P-IOTA

Subjects: Computer Science, Information Systems

Contributor: Amir Al Sadi, Carlo Mazzocca, Andrea Melis, Rebecca Montanari, Marco Prandini, Nicolò Romandini

The recent widespread novel network technologies for programming data planes are remarkably enhancing the customization of data packet processing. In this direction, the Programming Protocol-independent Packet Processors (P4) is envisioned as a disruptive technology, capable of configuring network devices in a highly customizable way. P4 enables network devices to adapt their behaviors to mitigate malicious attacks (e.g., denial of service). Distributed ledger technologies (DLTs), such as blockchain, allow secure reporting alerts on malicious actions detected across different areas. IOTA is a next-generation distributed ledger engineered to tackle the scalability limits while still providing the same security capabilities such as immutability, traceability, and transparency. P-IOTA integrates a P4-based data plane software-defined network (SDN) and an IOTA layer employed to notify about networking attacks.

Keywords: SDN ; P4 ; IOTA ; Tangle ; blockchain ; distributed ledger technology

1. Introduction

The advent of distributed technologies has led to the emergence of decentralized systems that rely on a network of nodes for computation and data storage. These systems facilitate the collaborative and distributed use of computational resources, as opposed to relying on a central authority, leading to more efficient resource utilization, improved security, and greater resilience. However, the very nature of distributed infrastructures intrinsically brings architectural vulnerabilities that can be exploited by attackers. One of the most-famous attacks that leveraged these architectures is the distributed denial of service (DDoS) [1], which seeks to disrupt network services and host connectivity in a distributed environment by overloading the network with unnecessary requests. Avoiding and mitigating DDoS attacks is a primary concern for many organizations.

Software-defined networking (SDN) is a cutting-edge networking approach that divides the control and data plane layers to carry out its specific tasks. In SDN, the physical network layer is seen as fully programmable, resulting in increased customization of data packet processing. Such a feature has greatly contributed to its widespread deployment across different cloud infrastructures. In this direction, the Programming Protocol-independent Packet Processors (P4) has emerged as an innovative programming language, operating at the data plane level, to configure network devices in a highly customizable manner. P4 allows full programming of networking devices while being target-independent. Furthermore, the capability of programming the data plane is boosting the ability to detect network attacks.

How to effectively and securely share information to detect attacks is a challenging task. Distributed ledger technologies (DLTs), such as blockchain, are digital systems spread across multiple locations that securely store information (transactions) without the need for a central entity. Blockchain represents the most-famous type of DLT; its data structure foresees a chain of blocks connected through hashes and validated by third-party entities (i.e., miners or validators) following a consensus protocol. However, the validation process consumes a significant amount of time and energy, which can hinder blockchain's efficiency and adoption for information sharing. To address these concerns, alternative DLTs, such as IOTA, are recently emerging as promising solutions. IOTA offers the same security features of the blockchain (i.e., immutability, traceability, and transparency) while addressing the efficiency concerns.

The differences between IOTA and blockchains have been widely investigated in the literature [2][3][4], with numerous studies showing that IOTA is a superior solution in terms of scalability, transaction rate, and efficiency, particularly with regard to energy consumption. IOTA outperforms traditional blockchains due to its low latency combined with the ability to send transactions without any fees [2]. Reference [4] presented an in-depth comparison of the performance of multiple consensus protocols where IOTA achieves the best performance with a transaction rate that is several orders of magnitude higher than the other protocols. Therefore, its lightweight consensus protocol makes it one of the few truly suitable technologies for Internet of Things (IoT) devices [3]. These properties are particularly relevant in SDN-based environments due to the strict latency requirements of the data plane. In the state-of-the-art, there are very few examples of research proposals that integrate P4 and DLTs.

2. P-IOTA Architecture

P-IOTA is tailored for distributed networks that belong to multiple organizations, such as cloud infrastructures, where computational and networking resources are often spread across geographic locations and critical information is stored. These types of networks are often treated as local networks (e.g., cloud-hosted installations) by system administrators, but it can be challenging to quickly detect and block threats while spreading alert information in such a distributed environment (**Figure 1**).

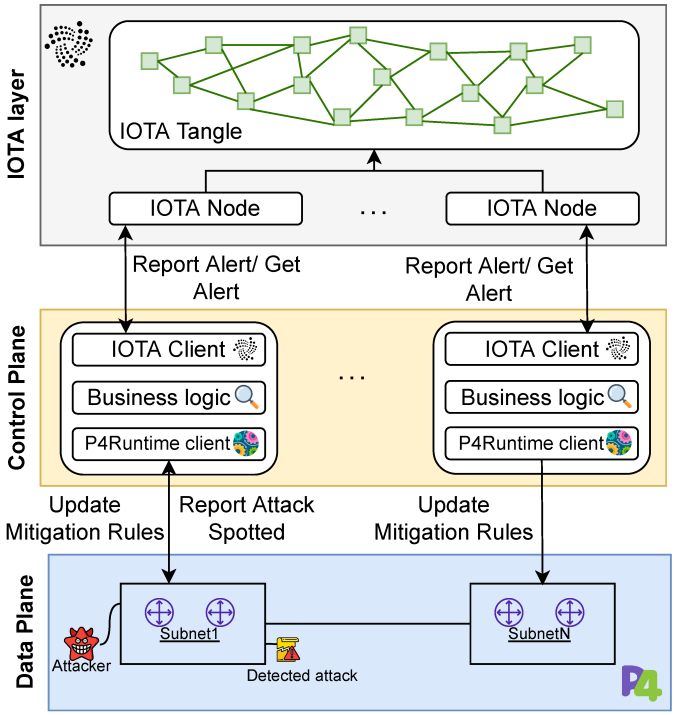

Figure 1. The P-IOTA architecture.

The main goal of this framework is to facilitate the dissemination of network attack alerts through IOTA. In order to generate alerts in a highly customized and efficient way, P-IOTA leverages an SDN-based architecture, involving a P4 data plane layer that detects network attacks. The generated alerts are then used to notify other controllers through the IOTA layer. The infrastructure consists of three main components:

- IOTA layer's main role is to notify and log alarms from the data plane and to share mitigation strategies. The IOTA layer notifies the portions of the network that can be impacted by the detected attack and disseminates the policy that should be applied to mitigate it.

- The control plane is responsible for managing and configuring the underlying physical network. It contains multiple local network managers (i.e., controllers), each of which controls a specific subnet. The controllers interact with the IOTA layer using an IOTA client and with the data plane using P4Runtime.

- The data plane is the layer hosting the physical devices that forward traffic. By using P4 and the programmable data plane, part of the detection intelligence can be moved from the control plane to the data plane. This allows for deep packet inspection and network-level probing to detect anomalies.

P-IOTA is designed to propagate real-time alerts from the data plane and deliver them quickly throughout a distributed environment. The IOTA Tangle maintains an immutable list of alerts in the form of a log, allowing for further investigations into the attack history offline without the risk of log cleaning. Moreover, the Tangle can be leveraged to share the countermeasure needed to mitigate the detected attacks. Hence, the solution offers intrusion detection capabilities on the data plane in the form of in-network detection, offloading a significant amount of detection intelligence to networking devices.

2.1. IOTA Layer

The IOTA layer comprises the IOTA nodes that hold a unified view of the Tangle. The decision to use IOTA to share information across different sites [5] was motivated by the following features:

- Efficient lookup: Each transaction can be tagged, making it easier to collect IPs from the Tangle. If another DLT were adopted, an additional tag within the transaction message would significantly slow down the time it takes to find a transaction.

- Zero-value transactions: IOTA enables neglecting cryptocurrency, reducing the complexity of managing IPs. In contrast, each controller would need to have sufficient funds to perform the operations.

- Scalability: The Tangle allows parallel validation of transactions without any intermediary. Such a capability overcomes blockchain-based solutions, where a transaction is not recorded until it is stored in a block.

Finally, the Tangle structure also shortens the time needed to record a new transaction. Transactions are recorded on the Tangle as soon as they are created, whereas, in blockchain-based solutions, they must wait until they are stored in a block.

2.1.1. IOTA Node

In a federation, each participating enterprise should have at least one IOTA node to receive notifications from other organizations. However, a company may not collaborate with external parties and may have multiple sites located in different regions. Therefore, to reduce latency and facilitate swift mitigation, a company may choose to deploy an IOTA node at each of its sites.

2.1.2. IOTA Tangle

The Tangle is the data structure employed to share information, such as alarms and mitigation, among different controllers. This information is shared through zero-value transactions that do not require validation and, hence, help maintain a unified view of the Tangle while keeping low latency and energy consumption. As discussed in the previous section, these features make IOTA a suitable choice for SDN-based scenarios where threat alerts and mitigation have to be quickly disseminated among devices that may have limited capabilities.

2.2. Control Plane

The control plane is responsible for managing, configuring, and monitoring the physical network. It consists of multiple geographically dispersed controllers, which are in charge of managing a single network. These controllers work together and receive alerts from the IOTA layer, which informs the correct nodes of potential attacks, as shown in **Figure 2**.

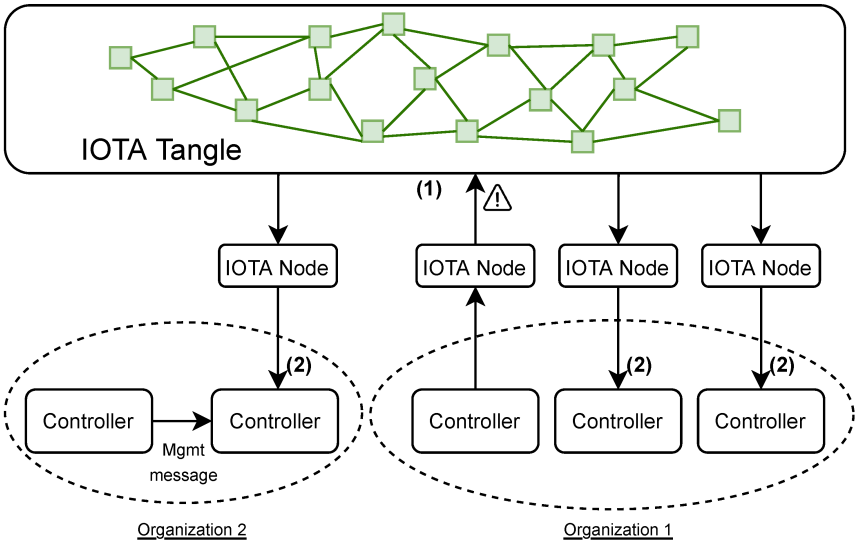

Figure 2. An example of organizations managing controllers associated with different subnets. In a federated environment, if an alert (1) is generated from a node, all interested controllers across organizations are notified (2).

Each controller acts as the primary management point for a local network. It keeps track of the status of networking devices, communicates with other controllers to make decisions about local network management strategies, and provides common control place services to monitor and administrate the data plane.

The control plane is made up of multiple controller instances, which are connected through messages. The components of each controller are:

- The IOTA client is responsible for connecting the controller instance to the corresponding IOTA node in the IOTA layer. It communicates with the IOTA node to send and receive alerts.
- The controller business logic handles the forwarding of the alerts to the IOTA client, sending management messages (e.g., congestion, link failures, etc.) to other controllers, and communicating with P4Runtime.
- P4Runtime is in charge of interacting with the networking through the P4Runtime Southbound Interface. It receives alerts generated from the data plane and installs the rules to react to these alerts.

As highlighted in **Figure 2**, organizations may manage multiple controllers, and if a controller detects a potential attack, it will communicate it to the IOTA node, which then notifies the interested controllers through the IOTA Tangle.

2.2.1. IOTA Client

The role of each controller in detecting and mitigating attacks is accomplished through the integration of an IOTA client. This client serves as a bridge between the controller and the IOTA node, allowing the exchange of information between the controller and the IOTA Tangle. One of the advantages of using IOTA clients is their lightweight design, which makes them suitable for deployment on devices with limited resources.

2.2.2. Controller Business Logic

This component plays a key role in managing and controlling the underlying network. It is responsible for expressing policies and communicating configuration or resource changes to neighboring controllers via management messages. The management messages are used to exchange information between physically close controllers, while the IOTA layer is in charge of disseminating alarms and mitigation strategies across a distributed network. In summary, the main functions of a controller include:

- Management messaging: sending messages to communicate with the neighbors' controllers.
- Alerting: forwarding alerts coming from the data plane to the IOTA node for further dissemination.
- Network configuration: interacting with and configuring the underlying network for forwarding or mitigation purposes.

This controller acts as the centralized core that manages the subnet and demonstrates the intelligence of the administration.

2.2.3. P4Runtime Client

This component is the client for the Southbound Interface that connects the controller business logic and the data plane level. P4Runtime abstracts the underlying hardware or software and offers agnostic APIs to the control plane to communicate with the physical network. The P4Runtime client is responsible for receiving communications from the data plane and performing two key functions:

- Installing match-action rules: it installs rules that specify forwarding logic or threat detection and mitigation strategies.
- Event listening: it listens for alerts from the data plane that indicate potential threats.

2.3. Data Plane

The data plane is in charge of processing and forwarding traffic. It includes networking devices such as switches and routers. Each controller is paired with one or more P4 border routers, which are capable of monitoring the traffic flowing in a given subnet and detecting abnormal behaviors. This allows the P4 switch to centrally inspect each network flow and determine if an attack is taking place. The programmability of P4 and the data plane enabled us to design pipelines that incorporate the detection of ongoing network attacks and normal forwarding behaviors. **Figure 3** reports the network topology used for the experiments.

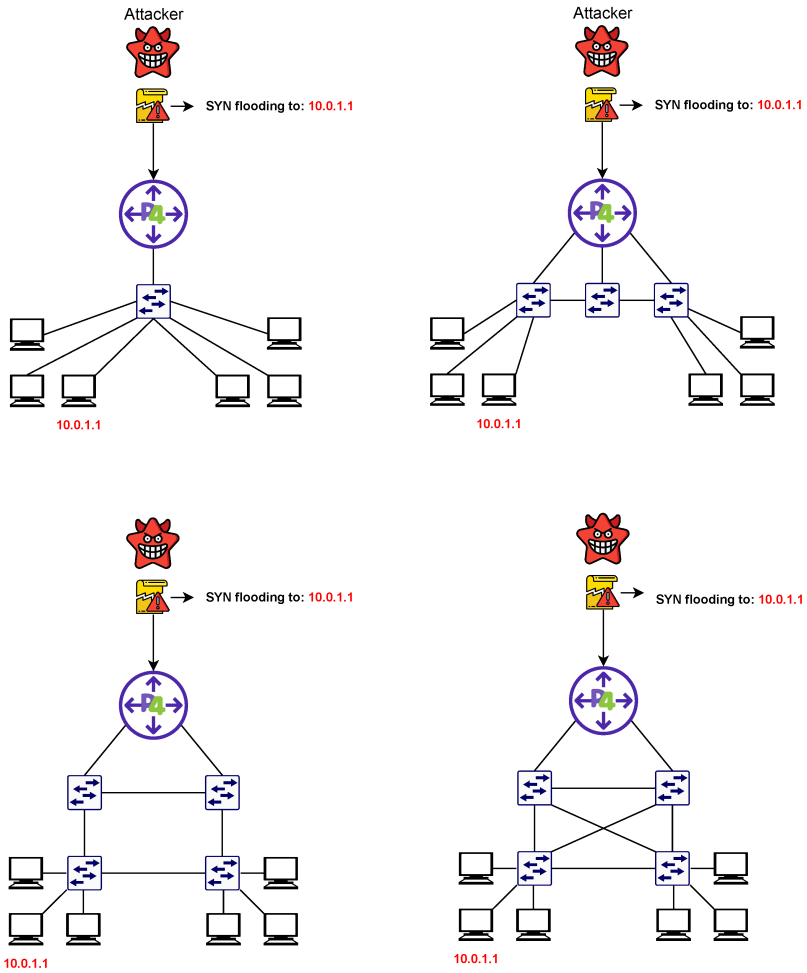

Figure 3. Network topology used for the testing phase. From the top-left corner, clockwise: single switch topology; linear topology; ring topology; fully connected topology.

References

1. Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl. 2016, 67, 147–165.
2. Alshaikhli, M.; Elfouly, T.; Elharrouss, O.; Mohamed, A.; Ottakath, N. Evolution of Internet of Things From Blockchain to IOTA: A Survey. IEEE Access 2022, 10, 844–866.
3. Auhl, Z.; Chilamkurti, N.; Alhadad, R.; Heyne, W. A Comparative Study of Consensus Mechanisms in Blockchain for IoT Networks. Electronics 2022, 11, 2694.
4. Rebello, G.A.F.; Camilo, G.F.; Guimarães, L.C.B.; de Souza, L.A.C.; Thomaz, G.A.; Duarte, O.C.M.B. A security and performance analysis of proof-based consensus protocols. Ann. Telecommun. 2021, 77, 517–537.
5. Mazzocca, C.; Sabbioni, A.; Montanari, R.; Colajanni, M. Evaluating Tangle Distributed Ledger for Access Control Policy Distribution in Multi-region Cloud Environments. In Proceedings of the Quality of Information and Communications Technology, Talavera de la Reina, Spain, 12–14 September 2022; Springer International Publishing: Cham, Switzerland, 2022; pp. 296–306.