as the signaling protocol for access control further enhances the security of the mechanism. CDAP is a robust protocol that has built-in measures to ensure the integrity and authenticity of signaling messages, thus improving the overall security of the access control mechanism.

I. INSIDERS RESISTANCE

RINA adopts a wider range of control field values, for instance, in connection and Quality of Service (QoS) identifiers. This strategy is specifically designed to resist insider threats, those threats posed by entities that have already gained access to the network or have somehow bypassed the authentication process, even in scenarios where cryptographic support might be absent.

The implications of RINA's insiders resistance for IoT network security are as follows:

- *Enhanced Security Through Larger Field Lengths*: The typical field lengths in RINA packets are longer than those in traditional IP-based protocols like TCP. This increases the complexity and computational effort required for an attacker to guess the correct values [36].
- *Increased Difficulty in Guessing Connection Information*: As stated in [33], the field lengths in RINA offer 2^{48} possibilities for connection information. This is substantially larger than the 2^{29} possibilities in TCP during data transfer, making it exponentially harder for an attacker to guess the connection information.

J. QOS

In RINA, each connection is established only after the source presents its QoS requirements, which typically include parameters such as the maximum requested bandwidth as outlined in [44]. This capability of RINA has important implications for IoT network security:

- *DoS Prevention*: A major security benefit of the RINA's QoS mechanism is its inherent resistance to Denial of Service (DoS) attacks. If an entity attempts to deviate from its specified QoS requirements, such as by generating excessive network traffic in an attempt to congest the network, its packets can be dropped at the first routing node. This acts as a form of DoS prevention, as it allows the network to maintain its service availability even in the face of potential attacks.
- *Traffic Regulation*: By enforcing QoS requirements at the connection level, RINA helps regulate network traffic. This means that each connection can only generate a certain amount of traffic, as specified by its QoS requirements. This helps prevent network congestion and maintains the overall performance and reliability of the network.
- *Monitoring and Detection*: The enforcement of QoS requirements can also serve as a basis for monitoring and detection mechanisms [45]. Any deviation from the specified QoS requirements can be flagged as potential malicious activity, enabling the early detection and mitigation of security threats.

K. RESILIENCY

In RINA, each DIF independently and transparently performs (multi-path) routing to the other DIFs. This design brings about several significant implications for IoT network security:

- *DIF-Level Resiliency*: Each DIF is capable of providing resiliency services to the upper DIFs. This means that even if a particular path or network segment becomes unavailable, the communication can still proceed via alternative paths, enhancing the overall reliability and availability of the network.
- *Heterogeneous Network Transport*: As noted in [46], this design also enables ''transport over heterogeneous networks''. This property allows IoT networks to operate over and across different types of networks, enhancing their interoperability and adaptability to different environments and requirements.
- *Mitigation of Single Points of Failure*: The independent routing mechanism of each DIF effectively decentralizes the network's routing process. This decentralization reduces the risk of single points of failure and makes the network more robust against attacks that target specific network components or paths.
- *Load Balancing*: Multi-path routing can distribute network traffic across multiple paths, helping to balance the load and prevent network congestion [47]. This load balancing can further enhance network performance and reliability, making it more difficult for attackers to disrupt the network through congestion-based attacks.
- *Rapid Recovery from Failures*: The resiliency feature also enables rapid recovery from network failures. If a particular path or DIF fails, the independent routing mechanism can quickly reroute the traffic through other operational paths or DIFs, minimizing the impact of the failure on the network's operation and service availability [48].

L. PERFORMANCE IMPROVEMENTS

Beyond the security benefits provided by RINA, the architecture also possesses some crucial features that markedly improve network performance, which are particularly attractive for IoT networks [49]. Various research studies[4] and international projects[5] have demonstrated that RINA can significantly enhance network performance in terms of throughput and delay [10]. These performance improvements indirectly contribute to IoT security in several ways as discussed in the above subsections.

M. COMPLEXITY REDUCTION

One of RINA's salient characteristics is its ability to simplify the overall network architecture, resulting in a significant reduction in complexity. This reduction can have far-reaching implications for the security of IoT networks [36].

In contrast to the current Internet with its plethora of protocols, RINA networks can fulfill security requirements with fewer protocols, flows, and distinct mechanisms. By decreasing the number of active instances of networking mechanisms, the complexity of managing and securing the network is significantly reduced.

For instance, RINA networks with a secured link layer inherently have fewer active instances of networking mecha-

[4] A comprehensive list of publications on RINA can be found at http://www.pouzinsociety.org/research/publications

[5] For more information, visit http://www.pouzinsociety.org/research/projects

nisms, leading to a more manageable and secure environment [36].

Furthermore, RINA reduces the size of routing tables [35], [50], [51], which has a dual benefit: it not only simplifies the management of the network but also minimizes the attack surface for potential intruders. Smaller routing tables mean fewer potential points of failure or compromise. The other benefits include:

- *Reduced Vulnerabilities*: With fewer protocols and mechanisms, there are fewer points of vulnerability that could be exploited by attackers.
- *Easier Management*: A less complex network is easier to monitor and manage, making it simpler to detect and respond to potential security threats [43].
- *Simpler Security Policies*: Less complexity allows for the creation of simpler, more robust security policies [52].
- *Better Resource Utilization*: Reducing the number of active instances of networking mechanisms allows for more efficient use of network resources, which can be beneficial for security.

VI. HOW RINA ADDRESSES THE EFFICIENCY AND SECURITY TRADE-OFF

In the evolving landscape of the Internet of Things (IoT), it has become increasingly important to address the trade-off between efficiency and security in network communications. This is where RINA comes to the fore, providing a compelling solution that does not compromise on either facet.

A. EFFICIENCY IN RINA

In terms of efficiency, RINA outperforms traditional network architectures due to its recursive and distributed nature. The architecture uses a minimalist approach, reducing the number of protocols, required flows, and distinct mechanisms, which not only simplifies network management but also leads to better resource utilization [36].

RINA's design also incorporates performance improvements, as demonstrated in various research studies and international projects [10], [49]. These studies have shown that RINA effectively improves network performance in terms of throughput and delay, which are critical for IoT networks.

Moreover, the RINA model promotes a more effective Quality of Service (QoS) management [44]. Connections in RINA are established based on the source's QoS requirements, which includes maximum requested bandwidth. This mechanism ensures that network resources are allocated efficiently and used optimally.

B. SECURITY IN RINA

RINA's distinct approach to network architecture also provides numerous security advantages. One of the key advantages lies in its inherent resistance to insider attacks, thanks to the wider range of control field values used, such as connection/QoS id [33].

Furthermore, the architecture's *divide-and-conquer* approach reduces the overall risk posed to the network. If a DIF is compromised, it does not affect the entire network [18]. Each DIF operates independently and transparently to others, providing inherent resilience and security.

Authentication is another strong security feature in RINA. All IPCPs must be authenticated before joining a DIF. This mechanism ensures that attackers cannot address IPCPs in a DIF without first undergoing the authentication process.

C. BALANCING EFFICIENCY AND SECURITY

RINA skillfully navigates the trade-off between efficiency and security in several ways. First, its programmable DIFs allow for new functionality to be developed as policies and plugged into existing mechanisms, minimizing the risk of creating new vulnerabilities while enhancing performance [36].

Second, its unique approach to addressing, with each DIF having its own hidden addresses, not only enhances security by making it harder for attackers to exploit IP addresses, but also increases efficiency by reducing the amount of overhead associated with managing global addresses.

Finally, RINA's simplified connection management, by adopting Watson's method, reduces the chance of connection misuse while enhancing efficiency by eliminating explicit control messages for connection establishment or closure [33].

In summary, RINA addresses the trade-off between efficiency and security by leveraging its unique recursive and distributed architecture, allowing it to provide superior performance without compromising on security. This makes RINA a promising architectural approach for the future of IoT communications.

VII. EMPLOYING RINA IN IOT – A USE CASE STUDY

To better understand the practical implications of RINA in IoT networks, we consider two use cases to discuss how RINA can be applied on. In the first one, *Home*, we assume that IoT devices can run a RINA stack, and in the second one, *Health*, we assume that devices have their own legacy protocol.

A. HOME

The smart home scenario is an ideal testbed for the application of RINA in the IoT context. In this setting, we consider a variety of smart devices, such as temperature sensors, smart light bulbs, home security cameras, and home automation systems, all provided by different vendors. The integration of these systems can pose a challenge due to the wide range of security and operational requirements, and the variety of legacy protocols involved.

The application of RINA in this context can provide a unified networking framework to alleviate these challenges. As shown in Fig. 6, we consider a common IoT network topology where wireless nodes, such as smart home devices, connect to an access point over a wireless protocol. In this case, the communication between the two devices (with IPCPs C1 and C2) requires a common DIF. Furthermore, the wireless node

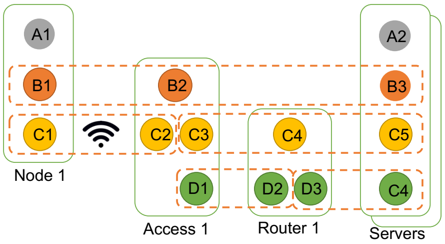


FIGURE 6. DIF arrangements for the home use case, where the IoT device can run a RINA stack.

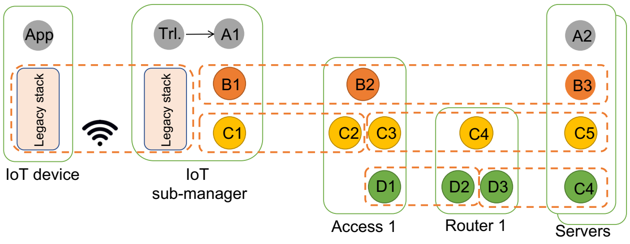


FIGURE 7. DIF arrangements for the health use case, where the IoT device cannot run a RINA stack.

must also belong to another DIF that spans over the network to reach the servers in the cloud.

In this scenario, the communication path traverses a network segment (between C3 and C5) that is not a member of the top DIF. This implies that packets between B2 and B3 are (or can be) inaccessible to Router1. This design provides an additional layer of security and privacy, as the data from the IoT devices in the home cannot be accessed or tampered with by unauthorized entities.

Moreover, this architecture allows for each segment of the path to customize its congestion control policy. For instance, the congestion controller between C3 and C5 can be tailored to the specific characteristics of that segment, while the congestion controller between C1 and C2 takes into account the conditions of the wireless link. This adaptability can enhance the efficiency and reliability of data transfers, which are key for seamless operation in a smart home environment.

Furthermore, each path segment can implement its own SDU protection policy, thereby enhancing the overall security of the network. At the same time, the node at B2 can perform any necessary operations on the PDU sent from B1 to reach B3. This feature ensures interoperability and smooth communication between IoT devices and the cloud servers.

B. HEALTH

The healthcare sector represents another significant area where IoT has been making a considerable impact, particularly in the field of patient monitoring and care. Wearable IoT devices have been instrumental in monitoring the health and behaviors of specific risk groups, such as elderly individuals, people recovering from illnesses, disabled individuals, and children. These devices aim to reduce risks, prevent accidents, issue preventive warnings, initiate corrective measures, or request assistance from *trusted* caregivers when necessary.

Fig. 7 depicts a sample topology of a health IoT device that does not inherently support RINA. As suggested by [53], these legacy IoT devices can be incorporated into a RINA network using a special type of gateway called an IoT sub-manager. The IoT sub-manager's primary purpose is to translate a legacy (non-RINA) IoT protocol to a common RINA protocol – CDAP. CDAP achieves commonality by focusing on operations such as read/write, create/delete, and start/stop on object models. This arrangement allows for seamless integration of legacy devices while maintaining the benefits of the RINA architecture.

The network segment from the IoT sub-manager to the servers is identical to the previous scenario; it routes packets seamlessly while taking into account their security, eliminating the need for an end-to-end connection. The IoT sub-manager plays a critical role in this architecture as it is responsible for translating the legacy protocol/packets from the IoT device into a format that can be understood by the RINA network. This translation operation is performed by the Trl module within the IoT sub-manager.

Once translated, the data is passed to IPC process A1, where it is treated in the same manner as data presented to A1 in Fig. 6. This arrangement implies that the IoT sub-manager should be a trusted device due to its critical role in data translation and transmission.

An important consideration when using IoT sub-managers is managing the data send rate of the IoT device. If the IoT device transmits data faster than the RINA network segment can handle, creating a bottleneck, the Trl module within the IoT sub-manager should be able to push back or slow down the App. This capability adds to the versatility of the translation function performed by the Trl module and ensures efficient and reliable data transmission in the health IoT network.

The incorporation of legacy IoT devices into a RINA network using IoT sub-managers can significantly enhance the security, reliability, and efficiency of health IoT networks. This arrangement allows for the secure and efficient monitoring of high-risk individuals, leading to improved patient care and outcomes.

C. SECURE MULTICAST

Secure multicast forms an integral part of IoT networking where one source node often needs to send data to multiple destination nodes. Such a feature becomes crucial in scenarios like home automation, where a single command needs to be dispatched to multiple devices, or in healthcare, where patient data may need to be shared with multiple healthcare providers simultaneously [54].

In the context of RINA, secure multicast can be implemented *effortlessly* and *efficiently*, eliminating the need for the complex security measures described for multicast CoAP applications in [54].

In RINA, security is an integral part of the architecture, not an add-on. The security in RINA is based on the principle of "only talk to known and authenticated IPC processes". This means that any IPCP, including those involved in multicast communication, must be authenticated before it can join a DIF. This authentication process ensures that only authorized processes can participate in the multicast communication, providing a high level of security. This also contrasts with the CoAP approach, which requires the establishment of a group key and a set of pairwise keys for secure multicast communication, a process that can be complex and resource-intensive.

Refer to Fig.6 and Fig.7, where the goal is to transmit data from an IoT device to several servers. This does not necessitate multiple separate connections from the IoT device to each server. Instead, RINA enables the use of a multicast destination address within DIF B. The process starts with IPCP B1 receiving a packet from the IoT device and sending it to B2. At this stage, the RMT (Relaying and Multiplexing Task) module within B2 comes into play. The RMT module examines the destination port(s) and identifies that there are multiple servers connected to Access1 via Router1, each having a distinct DIF with C3, C4, and C5.

Upon this identification, the RMT in B2 replicates the packet and dispatches it to all the identified ports. As a result, IPCP C5 in each of the servers receives a copy of the packet and forwards it to the higher layers in the stack. This multicast mechanism ensures the security of the packets within DIF B is maintained, as each packet remains within the boundaries of a single DIF, thus preserving the inherent security of the communication.

VIII. DISCUSSION

A. DEPLOYMENT

RINA represents a paradigm shift in network architecture, and like any groundbreaking technology, its adoption necessitates a phased approach. One of RINA's key strengths is its ability to operate over shim DIFs, enabling it to function even on a TCP/IP stack. This compatibility feature allows for a smoother transition from existing network architectures to RINA.

However, to fully leverage the benefits of RINA, extensive research has been conducted on its deployment strategies. For instance, the study performed in [53] demonstrates how RINA can be implemented as an architecture in IoT environments where nodes are incapable of running RINA directly. In such scenarios, nodes connect to an IoT sub-manager, allowing the rest of the network to operate as a RINA network. This approach effectively integrates RINA into current IoT systems.

In [55], the possibility of switching to RINA was evaluated in case a node can join a DIF directly via its first connected hop. In the RINAiSense project[6], the possibility of running RINA on limited devices such as sensors has been investigated. Deployment possibilities of RINA is also one of the main goals of OCARINA[7]. It was also shown that legacy applications that can use the TAPS API, can use RINA via a mapping of TAPS to RINA [56].

B. FURTHER RESEARCH TOPICS

The potential of RINA to facilitate secure end-to-end connections while allowing for their segmentation presents intriguing research opportunities and challenges. A key consideration in this context is performance optimization, particularly the implementation of an effective feedback mechanism within the recursive architecture. This mechanism is crucial for managing congestion controllers in a sequenced or stacked configuration [10].

In our previous work [57], we conducted an analytical evaluation of various feedback methods, assessing their impact on system stability and average queue length. Our findings indicated that strict pushback feedback, based solely on queue size, could lead to stability issues. This observation as well as our study in [58] underscore the need for a more sophisticated feedback method that does not rely exclusively on queue size.

In the same study [57], we utilized Scalable TCP. However, we believe that the performance could be further enhanced by adopting a congestion controller such as LGC [59]–[61]. In LGC, we employed the same ECN signaling used by DCTCP, but with a lower marking threshold. This modification resulted in smoother behavior and a shorter queue length.

Currently, we are developing a multihop congestion controller based on LGC for RINA. The outline of a recursive congestion control mechanism is depicted in [62]. This controller can leverage the flow aggregation capability provided by lower DIFs. This feature allows IoT devices to perform data aggregation [63], which can significantly reduce energy consumption. This is in contrast to packet aggregation [64], which is performed at the physical (or lower) layer to decrease protocol overhead [65]. Interestingly, these two approaches can be employed simultaneously in RINA, offering potential for enhanced efficiency.

In the context of IoT, the ability to perform both data and packet aggregation can have significant implications. Data aggregation [63] allows IoT devices to consolidate and summarize data before transmission, reducing the amount of data that needs to be transmitted and thus saving energy. This is particularly important for battery-powered IoT devices, where energy efficiency is a key concern.

On the other hand, packet aggregation [64] is performed at the physical (or lower) layer to decrease protocol overhead [65]. By combining multiple smaller packets into a larger one, packet aggregation can reduce the per-packet overhead, leading to more efficient use of network resources.

Furthermore, the development of appropriate SDU Protection policies is another important research direction. SDU Protection policies in RINA can provide a range of security services, including data integrity, confidentiality, and authentication. Developing SDU Protection policies that are tailored for constrained IoT devices can help to ensure that these devices can securely participate in a RINA network, despite their limited resources.

[6] See https://distrinet.cs.kuleuven.be/research/projects/RINAiSense

[7] See http://www.mn.uio.no/ifi/english/research/projects/ocarina

Finally, the development of multicast protocols for constrained IoT devices is another interesting research challenge. Multicast communication can be more efficient than unicast communication for certain types of IoT applications, such as those that involve group communication or data dissemination. However, designing multicast protocols that can operate efficiently and securely on constrained IoT devices is a non-trivial task.

IX. CONCLUSION

This paper delved into the inherent architectural performance and security intricacies of IoT networks, shedding light on the numerous challenges present in the current IoT network stacks. We illustrated that securing transport layer communication is not a straightforward task but a delicate trade-off balancing performance and security in IoT.

In the pursuit of an effective solution, we turned our attention towards RINA, a promising network architecture with recursive design principles. We explicated the fundamental data transfer mechanisms within RINA and emphasized the importance of embedded security at each layer of the communication stack.

Our exploration revealed that RINA's design inherently reconciles the traditional trade-off between transport layer security and efficiency. We showed that the EFCP module within each layer of RINA offers features that significantly resist against internal attackers. Between layers, RINA ensures security through SDU protection, separating this intra-layer and inter-layer security, which, in turn, facilitates protocol translation and connection splitting along the communication path.

To illustrate the practical application of our proposed solution, we presented two distinctive use cases, each benefiting uniquely from the integration of RINA. Whether an IoT device natively supports the RINA stack or not, we demonstrated architectural solutions that not only enhance security and performance but also facilitate secure multicast. Notably, secure multicast has been a long-standing requirement in the IoT landscape, yet remains largely unaddressed by current protocols while considering efficiency as well.

Our discussion extended to various RINA deployment methods, providing a comprehensive understanding of how this novel architecture can be practically implemented within diverse IoT scenarios. As we continue our exploration in this field, we envision future directions that further push the boundaries of IoT network performance and security, building upon the foundational principles and methods established in this paper.

In conclusion, we believe that RINA represents a significant stride towards overcoming the challenges that IoT networks face today. By rethinking network architecture and leveraging recursion, RINA provides a robust and scalable solution that stands to redefine the security and efficiency paradigms in IoT networks.

ACKNOWLEDGMENT

It should be noted while the content of this paper is human-generated, Generative-AI, in particular ChatGPT-4 (https://chat.openai.com/) has been used for editing, proof-reading, and increasing the readability of sentences. The final round of proof-reading has been done by the authors.

REFERENCES

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10 – 28, 2017.

[2] O. Garcia-Morchon, S. Kumar, and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges," RFC 8576, Apr 2019. [Online]. Available: https://rfc-editor.org/rfc/rfc8576.txt

[3] C. Caini, R. Firrincieli, and D. Lacamera, "PEPsal: a Performance Enhancing Proxy for TCP satellite connections," *IEEE Aerospace and Electronic Systems Magazine*, vol. 22, no. 8, pp. 7–16, 2007.

[4] Z. Shelby, K. Hartke, and C. Bormann, "The Constrained Application Protocol (CoAP)," RFC 7252, Jun 2014. [Online]. Available: https://rfc-editor.org/rfc/rfc7252.txt

[5] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC 6347, Jan 2012. [Online]. Available: https://rfc-editor.org/rfc/rfc6347.txt

[6] A. Stanford-Clark and H. L. Truong, "Mqtt version 3.1.1," OASIS Standard, Standard mqtt-v3.1.1-os, 2014. [Online]. Available: https://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html

[7] P. I. R. Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, "Securing the internet of things: challenges, threats and solutions," *Internet of Things*, vol. 5, pp. 41–70, 2019.

[8] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294–1312, thirdquarter 2015.

[9] J. Day, *Patterns in Network Architecture: A Return to Fundamentals*. Prentice Hall, 2007.

[10] P. Teymoori, M. Welzl, G. Stein, E. Grasa, R. Riggio, K. Rausch, and D. Siracuss, "Congestion control in the Recursive Internetwork Architecture (RINA)," in *IEEE International Conference on Communications (ICC), Next Generation Networking and Internet Symposium*, May 2016.

[11] "Ieee standard for local and metropolitan area networks–part 15.4: Low-rate wireless personal area networks (lr-wpans)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1–314, Sept 2011.

[12] G. Montenegro, C. Schumacher, and N. Kushalnagar, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," RFC 4919, Aug 2007. [Online]. Available: https://rfc-editor.org/rfc/rfc4919.txt

[13] P. Thubert and J. Hui, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," RFC 6282, Sep 2011. [Online]. Available: https://rfc-editor.org/rfc/rfc6282.txt

[14] E. Rescorla and T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, Aug 2008. [Online]. Available: https://rfc-editor.org/rfc/rfc5246.txt

[15] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. L. Aguiar, and A. V. Vasilakos, "Information-centric networking for the internet of things: challenges and opportunities," *IEEE Network*, vol. 30, no. 2, pp. 92–100, 2016.

[16] T. Ramezanifarkhani and P. Teymoori, "Securing the internet of things with recursive internetwork architecture (rina)," in *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2018, pp. 188–194.

[17] Y. Yang, L. Wu, and et al., "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, 2017.

[18] J. Day, I. Matta, and K. Mattar, "Networking is IPC: a guiding principle to a better internet," in *Proc. ACM CoNEXT*, 2008, p. 67.

[19] J. Suarez, J. Quevedo, I. Vidal, D. Corujo, J. Garcia-Reinoso, and R. L. Aguiar, "A secure iot management architecture based on information-centric networking," *Journal of Network and Computer Applications*, vol. 63, pp. 190–204, 2016.

[20] R. Ravindran, Y. Zhang, L. A. Grieco, A. Lindgren, J. Burke, B. Ahlgren, and A. Azgin, "Design Considerations for Applying ICN to IoT," Internet Engineering Task Force, Internet-Draft draft-irtf-icnrg-icniot-03, May 2019, work in Progress.

[21] C. Fang, H. Yao, Z. Wang, W. Wu, X. Jin, and F. R. Yu, "A survey of mobile information-centric networking: Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, 2018.

[22] T. T. Thai, D. M. L. Pacheco, E. Lochin, and F. Arnal, "SatERN: a PEP-less solution for satellite communications," in *Proc. IEEE ICC*, 2011.

[23] D. Bimschas, H. Hellbrück, and et al., "Middleware for smart gateways connecting sensornets to the internet," in *Proceedings of the 5th International Workshop on Middleware Tools, Services and Run-Time Support for Sensor Networks*. ACM, 2010, pp. 8–14.

[24] B. Kang, D. Kim, and H. Choo, "Internet of everything: A large-scale autonomic iot gateway," *IEEE Transactions on Multi-Scale Computing Systems*, vol. PP, no. 99, pp. 1–1, 2017.

[25] R. Alexander, A. Brandt, J. Vasseur, J. Hui, K. Pister, P. Thubert, P. Levis, R. Struik, R. Kelsey, and T. Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, Mar 2012. [Online]. Available: https://rfc-editor.org/rfc/rfc6550.txt

[26] L. Das, M. Gupta, P. Anand, L. Ahuja, V. Bibhu, and J. Pateria, "Recent aspects of ipv6 on security challenges in iot," in *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*. IEEE, 2023, pp. 890–896.

[27] I. Psaras, L. Saino, and G. Pavlou, "Revisiting resource pooling: The case for in-network resource sharing," in *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*, ser. HotNets-XIII. New York, NY, USA: ACM, 2014, pp. 24:1–24:7. [Online]. Available: http://doi.acm.org/10.1145/2670518.2673875

[28] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[29] V. Marinakis and H. Doukas, "An advanced iot-based system for intelligent energy management in buildings," *Sensors*, vol. 18, no. 2, p. 610, 2018.

[30] D. Bringhenti, F. Valenza, and C. Basile, "Toward cybersecurity personalization in smart homes," *IEEE Security & Privacy*, vol. 20, no. 1, pp. 45–53, 2021.

[31] L. Liu, E. Stroulia, I. Nikolaidis, A. Miguel-Cruz, and A. R. Rincon, "Smart homes and home health monitoring technologies for older adults: A systematic review," *International journal of medical informatics*, vol. 91, pp. 44–59, 2016.

[32] J. Huang, Q. Duan, Y. Zhao, Z. Zheng, and W. Wang, "Multicast routing for multimedia communications in the internet of things," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 215–224, 2016.

[33] G. Boddapati, J. Day, I. Matta, and L. Chitkushev, "Assessing the security of a clean-slate internet architecture," in *20th IEEE International Conference on Network Protocols (ICNP)*. IEEE, 2012.

[34] E. Grasa, O. Rysavy, O. Lichtner, H. Asgari, J. Day, and L. Chitkushev, "From protecting protocols to layers: Designing, implementing and experimenting with security policies in rina," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–7.

[35] S. Leon, J. Perello, and et al., "Benefits of programmable topological routing policies in rina-enabled large-scale datacenters," in *Global Communications Conference*. IEEE, 2016.

[36] J. Small, "Patterns in network security: An analysis of architectural complexity in securing recursive inter-network architecture networks," Master's thesis, Boston University Metropolitan College, 2012.

[37] "Pouzin society," 2019. [Online]. Available: http://pouzinsociety.org/

[38] Next Generation Protocols (NGP) ETSI Industry Specification Group (ISG), "GR NGP 009 - V1.1.1 - Next Generation Protocols (NGP); An example of a non-IP network protocol architecture based on RINA design principles," ETSI, Tech. Rep., 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gr/NGP/001_099/009/01.01.01_60/gr_ngp009v010101p.pdf

[39] R. W. Watson, "Timer-based mechanisms in reliable transport protocol connection management," *Computer Networks (1976)*, vol. 5, no. 1, pp. 47–56, 1981.

[40] T. Kunchok, V. Kirubanand *et al.*, "A lightweight hybrid encryption technique to secure iot data transmission," *International Journal of Engineering & Technology*, vol. 7, no. 2.6, pp. 236–240, 2018.

[41] J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle, and V. Singh, "A survey of payment card industry data security standard," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 3, pp. 287–303, 2010.

[42] A. Molina Zarca, M. Bagaa, J. Bernal Bernabe, T. Taleb, and A. F. Skarmeta, "Semantic-aware security orchestration in sdn/nfv-enabled iot systems," *Sensors*, vol. 20, no. 13, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/13/3622

[43] C.-M. Mathas, C. Vassilakis, N. Kolokotronis, C. C. Zarakovitis, and M.-A. Kourtis, "On the design of iot security: Analysis of software vulnerabilities for smart grids," *Energies*, vol. 14, no. 10, 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/10/2818

[44] S. L. Gaixas, J. Perelló, and et al., "Assuring qos guarantees for heterogeneous services in rina networks with δq," in *Cloud Computing Technology and Science , 2016 IEEE International Conference on*. IEEE, 2016.

[45] A. Protogerou, S. Papadopoulos, A. Drosou, D. Tzovaras, and I. Refanidis, "A graph neural network method for distributed anomaly detection in iot," *Evolving Systems*, vol. 12, pp. 19–36, 2021.

[46] E. Trouva, E. Grasa, and et al., "Transport over heterogeneous networks using the rina architecture," in *Proceedings of the 9th IFIP TC 6 International Conference on Wired/Wireless Internet Communications*, 2011.

[47] M. Marek, P. Teymoori, S. Gjessing, and M. Welzl, "High-rate data transfer with congestion-aware multipath routing," in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6.

[48] B. S. Neelam and B. A. Shimray, "Applicability of rina in iot communication for acceptable latency and resiliency against device authentication attacks," in *2021 6th International Conference for Convergence in Technology (I2CT)*. IEEE, 2021, pp. 1–7.

[49] E. Trouva, E. Grasa, J. Day, I. Matta, L. T. Chitkushev, P. Phelan, M. P. De Leon, and S. Bunch, "Is the internet an unfinished demo? meet rina!" in *TERENA Networking Conference*, 2010, pp. 1–12.

[50] F. Hrizi and A. Laouiti, "Hierarchical small world overlay for efficient forwarding in volunteer clouds," in *IEEE 31st International Conference on Advanced Information Networking and Applications*. IEEE, 2017.

[51] F. Hrizi, A. Laouiti, and H. Chaouchi, "Sfr: Scalable forwarding with rina for distributed clouds," in *Network of the Future (NOF), 2015 6th International Conference on the*. IEEE, 2015, pp. 1–6.

[52] I. Marcu, G. Suciu, C. Bălăceanu, A. Vulpe, and A.-M. Drăgulinescu, "Arrowhead technology for digitalization and automation solution: Smart cities and smart agriculture," *Sensors*, vol. 20, no. 5, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/5/1464

[53] M. Rizinski, J. Day, and L. Chitkushev, "IoT Architecture based on RINA," in *7th International Workshop on RINA, co-located with IEEE ICIN 2020*. Paris: IEEE, 2020.

[54] C.-S. Park, "Security architecture for secure multicast coap applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3441–3452, 2020.

[55] K. Ciko and M. Welzl, "First contact: Can switching to rina save the internet?" in *6th International Workshop on the Recursive InterNetwork Architecture (RINA 2019), co-located with IEEE ICIN 2019*. IEEE, 2019, pp. 37–42.

[56] K. Ciko, M. Welzl, and M. Marek, "Taps and rina: Do they fit together?" in *7th International Workshop on RINA 2020, co-located with IEEE ICIN 2020*. Paris: IEEE, 2020.

[57] D. A. Hayes, P. Teymoori, and M. Welzl, "Feedback in recursive congestion control," in *European Workshop on Performance Engineering*. Springer, 2016, pp. 109–125.

[58] M. Welzl, P. Teymoori, S. Islam, D. Hutchison, and S. Gjessing, "Future internet congestion control: The diminishing feedback problem," *IEEE Communications Magazine*, vol. 60, no. 9, pp. 87–92, 2022.

[59] P. Teymoori, D. Hayes, M. Welzl, and S. Gjessing, "Even lower latency, even better fairness: Logistic growth congestion control in datacenters," in *IEEE LCN*. IEEE, 2016, pp. 10–18.

[60] P. Teymoori and M. Welzl, "Lgcc: Food chain multi-hop congestion control," *Research report http://urn. nb. no/URN: NBN: no-35645*, 2020.

[61] K. Ciko, P. Teymoori, and M. Welzl, "Lgc-shq: Datacenter congestion control with queueless load-based ecn marking," *ACM SIGCOMM Computer Communication Review*, vol. 52, no. 4, pp. 2–11, 2022.

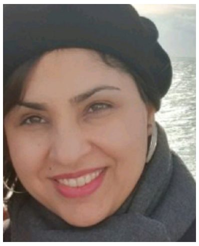
[62] M. Welzl, P. Teymoori, S. Gjessing, and S. Islam, "Follow the model: How recursive networking can solve the internet's congestion control problems," in *2020 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2020, pp. 518–524.

[63] P. Teymoori, M. Kargahi, and N. Yazdani, "A real-time data aggregation method for fault-tolerant wireless sensor networks," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, 2012.

[64] P. Teymoori, A. Dadlani, K. Sohraby, and K. Kim, "An optimal packet aggregation scheme in delay-constrained ieee 802.11n wlans," in *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, 2012, pp. 1–4.

[65] P. Teymoori, N. Yazdani, S. A. Hoseini, and M. R. Effatparvar, "Analyzing delay limits of high-speed wireless ad hoc networks based on ieee 802.11n," in *2010 5th International Symposium on Telecommunications*, 2010, pp. 489–495.

PEYMAN TEYMOORI is an Associate Professor at the University of South-Eastern Norway (USN). He obtained his Ph.D. in Computer Science from the University of Tehran, specializing in Wireless Adhoc Networks. Post-graduation, he further enriched his research portfolio as a Postdoctoral and then as a Senior Research Fellow at the University of Oslo, before transitioning to his current role at USN. His research area includes the modeling, optimization, and performance evaluation of communication networks, the Recursive InterNetwork Architecture (RINA), and networking technologies like Internet of Things (IoT), 5G/6G, WiFi, and Ad hoc Networks.



TOKTAM RAMEZANIFARKHANI is an Associate Professor specializing in Cybersecurity. She has devoted her academic and professional career to the field of information security, with a particular focus on various aspects of cybersecurity. Her research interests span a broad spectrum, ranging from theoretical foundations to practical applications. These include software security, application and language-based security, vulnerability analysis, penetration testing, IoT security, and the application of formal methods in information security. She also has a keen interest in the human aspects of cybersecurity, recognizing the critical role that individuals play in maintaining secure systems.