Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks

Zarca, Alejandro Molina; Bernabe, Jorge Bernal; Skarmeta, Antonia; Alcaraz Calero, Jose M.

Published in:
IEEE Journal on Selected Areas in Communications

DOI:
10.1109/JSAC.2020.2986621

Published: 30/06/2020

Document Version
Peer reviewed version

Zarca, A. M., Bernabe, J. B., Skarmeta, A., & Alcaraz Calero, J. M. (2020). Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks. *IEEE Journal on Selected Areas in Communications*, *38*(6), 1262-1277. [9060972]. https://doi.org/10.1109/JSAC.2020.2986621

Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks

Alejandro Molina Zarca*, Jorge Bernal Bernabe*, Antonio Skarmeta*,
Jose M. Alcaraz Calero†
*University of Murcia
{alejandro.mzarca, jorgebernal, skarmeta}@um.es
†University of the West of Scotland
jose.alcaraz-calero@uws.ac.uk

Abstract

As the IoT adoption is growing in several fields, cybersecurity attacks involving low-cost end-user devices are increasing accordingly, undermining the expected deployment of IoT solutions in a broad range of scenarios. To address this challenge, emerging Network Function Virtualization (NFV) and Software Defined Networking (SDN) technologies can introduce new security enablers, thereby endowing IoT systems and networks with higher degree of scalability and flexibility required to cope with the security of massive IoT deployments. In this sense, honeynets can be enhanced with SDN and NFV support, to be applied to IoT scenarios and therefore strengthening the overall security. IoT honeynets are virtualized services simulating real IoT networks deployments, so that attackers can be distracted from the real target. In this paper, we present a novel mechanism leveraging SDN and NFV aimed to autonomously deploy and enforce IoT honeynets. The system follows a security policy-based approach that facilitates management, enforcement and orchestration of the honeynets and it has been successfully implemented and tested in the scope of H2020 EU project ANASTACIA, showing its feasibility to mitigate cyber-attacks.

Index Terms

Cybersecurity, IoT, Honeynet, SDN, NFV, Security Policies

I. Introduction

The Internet of Things comprises billions of heterogeneous devices interacting each other and generating enormous assorted data traffic. Constrained IoT devices strives to perform their tasks in potential hostile environments, whereby security and privacy aspects are even more difficult

to address with hardware limitations in terms of computational power, memory and battery. Besides, the low-power wireless connectivity, Machine-to-Machine (M2M) interaction models, low-cost and unattended deployments, as well as the pervasive and dynamic environments sparks new security and privacy threats. Diverse types of evolved cyber-attacks such as for instance, distributed deny of service (DDoS) attack that are making use of infected IoT bots (e.g. mirai), are starting to appear in IoT [1].

To address this new kind of IoT-based cyber-attacks, diverse scalable security mechanisms and strategies are emerging to mitigate them [2]. In this regard, honeynets can be used to help countering cyber-attacks in IoT. Honeynets are comprised of a network of honeypots, which aim to be used as baseline to detect cyber-attacks (e.g. botnets) and to learn about attackers behaviors, making them believe that they are accessing to the real network, when they are in fact, accessing to a simulated, controlled and isolated network.

A highly-interaction honeypot (HIH) honeynet can imitate the activities of the production network, by hosting a variety of honeypots and services, to which an attacker is redirected to access to make him wasting his time. This can give some extra time for the real system to take proper reaction and countermeasures in order to mitigate cyber-attacks and learn for future attack attempts. HIHs can capture not only the network activity, but also the system activity. However, HIHs can increase resource consumption in large-scale deployments. Honeynets, and in turn, honeypots, are not subject to deploy and implement all the services and functionalities of the production system. Indeed, honeypots usually provide simulations of only certain services to reduce maintenance cost. Unlike HIH, low-interaction honeypots (LIH) simulates only part of the network and services. So far honeynets have been studied and applied successfully mainly for protecting traditional distributed networks and systems, such as Cloud and Grid infrastructures and services. However, their application to the Internet of things has not yet paid enough attention.

, configure, generate and enforce virtual honeynet is a complex and tedious task, that becomes even more complex, when the honeynet needs to be adapted on demand to the pervasive network environment. Therefore, it is necessary to devise an automated framework to configure, deploy and manage a flexible honeynet. In this paper, we present an autonomic virtual IoT honeynet deployment mechanism that relies on NFV for orchestration. The use of Network Function Virtualization (NFV) for honeynets management enables an efficient way of deploying virtual HIH, empowering dynamic configuration and reconfiguration while maintaining the HIH configuration equivalent to the real IoT environment deployed in production.

Since an IoT network is composed of different sensor nodes, commonly equipped with a special kind of Operating Systems, such as Contiki OS [3], specially customized for constrained IoT devices, our proposal is able to set up virtual IoT honeynets on demand, not only as a proactive measure but also as a reactive countermeasure to mitigate cyber-attacks, emulating a real IoT network of sensors to which the attacker is redirected. In our proposal, data and control plane of the honeynet are managed in a centralized way through an Software Defined Networks (SDN) architecture. The SDN controller is in charge of providing traffic filtering and forwarding capabilities, as well as a redirection mechanism to divert traffic connections between the real IoT environment and the virtual one. To the best of our knowledge, this is the first attempt to define a mechanism to dynamically deploy virtual IoT honeynets through SDN and NFV, that can emulate a real physical IoT network of devices.

The proposed system has been designed as part of a holistic cyber-security framework that is being developed in the scope of ANASTACIA EU research project [4]. The ANASTACIA framework follows a context-awareness approach that can provide support for decision-making, thanks to the continuous analysis of the network situation provided by the monitoring module. It endows the system with on-demand dynamic deployment and update of honeypot services for the virtual IoT honeynet.

The rest of the paper is organized as follows: Section II discusses the state of the art. Section III introduces the general ANASTACIA security framework. Section IV delves into the proposed solution for virtual IoT honeynets dynamic deployment through SDN-NFV. Section V describes the implementation performed for the autonomic deployment of the virtual IoT honeynets. Section VI reports the experimental results to enforce virtual IoT honeynets through SDN-NFV. Finally, Section VII concludes the paper with a set of final remarks and presenting future research lines.

II. Related work

A. SDN-NFV related work

To achieve confidentiality, integrity and availability with self-healing, and self-repair capabilities in wireless environments, new context-aware and autonomic softwarized frameworks, such as SELFNET [5] focused on 5G networks, and ANASTACIA targeting IoT networks [6] are starting to emerge.

These frameworks are inspired by SECurity-as-a-Service (SECaaS) [7] approach, that enables dynamic management of security mechanisms in virtualized and softwarized environments. SDN and NFV can play key roles to leverage virtual security solution aimed to face the increasing IoT threats [8], since they provide many advantages to deploy and dynamically migrate security countermeasures within networks. Indeed, SDN introduces a set of new features that can be leveraged to provide security: (i) programmability, to enable dynamic deployment of virtual network secure zones; (ii) visibility of the whole network on the control plane, to simplify the monitoring and detection of distributed attacks; (iii) dynamic flow control, providing more flexibility in the implementation of access control functions for security reactions.

Some research efforts have already proposed models for virtualized security services [9]. Bull et al [10] propose several examples of security applications using SDN, whereas the feasibility of deploying various SDN-based security functions has been investigated in [11]. Another survey [12], is focused on SDN strengths and weaknesses against Distributed Denial of Service (DDoS) attacks in cloud computing environments, topic that is also treated by Choi et al. [13], which suggest a network architecture where DDoS protection is carried out by limitation of the amount of flow allowed for the same application per data source.

Regarding SDN in IoT, Xu et al. [14] describe an smart security mechanism to defend against new flow attacks in SDN-based IoT by using a dynamic access control prior adding new flows to the SDN-switch. This type of attacks relies on sending packets that are going to be forwarded to the SDN controller in order to produce a DDoS attack therein. A secure SDN IoT network architecture, BlackSDN [15], is proposed to increase protection of IoT communications by encrypting both meta-data and packet payload, using an SDN controller as a trusted third party. Furthermore, NFV allows for on-demand deployment of virtual security functions within network, thus allowing security function to be deployed in the appropriate place, avoiding then traffic rerouting currently happening in classical approaches. Authors in [16] propose the use of an SDN gateway as an architectural decision to allow the monitoring of traffic originated from and directed to IoT devices, enabling the detection of anomalous behaviour and then, performing an appropriate response (blocking, forwarding, or applying Quality of Service). Choi et al. [17] propose strategies for establishing a security framework based on a software-defined IoT environment and efficient provision of security services such as authentication, access control, and lightweight encryption. The aforementioned works do not exploit the NFV benefits to increase on-demand scalability and dynamic deployment of virtual security functions within the network.

The joint use of SDN and NFV security features for IoT is currently at a preliminary stage and significant efforts are still required to fully exploit their benefits. Furthermore, the integration with existing security solutions, especially for IoT, is still missing. To this aim, ANASTACIA EU H2020 project [4] [18] is devising a policy-based security framework for IoT deployments, capable of taking autonomous decisions, making use of SDN and NFV to provide dynamic security enforcement based on monitoring methodologies and tools.

B. HoneyNets related Work

The dynamic deployment of honeynets has been already studied in the past. Hecker et al. [19] proposed a dynamic approach that is capable of setting up LIH with the combination of both, passive scanning that listens the network traffic, and active scanning, that injects additional traffic in the network to obtain a more complete assessment of the network. Guerra et al [20] also describe a low interaction virtual IoT Honeypot which simulates 4 common IoT devices: camera, printer, video game console and cash registering machine. While defeating scanning, by providing wrong OS information, the rest of the attack cycle is redirected in a wrong way since the gathered information is not correct, that it turns the attack unsuccessful. Our goal is similar, however, our paper is intended to deal with HIH honeynets, rather than LIHs.

multi-purpose IoT honeypot was studied in [21], aimed to analyze some of the existing attack patterns on IoT systems, and design a honeypot for IoTs that can handle attacks, capturing attacks coming through four channels: Telnet, SSH, HTTP and CWMP. The captures are then analyzed to find common patterns and gain intelligence.

Regarding HIH, SIPHON [22] proposes a High-Interaction physical honeypots, that aims to adapt Honeypots for improving the security of IoTs. They leveraged IoT devices that are physically deployed and connected through wormholes, which are appealing for attackers and distributed around the world. Besides, in [23], authors analyse the rise of honeypot sandboxing analyzing Telnet-based attacks against various IoT devices running on different CPU architectures and captures malware examples.

Taking advantage of SDN capabilities, Wonkyu Han et al. [24] proposed a SDN-based intelligent honeynet called HoneyMix, which leverages the rich programmability of SDN to circumvent attackers detection mechanisms and enables fine-grained control of the data path. HoneyMix establishes multiple connections with a set of honeypots and selects the most desirable connection to inspire attackers to remain connected.

Some of the previous references provide an important contribution about particular IoT honeypots solutions. However, unlike them, this paper focuses on HIH honeynets that might replicate the whole IoT network, not only a particular IoT Honeypot. In that sense, deploying honeynets in a virtual environment [25] brings many benefits (e.g., maintenance) that a deployment in a physical environment cannot provide. Traditional virtualization technologies such as Kernel-based virtual machines (KVM), and lightweight alternatives such as Linux containers (LXC) [26] have been considered for the dynamic virtual deployment of the honeynets. However, they have not been applied broadly in Internet of Things.

W.Fan et al. [27] proposed a versatile framework for honeynet deployment to investigate the attacker's behavior. Although it is an important advance beyond the state of the art, their framework does not rely on NFV-SDN and their envisaged honeynets are not intended to cover IoT scenarios, and also the framework is not managed by means of security policies. In addition, their honeynets are mainly employed for investigating the attacker, whereas our research focused also on using the honeynets as Virtual Network Security Function (VNSF), which allows applying dynamic and timely countermeasures to mitigate cyber-attacks, as part of a broader autonomic security framework that deals with the security in cyber physical system (CPS) and IoT scenarios.

Finally, Gen-III honeynets [28] introduced honeywall to enable transparent network monitoring by provisioning layer-2 bridging, which is difficult for attackers to detect. However, Gen-III honeynets are providing coarse-grained data control, which can be solved through SDN paradigm as proposed by [29]. In such a paper, authors proposed an SDN architecture for hybrid honeypot systems that uses a transparent TCP connection handover mechanism to redirect traffic between honeypots, providing traffic filtering capabilities based on alerts generated by Snort intrusion detection system (IDS). In a similar way to our proposal, they react against the attack and divert traffic using SDN, but they do not make use of NFV and their honeynets are not intended to virtualize IoT networks.

Table I shows a comparison of the analyzed solutions focused on the level of interaction, the target (honeypot or honeynet), whether the solution is related to IoT, whether it follows a policy-based, SDN-based or NFV-based approach, whether it provides dynamic deployment, and if the solution has been properly implemented and validated. As it can be seen, there were not yet available a solution like the proposed herein, able to deploy dynamically IoT specific honeynets, with a high-level of interaction, though SDN, NFV and security policies, which in addition, has been properly validated.

Solution	Int. level	Target	IoT	Policy-b	SDN-b	NFV-b	Dyn. dep.	Impl./Val.
Hecker et. al [19]	Low	Honeynet	NO	NO	NO	NO	NO	YES
HoneyIo4 [20]	Low	Honeypot	YES	NO	NO	NO	NO	YES
Krishnaprasa [21]	High/Low	Honeypot	YES	NO	NO	NO	NO	YES
HoneyMix [24]	High/Low	Honeynet	NO	NO	YES	NO	NO	NO
Guarnizo et. al [22]	High	Honeypot	YES	NO	NO	NO	NO	YES
IoTPot [23]	High/Low	Honeypot	YES	NO	NO	NO	NO	YES
Provos et.al [25]	Low	Honeynet	NO	NO	NO	NO	NO	YES
Memari et.al [26]	High/Low	Honeynet	NO	NO	NO	NO	NO	YES
Fan et. al [27]	High/Low	Honeynet	NO	NO	NO	NO	NO	YES
Fahim H. et al [28]	Low	Honeynet	NO	NO	NO	NO	NO	YES
Proposed model	**High**	**Honeynet**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

TABLE I: Honeynet SOTA Comparison

III. Security framework overview

A. Architecture overview

The envisioned security framework aims at exploiting the features of SDN/NFV-based security enablers to ensure self-protection, self-healing, and self-repair capabilities in IoT systems, complementing conventional security approaches. To this aim, security policies are defined according to different level of abstraction, to ensure higher flexibility and manage security control over heterogeneous networks. The required security actions can be enforced in different kinds of physical and virtual appliances, including both IoT networks and softwarized networks.

The proposed architecture includes three main planes, as shown in Figure 1.

1) User Plane: The administrator plane provides interfaces and tools allowing administrators to specify the desired security policy definitions. Its policy editor provides an intuitive and user-friendly tool to configure security policies in a high-level security language, governing the configuration of the system and network, such as authentication, authorization, filtering, channel protection, and forwarding.

2) Security Orchestration plane: The Security Orchestration plane enforces policy-based security mechanisms and provides run-time reconfiguration and adaptation of security enablers, thereby providing the framework with intelligent and dynamic behavior. It is an innovative layer of our architecture that provides dynamic reconfiguration and adaptation in case of deviation from the expected behaviour.

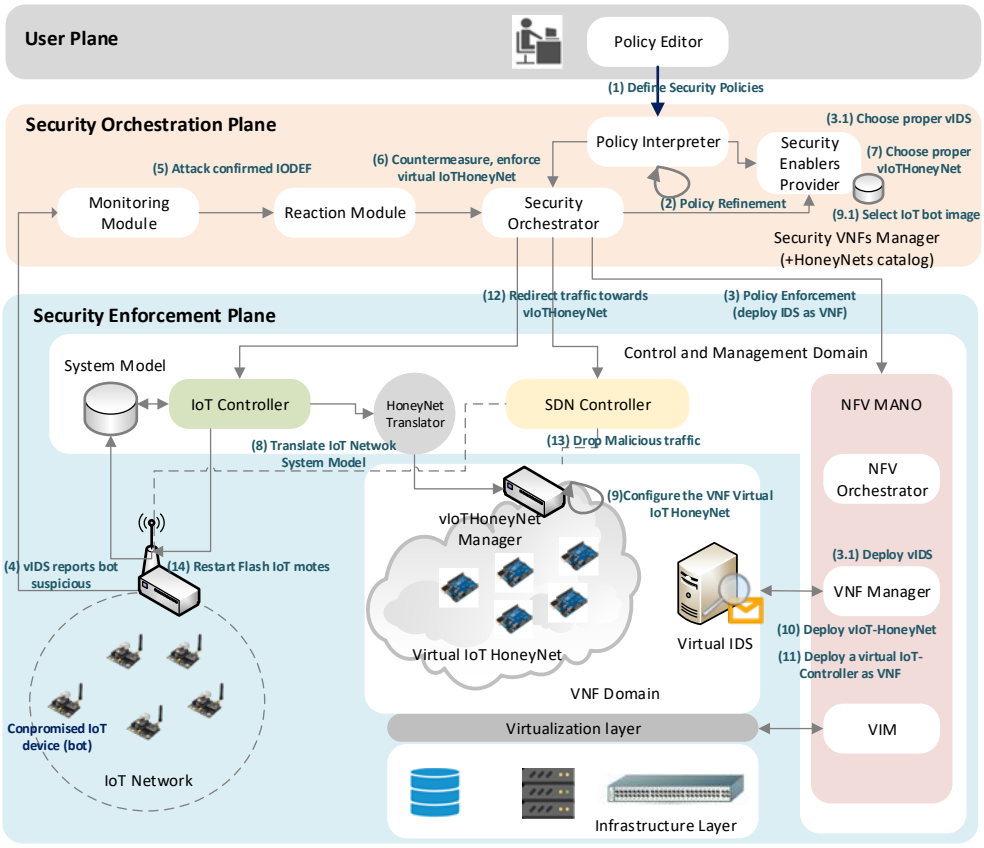


Fig. 1: High level overview architecture

The *Policy Interpreter* module plays a key role in the refinement of security policies. The high-level policies are first refined into medium-level security policy language, which allows to specify workflows related to security procedures in a technology-agnostic way. Then, these policies are translated into specific low-level configurations according to the selected enablers. The policy refinements process are further detailed in Section IV-C.

The *Security Enablers Provider* identifies the available security enablers according to the required capabilities and their relevant resource requirements. It also manages the security enabler plugins which implements the translation to low-level configurations.

The *Monitoring* component collects security-focused real-time information related to the system behavior from physical/virtual appliances. Its main objective is to provide alerts for the reaction module in case something is misbehaving. Security probes such as Intrusion Detection Systems (IDS) as well as flow and resource monitoring probes are deployed into the SDN, NFV and IoT infrastructure domains to support the monitoring services.

The *Reaction* component is in charge of providing appropriate countermeasures, e.g., by selecting policies stored in the relevant repository and by requiring reconfiguration of the security enablers to cope with the detected threat.

The *Security Orchestrator* supervises the orchestration of the security enablers to be deployed into the Security Enforcement Plane according to the policy requirements. In addition, at run-time, it analyses the reaction outcomes and orchestrates the corresponding countermeasures. In this way, the overall framework aims to achieve self-healing and resilience capabilities, by constantly ensuring the satisfaction of the security requirements defined in the end-user policies.

3) Security Enforcement Plane: The security enforcement plane is divided in different domains. The *Control and Management domain* supervises the usage of resources and run-time operations of security enablers deployed over software-based and IoT networks. A set of distributed SDN controllers takes charge of communicating with the SDN-enabled network elements to manage connectivity in the underneath virtual and physical infrastructure. NFV ETSI MANO-compliant modules provide support for the secure placement and management of virtual security functions over the virtualized infrastructure. As the envisioned framework aims to cover legacy IoT scenarios, different IoT controllers can be used to manage IoT devices as well as low power and lossy networks (LoWPANs). These IoT controllers are usually deployed at the network edge (e.g., gateways) to enforce security functions in heterogeneous IoT domains.

The *Infrastructure and Virtualization domain* comprises all the physical machines capable of providing computing, storage, and networking capabilities, as well as the virtualization technologies, to provide an Infrastructures as a Service (IaaS) layer. This domain also includes the network elements responsible for traffic forwarding, following the SDN controller rules, and a distributed set of security probes for data collection to support the monitoring services.

VNF domain accounts for the VNFs deployed over the virtualization infrastructure to enforce security within network services. Specific mechanisms will be developed to verify the trustworthiness of VNFs and to continuously monitor their key parameters, as well as specific attentions will be addressed to the provisioning of advanced security VNFs (such as virtual firewall, IDS/IPS, channel protection, etc.), capable to provide the defense mechanisms and threat countermeasures requested by security policies (e.g., the virtual IoT honeynet (vIoTHoneynet) Manager in charge of controlling the vIoTHoneynets, will be deployed as VNF).

IoT domain comprises the IoT devices to be controlled. This includes the security enablers, actuators or software agents needed to enforce the security directives coming from the orchestration

plane and managed at the enforcement plane by the IoT Controller. For instance, a special kind of local security agent can be deployed in IoT devices to protect the communications between two devices.

IV. Policy-based deployment of IoT honeynets based on SDN-NFV

A. Virtual IoT honeynets

Our proposal simulates a real IoT sensors' network to which the attacker is redirected to be distracted and investigated, countering the damage of his attack. Unlike traditional solutions, in our proposal, honeynets can be deployed not only pro-actively, but also reactively, as a countermeasure to mitigate cyber-attacks, according to the reaction provided by reaction module. Besides, connectivity and data control in the honeynet is managed centralized through SDN. The SDN controller is in charge of providing traffic filtering and forwarding, as well as a redirection mechanism to divert and transfer the traffic connections from the real IoT network to the virtual IoT honeynet, according to the necessities of intrusion investigations.

The honeynets definition in terms of network and service topologies evolve dynamically according to the context and the actual IoT physical deployment. To this aim, the system model is kept up to date, fed through monitoring services by probe modules such as IoT crawlers, IDS, FlowMon, notifications, etc., in charge of generating automatically the description of the honeynet by scanning the target production network, whereby obtaining the necessary system and network data such as, IP address, operating system, services and open ports. Once the information has been properly gathered, honeynets are modeled using an extended version of the Technology Independent Honeynet Description Language (TIHDL) [30] which, in turn, inherits from the Common Information Model (CIM) [31]. Our honeynet description model improves TIHDL by including additional concepts needed for modeling IoT virtual honeynets, such as, physical location of the devices, resources provided by the IoT devices, and so on, as it is defined in section IV-B.

By using a well-defined model as the TIHDL extended one, it can be analyzed and translated in order to transform the model information in configurations for virtual environments. For instance, the Cooja [32] simulator for wireless sensor networks enables a holistic high interaction simulations for the Contiki [3] operating system of IoT devices. Cooja allows simulations at network level, operating system level, and machine code instruction set level, enabling the deployment of virtualized HIH honeynets. When the virtual environment configuration is ready

to be deployed, a vIoTHoneyNet Manager is installed in an Virtual Network Function (VNF), and it is deployed dynamically by the NFV-MANO. In this sense, the Honeynets deployment can be performed at the proper network location to protect users against the cyber-attack.

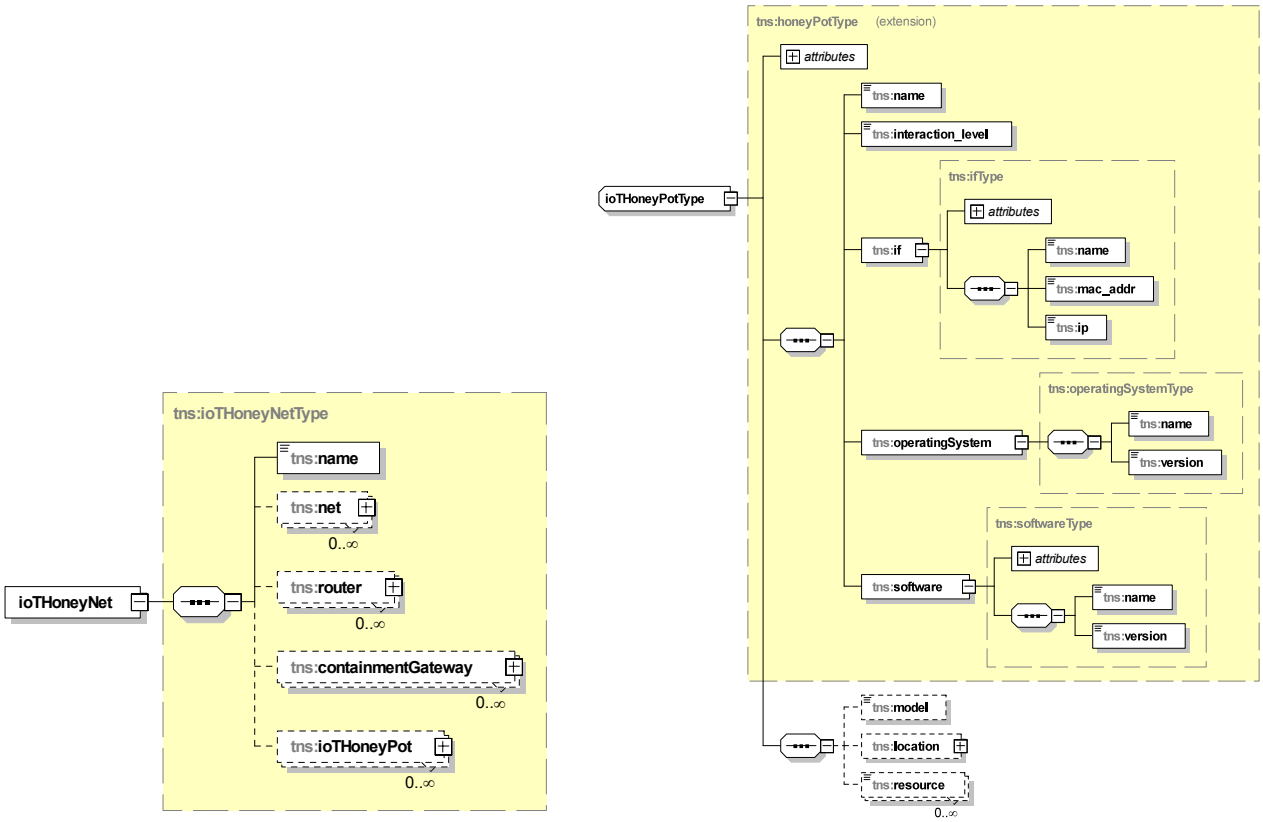
Once the VNF has been deployed, the virtual IoT devices in the honeynet start simulation sensor values, randomly generated in the scope of some margins, given by the standard deviation over the mean values that the real IoT system was reporting so far. Besides, the system is designed to offer capabilities for reconfiguring the scenario. The probe module collects in real time updates from the real production network, adjusting the network structure of the virtual honeynet accordingly. Furthermore, the framework is designed to continuously monitor the real IoT devices in order to extract information to be used to provide a HIH of the IoT honeynets, so that in case of an infected device is detected an alert and reaction is raised generating then a dynamic up-to-date virtual IoT honeynet deployment with the updated IoT honeypots.

B. Virtual IoT honeynets data model

The context information maintained and managed by the System Model database of the *Control and Management Domain* layer of the framework provides meta-model data needed to interpret the concepts expressed in the high-level security policy language. The Context Information encompasses the environmental information retrieved from the security enforcement plane.

The monitored information, along with the real time instantiated system model is defined in a common language such as CIM (Common Information Model) [31] from DMTF. CIM provides a modelling mechanism to represent concepts available in IT domains. Indeed, some operating systems and platforms already support retrieving the current and instantiated status of the system in CIM model, providing detailed information about the managed system. This description can be used to retrieve information about which capabilities are provided by different system components, as well as particular network configurations, in order to perform the policy refinement from high-level security policy to medium-level policy language. The DTMF also provides other standard models to represent specific components of the underlying virtual environment, such as OVF, VMAN, CIMI and hardware infrastructure (e.g. SMASH, Redfish). For example, a packet filtering policy should be applied by a firewall element which has network traffic filtering capabilities, and the needed of extra information such as network IP addresses associated to a user or a device identifier can be obtained from the instantiated system model.

Nonetheless, CIM does not directly provide concepts for representing honeynets. To fill this gap, the Technology Independent Honeynet Description Language (TIHDL) [30] extends CIM allowing to represent flexible virtual honeynet models, which can comprise a combination of heterogeneous platforms for deploying honeynet in virtual networks and also deploy hybrid honeynet for both, low-interaction honeypots and high-interaction honeypots. However, TIHDL was not designed having Internet of Things in mind. Several concepts need to be added, and some others re-designed, in order to model properly vIoTHoneynets. To this aim, our proposal extends TIHDL to represent several concepts needed to deploy vIoTHoneynets. Fig. 2a represents the root concepts in a Honeynet class.



(a) Virtual IoT HoneyNets system model

(b) Virtual IoT HoneyNets system model. IoT HoneyPot class

Fig. 2: IoT HoneyNets system data model schema

Every *IoTHoneyNet* is comprised of several *Nets, Routers, Honeypots* and *ContainmentGatways*. The *ContainmentGatway* class aims to represent honeywalls and their interfaces. Notice that, although it has omitted in the model for the sake of simplicity, the classes inherit from al-

ready existing classes in CIM. For instance, *Router* and *HoneyPot* extends from *ComputerSystem*, and *Interface* inherits from *NetworkPort*.

The *IoTHoneyPot* class is represented in Fig 2b. A honeypot in IoT needs special attributes that are not needed in traditional honeypots. For instance, IoT honeypots can be placed in wireless devices which are deployed in a particular location. To represent this notion, the *IoTHoneyPot* class features the attribute *Location*. Besides, an IoT device usually is endowed with several supplied sensors and *resources* (e.g. temperature). In addition, the particular *model* of the IoT device (e.g. Sky mote) is also important to be able to instantiate highly-interactive virtual honeypots.

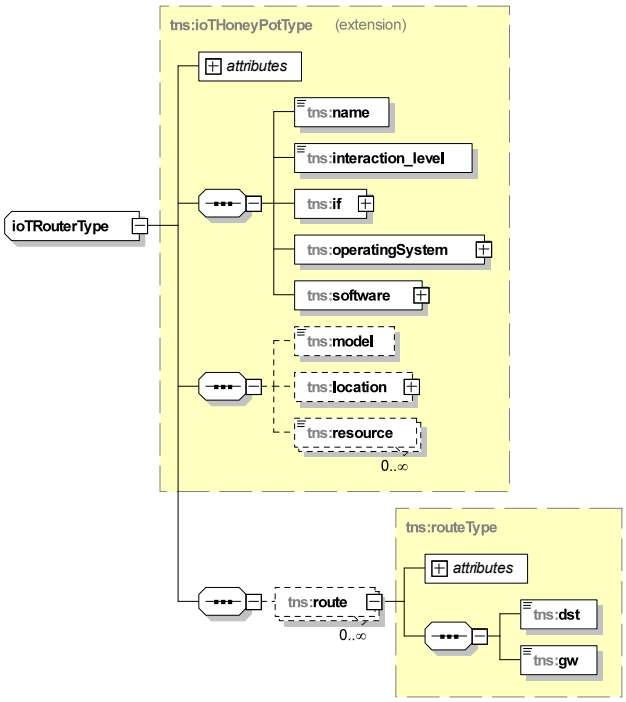


Fig. 3: Virtual IoT HoneyNets system model. Router class

The rest of the classes related to the *IoTHoneyPot* encompasses: *Interfaces* (Mac, IP, net), the *InteractionLevel* (low or high-interactive honeypot), *OperatingSystem* (e.g. Contiki) and *Software* deployed in the honeynet (e.g., Erbium).

Finally, the *IoTRouterType* is represented in the diagram of Fig. 3. IoT networks can be comprised of multi-hop wireless networks in which the IoT devices can act as routers to deliver the packet to the next hop. As in the *IoTHoneyPot* class, the routers also need to represent concepts such as *model*, *location* and *resource*. Besides, the *Router* class holds the routing table

with the set of entries (destination-gateway) needed to represent accurately, in the vIoTHoneyNet, the same network topology than in the real physical IoT network. Moreover, the *Router* class is associated to a particular software of routing protocol (e.g., RPL). Modeling these concepts will allow to configure the vIoTHoneyNet exactly as it is the the real IoT deployment.

C. Policy-based security management in SDN/NFV-enabled networks

IoT deployments are comprised of disparate kind of devices which might differ a lot in the available resources, implemented protocols, or connectivity technology employed. Besides, some domains are prone to receive more attacks than others and the level of criticality varies among deployments, thereby changing the economic or strategic interest from attackers. Consequently, different security requirements might apply to different IoT deployments. The security refinement process defined herein is based upon a policy based strategy for the enforcement and management of security requirements over an IoT platform providing interoperability and avoiding vendor lock-in. Security policies are a flexible way to tailor the security requirements needed by an IoT platform to the specific domain where the IoT platform is deployed. Them also ease the security management activities required to control the fulfillment of the claims included in the policy, allowing to set up monitoring activities, measurements, thresholds, alerts, reaction activities, etc.

In this way, security policy operations are divided into three main tasks. Namely, the process that parses the high level policy into a machine readable format (policy refinement), the transformation of that policy format into low level configuration rules (policy translation) and the process for configuring the system (policy enforcement). The sequence diagram of Fig. 4 shows the main workflow for a proactive policy definition and its refinement from High-level Security Policy Language (HSPL) to Medium-level Security Policy Language (MSPL) based on [33], as well as the policy translation process from MSPL to low-level configurations.

First, the security administrator defines the security policy in HSPL (Fig. 4-step 1). Then, the Policy Interpreter receives a policy enforcement request, starting the refinement process by the identification of the capabilities (Fig. 4-step 3), understanding a capability as a main purpose of the policy (e.g., filtering capability will be identified when a security policy is defined in order to drop traffic).

Once the Policy Interpreter has identified the capabilities, it performs a request to the Security Enabler Provider (Fig. 4-step 4), with the aim to get a list of Security Enablers capable to enforce the mentioned capabilities. In this context, a Security Enabler corresponds to a piece

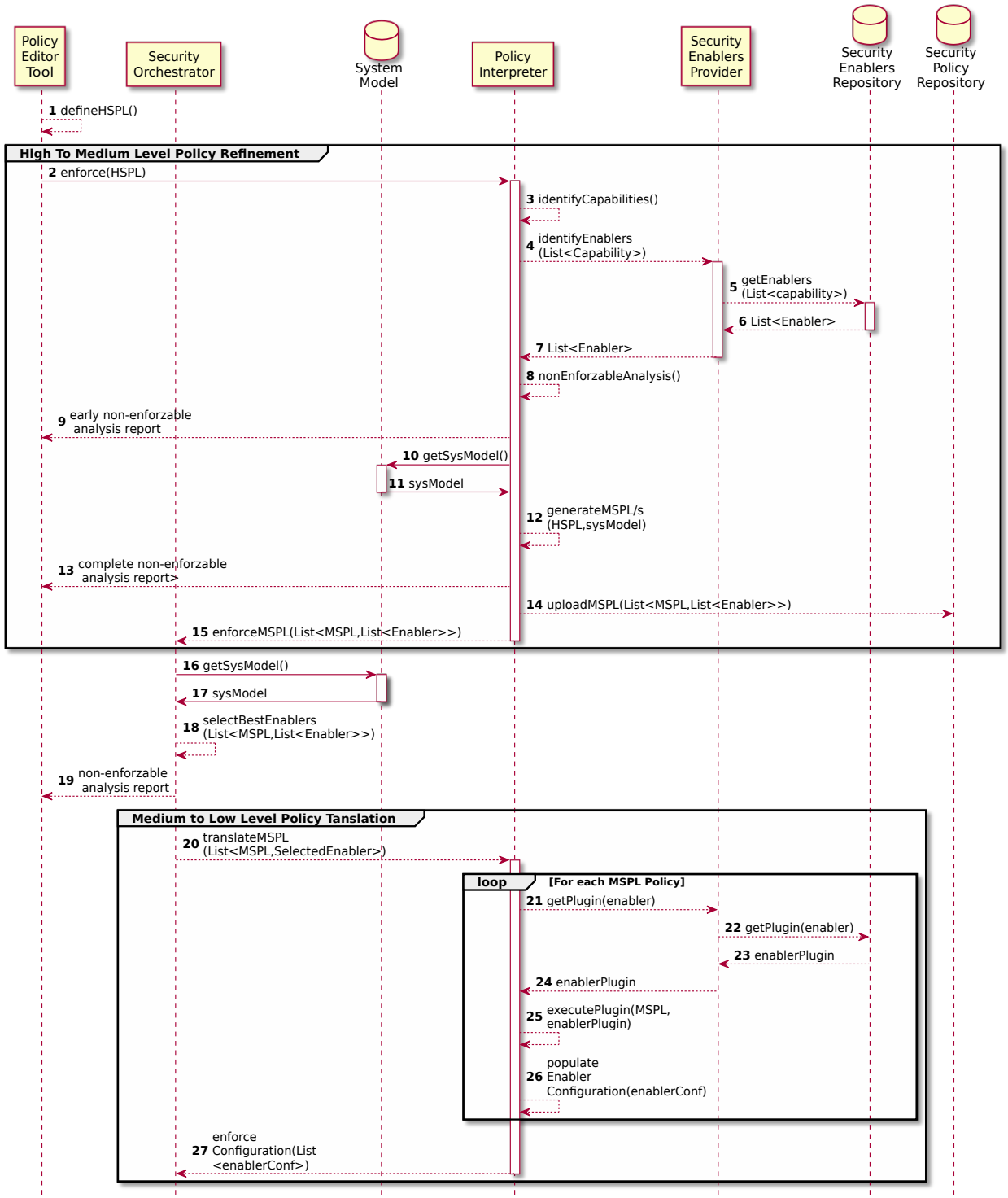


Fig. 4: Policy Refinement and Policy Translation processes

of software or hardware capable to implement some specific security properties (e.g., filtering, forwarding...). The Security Enabler Provider then returns the aforementioned list of Security Enablers for each capability. Afterwards, the Policy Interpreter verifies whether each security policy could be enforced using at least one of the Security Enabler received (Fig. 4-step 8).

If the security policy could not be enforced, the Policy Interpreter returns a non-enforzable analysis to the user, indicating the issue (Fig. 4-step 9). Otherwise, the Policy Interpreter retrieves system model information (e.g., technical information of an IoT device) and it performs the policy refinement taking into account the capability of the HSPL policy as well as the specific system model information in order to generate one or several (e.g., bi-directional behavior) MSPL policies (Fig. 4-step 12). Like in the previous case, if there is some issue during the refinement, the user is notified with a non-enforzable analysis but, in other case, the MSPL policy and the list of available security enablers are uploaded to the Security Policy Repository and they are also sent to the Security Orchestrator in order to proceed with the best security enabler selection for the medium-level security policy translation process (Fig. 4-steps 14,15).

When the Security Orchestrator receives the MSPL policy and the list of security enablers, it retrieves information about the underlying technologies in order to select the best security enabler for the policy enforcement by using the current context and system information to make the decision (Fig. 4-steps 16,17,18). Then, the Security Orchestrator requests the MSPL translations to the Policy Interpreter for each pair of MSPL and selected security enabler. The Policy Interpreter retrieves from the Security Enabler Provider the plugin which implements the MSPL translation for the selected security enabler, and executes it, generating the expected low-level configurations (Fig. 4-steps 21-27), which are sent to the Security Orchestrator (Fig. 4-step 23) who proceeds with the enforcement process.

Fig. 5 shows the policy enforcement process. The Security Orchestrator receives the enablers configuration and it triggers the enforcement process through the SDN Controller, the IoT Controller, the NFV MANO (Fig. 5-steps 1,2,3) or even by a direct communication with the security enabler (e.g., legacy physical router), depending on the requirements of the security policy. On the one hand, if a specific VNF is required, and it is not already deployed, the NFV-MANO creates, configures and deploys a new one (Fig. 5-steps 6,7). Otherwise the NFV-MANO just enforce the received configuration over the VNF. Besides, if the security policy is SDN related, the SDN Controller is in charge of enforcing the policy over the managed SDN network (Fig. 5-steps 4,8). Finally, if the security policy is IoT related, the IoT Controller

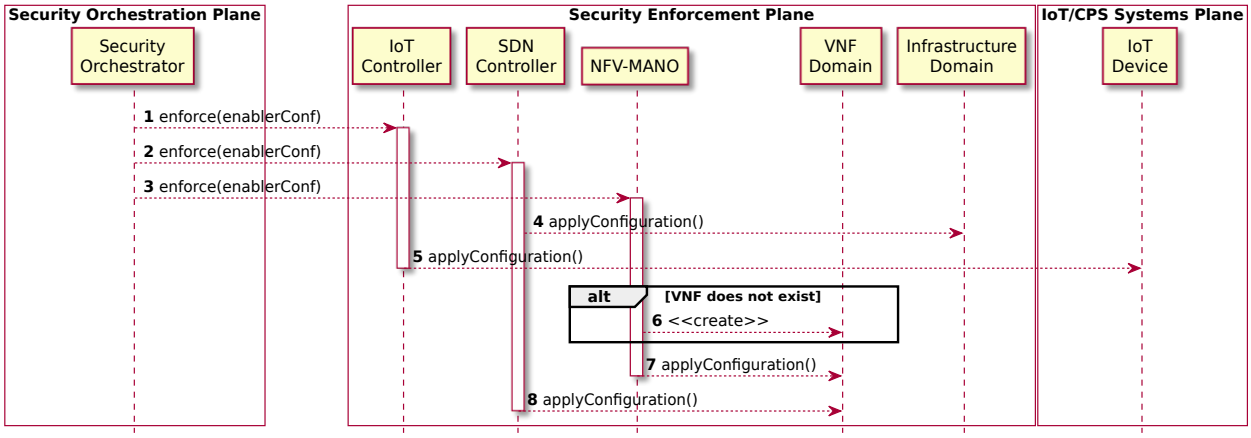


Fig. 5: Policy Enforcementj process

enforces the IoT configurations over the managed IoT devices by using specific IoT constrained protocols (Fig. 5-steps 5).

D. Attack detection and virtual IoT Honeynet dynamic configuration and deployment

By following the previous policy-based approach it is possible to define a set of pro-active security policies in order to configure and deploy monitoring agents which feeds the reaction part of the framework. Thus, the monitored data is filtered, processed and analyzed, issuing verdicts about anomalies occurring in the monitored platform (potential threats or ongoing attacks). The identified events are notified to the reaction module of the framework which creates countermeasures (i.e. a set of security policies) reacting to threats or attacks, and triggering the countermeasure's enforcement. Besides, the security reaction process is also able to notify the administrator, who might provide feedback and trigger critical countermeasures that require explicit consent or to override the security policy.

When the reaction countermeasure is performed automatically, the reaction module generates and provides a set of countermeasures as new security policies to the Security Orchestrator, which acts similar to when it receives the MSPLs from the Policy Interpreter in the pro-active scenario. Fig. 6 shows the main workflow regarding a botnet DDoS attack detection, instantiated for an IoT honeynet deployment countermeasure. First, a previously deployed IDS VNF detects the signature of DDoS attack of the botnet (e.g., Mirai) (Fig. 6-steps 1,2). The infected zombie (bot) in the IoT domain can be detected based on flow-based metrics, which are sent to ANASTACIA monitoring module for further analysis. The Monitoring module analyzes

the thread and communicates the alert (e.g. IODEF) to the reaction module (Fig. 6-step 3,4), which is in charge of making the decision regarding the particular kind of countermeasure to be taken. In this case, the reaction module indicates that IoTHoneynet and networking operations that must be enforced, so it requests the enforcement of the countermeasures to the Security Orchestrator (Fig. 6-step 6).

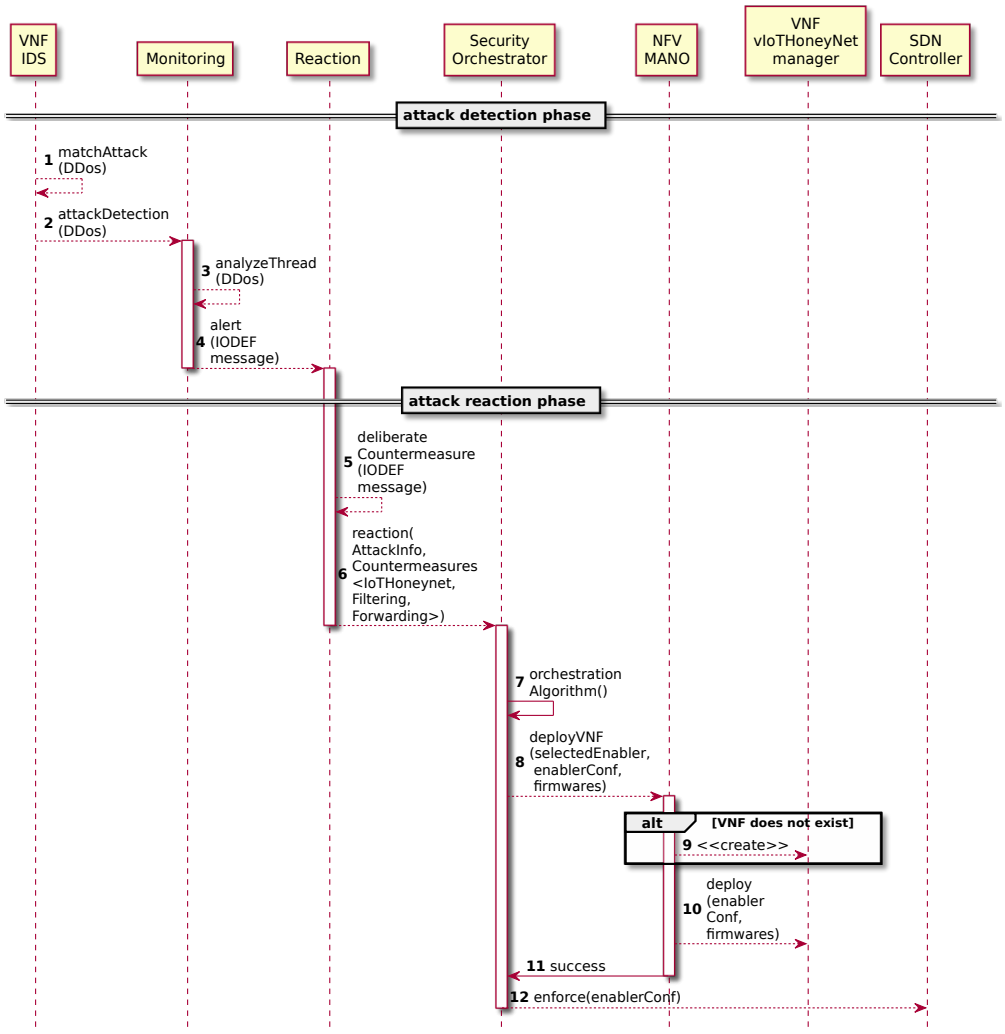


Fig. 6: IoTHoneyNet deployment process

The Security Orchestrator receives the attack information as well as countermeasures (which could be security policies pending to be fulfilled) and it executes the orchestrator algorithm (Fig. 6-step 7). Algorithm 1 shows the pseudo-code of orchestration algorithm.

```
Data: AI = attackInfo, C = {countermeasuresList}
Result: EnforcedC' ⊂ C
for c in C do
    if c has unsatisfied dependencies then
        queue(c);
        continue;
    end
    sm ← getSystemModel(c);
    if c ⊂ {IoTContermeasures} then
        ioTsm ← getIoTSystemModel(c);
        sm ← sm ∪ ioTsm;
    end
    mspl ← fillMSPL(c, sm);
    candidates ← getEnablerCandidates(mspl);
    se ← selectEnabler(mspl, candidates, sm);
    conf ← translate(mspl, se);
    if mspl ⊂ {HoneynetMSPLs} then
        cf ← genCustomFirmware(conf, AI);
    end
    enforce(conf, se, cf) end
```

Algorithm 1: Security Orchestrator Algorithm for countermeasures enforcement

The algorithm iterates over the countermeasures verifying whether there is any unsatisfied dependency. If so, the countermeasure is queued until the dependency is solved (filtering and forwarding will depend on the vIoTHoneynet deployment). Otherwise, the algorithm retrieves system model information of the underlying technologies related to the elements involved in the countermeasure. If the countermeasure is related with IoT, the algorithm also includes in the system model the IoT infrastructure information available in the IoT Controller. The information of the infrastructure and the countermeasure are then used in order to fulfill the MSPL policy. The algorithm then retrieves a list of security enabler candidates capable of enforcing the MSPL policy, and it selects the best candidate by considering the current status of the infrastructure (system model), the candidates and the security policy requirements.

Once the best security enabler is selected, the algorithm obtains the enabler configuration by

a MSPL policy translation. If the security policy is IoT Honeynet related, a custom firmware generation could be required in order to emulate not only the current infrastructure, even the specific attack behaviour (e.g., emulate a Mirai botnet). Finally, the enabler configuration is enforced through the selected enabler (Fig. 6-steps 8,12). For the vIoTHoneynet, the NFV-MANO verifies if there is already deployed a suitable VNF which implements the vIoTHoneynet manager. If so, the vIoTHoneynet configuration is sent to the vIoTHoneynet manager who starts the vIoTHoneynet according on the received parameters. Otherwise, the process is barely the same, but the NFV-MANO first creates a suitable VNF instance for the vIoTHoneynet manager.

When the vIoTHoneynet is running, the Security Orchestrator receives a notification from the vIoTHoneynet agent, which verifies whether the event satisfies any queued countermeasure. If so, it process and enforces the filtering and forwarding policies through the SDN controller in a transparent way for the attacker. On the one hand, the traffic from the real IoT domain to the attacker as well as the traffic from the real IoT domain which is generating the DDoS attack are filtered. On the other hand, the traffic from the attacker to the real IoT infrastructure is redirected to the vIoTHoneynet and the simulated DDoS generated by the vIoTHoneynet is also filtered. In this way the attacker believes he is still controlling the affected bot device, but the attack is unsuccessful and the process allows security administrators take advantage of the situation (e.g., learning the attacker methodology).

V. Implementation

Figure 7 shows the deployment that has been instantiated, based on the developments carried out in the scope of this research in order to perform the testing of the proposed architecture. The monitoring module is instantiated using the XL-SIEM tool, which is a Security Information and Event Manager able to detect issues along the architecture by monitoring network resources, provided by Atos. XL-SIEM is able to infer cyber-atacks by analyzing the detected anomalies. Those issues are notified to the Reaction module, providing the information in the Incident Object Description Exchange Format IODEF [34] standard. The Reaction module analyzes the threats and it generates a reaction which is sent to the Security Orchestrator in an adequate format, able to represent the coordination and execution of command and control for cyber-defense components, i.e., the Open Command and Control (OpenC2) [35] language. Once the Security Orchestrator knows the reaction, it performs the requested modifications over the architecture by using security policies. To provide policy definition, refinement, and translation features, a

Policy Editor Tool and a Policy Interpreter have been implemented in Python, based on the outcomes of the SECURED project policy models [33].

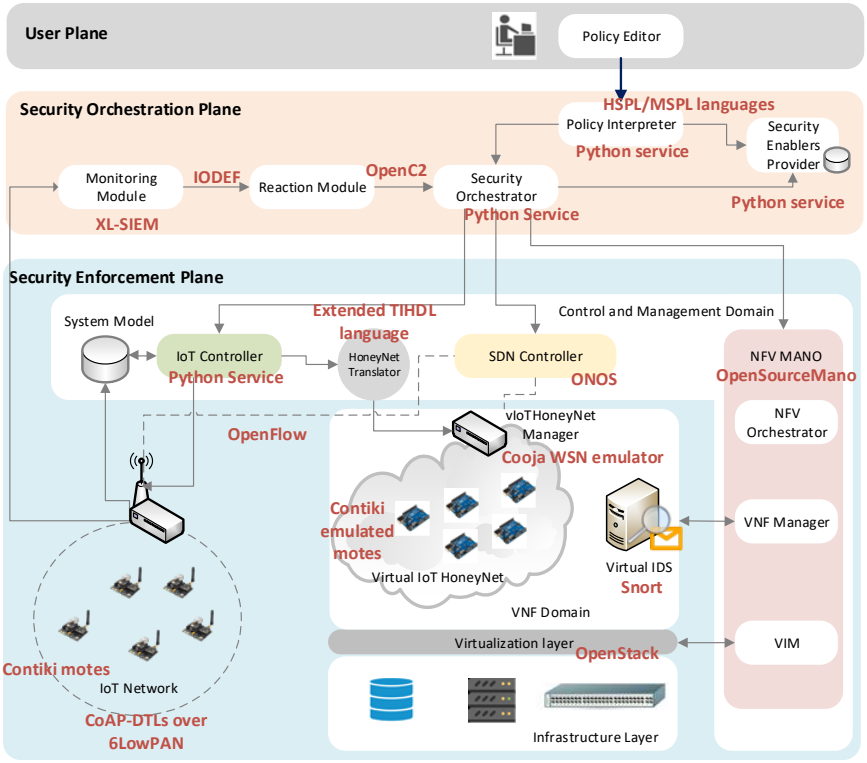


Fig. 7: Architecture instantiation and implementation

Specifically, different plugins have been implemented for the policy translation from MSPL to low-level configurations. Namely, a plugin translates MSPL IoT HoneyNet policies into Cooja emulator configurations which can be applied by the Northbound API of our vIoTHoneyNet manager. Listing 1 provides an MSPL policy example which embeds the IoT system model. The *virtualIoTHoneyNetAction* specifies the action to be performed over the honeynet (other actions such as reconfigure, stop or restart the environment could be specified), whereas the *IoTHoneyNet* model describes general information regarding the network and the honeynet itself, like identifications or descriptions. More concrete information is provided about the main elements such as *routers* and *IoTHoneyPots*, like their interaction levels (LOW, HIGH), defined as the degree of replication between the real and virtual environments, the operating system, the installed software and its version, the available resources of the IoT honeypot (e.g., temperature sensor, humidity sensor...) and even its physical location expressed in Cartesian coordinates.

```
<configurationRule>
 <configurationRuleAction xsi:type='VIoTHoneyNetAction' >
  <VIoTHoneyNetActionType>DEPLOY</VIoTHoneyNetActionType>
    <ioTHoneyNet >
      <name>REST with RPL router</name>
      <net id="1"> <name>net</name></net>
      <router id="1">
        <name>Wismote RPL Root</name>
        <interaction_level>LOW
        </interaction_level>
        <if id="1" net="str1234">
          <name>i1</name>
          <mac_addr>ROUTER_MAC</mac_addr>
          <ip>ROUTER_IP</ip>
        </if>
        <operatingSystem>
          <name>contiki</name><version>2.7</version>
        </operatingSystem>
        <software id="1">
          <name>RPL</name><version>3.14</version>
        </software>
        <model>Wismote</model>
        <location><x>33.2601</x><y>30.6432</y></location>
        <resource>TEMPERATURE</resource>
      </router>

      <ioTHoneyPot id="2">
        <name>Erbium Server</name>
        <interaction_level>LOW</interaction_level>
        <if>...</if>
        <operatingSystem>
            <name>contiki</name>
        </operatingSystem>
        <software id="1">
          <name>Erbium Server</name><version>3.14159</version>
        </software>
        <model>Sky</model>
        <location>...</location>
        <resource>Temperature</resource>
      </ioTHoneyPot>
       ...
    </ioTHoneyNet>
   </configurationRuleAction>
</configurationRule>
```

Listing 1: IoT HoneyNet Model Example

```
<simconf>
 <motetype>
  se.sics.cooja.mspmote.WismoteMoteType
  <identifier>1</identifier>
  <description>Wismote RPL Root</description>
  <source>border-router.c</source>
  <commands>make border-router.wismote
      TARGET=wismote</commands>
  <firmware>border-router.wismote</firmware>
  <moteinterface>Position</moteinterface>
  <moteinterface>IPAddress</moteinterface>
 </motetype>

 <motetype>
  se.sics.cooja.mspmote.WismoteMoteType
  <identifier>2</identifier>
  <description>Erbium Server</description>
  <source>coap-server.c</source>
  <commands>make coap-server.wismote
      TARGET=wismote</commands>
  <firmware>coap-server.wismote</firmware>
  <moteinterface>Position</moteinterface>
  <moteinterface>IPAddress</moteinterface>
  <moteinterface>TEMPERATURE</moteinterface>
 </motetype>

 <mote>
  <breakpoints></breakpoints>
  <interface_config>
   org.contikios.cooja.interfaces.Position
   <x>33.2601</x><y>30.6432</y><z>0.0</z>
  </interface_config>
  <interface_config>
   org.contikios.cooja.mspmote.
       interfaces.MspMoteID
   <id>1</id>
  </interface_config>
  <motetype_identifier>1</motetype_identifier>
 </mote>
  ...
</simconf>
```

Listing 2: Corresponding Cooja CSC model

Listing 1 shows example of MSPL and its corresponding translation into Cooja Simulation Model configurations (CSC model) as shown in Listing 2. As it can be observed, it allows specifying the type of IoT device (*motetype*), even including the source code to be compiled, or directly the IoT firmware, as well as the platform and available resources.

Besides the vIoTHoneynet configuration, additional policy enforcements must be accomplished like filtering and forwarding, in order to set-up the network to accommodate the new virtual appliance, and redirecting the attacker to the vIoTHoneyNet. In this sense, it has been developed

a plugin to translate MSPL filtering and forwarding policies to specific SDN ONOS Controller Northbound API configurations.

```
<configurationRule>
 <configurationRuleAction xsi:type='FilteringAction'>
  <FilteringActionType>DENY</FilteringActionType>
 </configurationRuleAction>
 <configurationCondition xsi:type='FilteringConfCondition'>
  <packetFilterCondition>
   <SourceAddress>aaaa::/64</SourceAddress>
   <DestinationAddress>cccc:2/128<DestinationAddress>
   <Interface>2</Interface>
   ...
 <externalData xsi:type='Priority'><value>60000</value>
    ...
</configurationRule>

<configurationRule>
 <configurationRuleAction xsi:type='TrafficDivertAction'>
  <TDivertActionType>FORWARD</TDivertActionType>
   <packetDivertAction>
    <packetFilterCondition>
     <Interface>3</Interface>
     ...
  </configurationRuleAction>
  <configurationCondition xsi:type='TDivertConfCondition'>
   <packetFilterCondition>
    <SourceAddress>cccc::2/128</SourceAddress>
    <DestinationAddress>aaaa::/64</DestinationAddress>
    <Interface>1</Interface>
    ...
  <externalData xsi:type='Priority'> <value>60000</value>
  ...
</configurationRule>
```

Listing 3: MSPL Filtering Example

```
[{"priority": 60000,
  "treatment": {
   "instructions": [{"type": "NOACTION"}]},
  "selector": {
   "criteria": [
     {"type": "IPV6_SRC","ip": "aaaa::/64"},
     {"type": "IPV6_DST","ip": "cccc::2/128"},
     {"type": "IN_PORT","port": "2"}]}},

{"priority": 60000,
 "treatment": {
  "instructions":[{"type": "OUTPUT","port": "3"}]}
 "selector": {
  "criteria": [
    {"type": "IPV6_SRC","ip": "cccc::2/128"},
    {"type": "IPV6_DST","ip": "aaaa::/64"},
    {"type": "IN_PORT","port": "1"}]}}]
```

Listing 4: ONOS Northbound Filtering Configuration Example

Listing 3 shows an example of filtering and forwarding security policies. The filtering policy indicates the traffic that goes from the real IoT deployment (*AAAA::/64*) to the attacker (*CCCC::2/128*) must be dropped. On the other hand, the forwarding policy indicates the traffic coming from the attacker to the real IoT deployment must be redirected to the interface where the vIoTHoneynet has been deployed. Listing 4 shows the configuration obtained after the policy translation process for filtering and forwarding policies using ONOS as SDN security enabler. Specifically, it provides the filtering and forwarding rules to be applied through the ONOS Northbound API.

Regarding the orchestration, it has been developed a Python application which allows to enforce the aforementioned security policies by applying the configuration or tasks to the different policy enforcement points. In the case of the vIoTHoneyNet security policy, the Security Orchestrator implementation is also in charge of obtaining the IoT physical architecture model

in a extended TIHDL format from the IoT Controller, and include it in an IoTHoneynet MSPL security policy. Once the MSPL has been generated, the Security Orchestrator gets the final Cooja configuration through the Policy Interpreter, which executes the vIoTHoneyNet plugin in order to translate the IoT system network modeled in our extended TIHDL language into Cooja configuration. Cooja has been chosen, since it allows developing the IoT device functionality in C language, customizing, compiling, loading it into the platform, and even providing the real IoT device locations in coordinates, as well as interesting parameters such as the transmission range, interference range and success ratio for LoWPANs.

Once the Cooja CSC model has been obtained, the Security Orchestrator selects the proper firmwares to replicate the real IoT behavior and it requests the deployment of the vIoTHoneyNet with the specific configuration and firmwares through the NFV-MANO. In order to deploy on demand the vIoTHoneyNet, the our vIoTHoneyNet manager implementation provides an API capable to receive the Cooja CSC model and the specific firmwares, in order to configure and execute the Cooja simulation in the VNF. When the simulation has been started and the network is ready to be reachable from outside (i.e., routing protocol algorithm has converged), the vIoTHoneyNet manager warns the Security Orchestrator, which enforces the filtering and traffic divert policies through ONOS SDN controller in order to redirect the traffic generated or received for the physical architecture to the virtual one. Besides, it drops the malicious traffic sent to the victim in order to mitigate the current attack.

VI. Performance Evaluation

The section aims to determine the feasibility of the deployment for the proposed virtual IoT honeynet mechanism. The goal is to apply an IoT honeynet security policy as reaction countermeasure to mitigate an attack in a reasonable time, deploying a virtual IoT honeynet as much realistic as possible to the real physical IoT deployment. The performance tests have been carried out by applying 100 times IoT Honeynet security policies over each of the two different sections on the Smart Building floors we are using in our premises. IoT sensors are heterogeneous in terms of sensoring capabilities and operating system version installed for each floor.

The full time of the IoT honeynet policy deployment has been split in different times to allow a fine-grain analysis, as is shown in figure 8. In the translation among the physical model to the virtual one, it is measured the time taken by translator plugin to provide the Cooja CSC

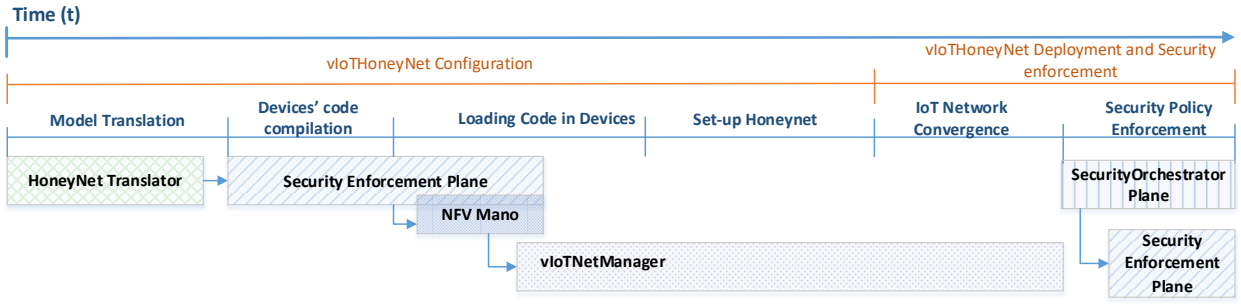


Fig. 8: Testbed measured times representation

model from the IoT HoneyNet physical model (i). For the compilation (ii) and load (iii) of the IoT devices code, it is measured the time taken to compile the code for all IoT devices and the time required to load the compiled code into the IoT devices. In addition, it is considered the overall time required by the simulation to be ready, i.e., all IoT devices are up and running (iv). In case the simulation uses a routing algorithm, the IoT network convergence time measures the time needed by the router to learn a route to all IoT devices (v). Finally, the Policy Enforcement time measures the time taken to apply the network policy configurations in order to filter and divert the traffic, as described in previous section (vi). The tests have been supported by a virtual machine with 4 CPUs and 2 GB of RAM memory. This virtual machine has been hosted in an Intel Core i7-2600 at 3.40 GHz with 8 GB of RAM memory.

Regarding the use cases, Figure 9 shows the first use case corresponding to first floor of our building, which is comprised by 20 sky motes distributed along 30x15m, executing Contiki OS 2.7, empowered by 8 Mhz, 10KB RAM and 48KB Flash, measuring humidity, temperature, light and CO2. One of them is a RFID sensor as door keeper, and finally, there is one more as a router using RPL as routing algorithm, which connects all sensors to the smart build network.

On the other hand, figure 10 shows the second floor use case which is comprised by 50 wismote motes, distributed along 37.5x15m, executing contiki OS 3.1, empowered by 16 Mhz, 16KB RAM and 128KB Flash, measuring humidity, temperature, light, presence and CO2. In this case, all doors are equipped by RFID sensors, and finally, at the same way of the previous case, there is one more as a router using RPL as routing algorithm, which connects all sensors to the smart build network.

Figures 11a and 11b s the time taken for each step in the vIoTHoneyNet policy deployment process in order to virtualize up to 50 Sky and Wismote motes respectively, without taking into

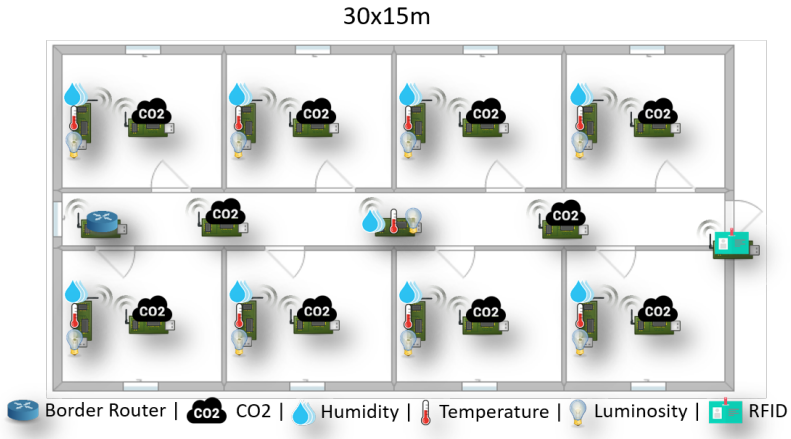


Fig. 9: Sky 20 physical distribution

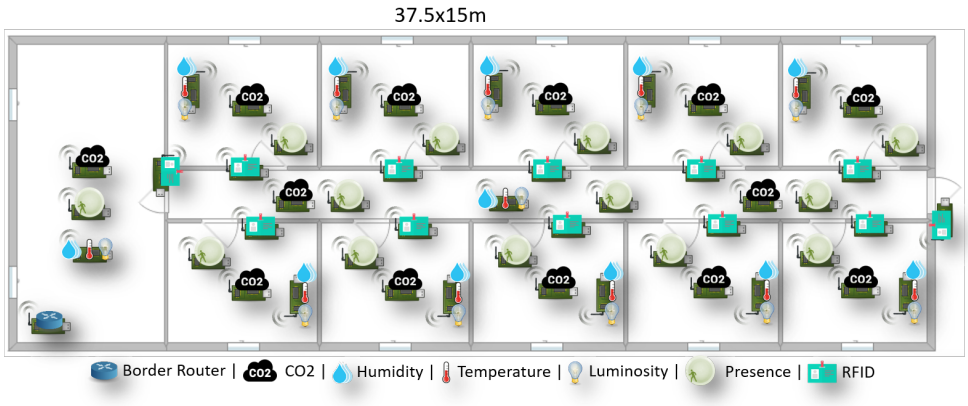
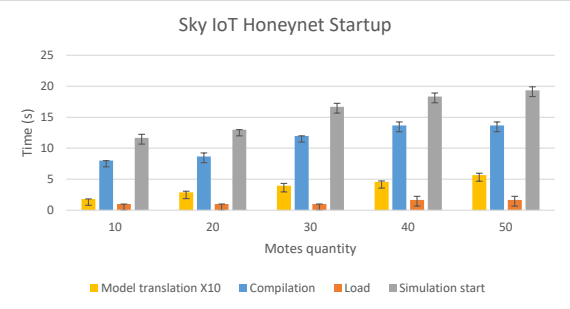


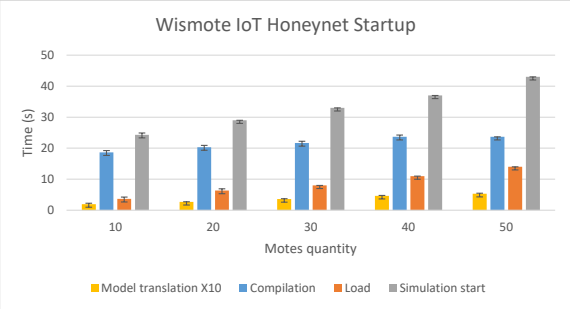
Fig. 10: Wismote 50 physical distribution

account the spatial location. In both cases all parameters increases as the number of IoT devices scales. The translation time is similar in both cases, since the cooja models are quite similar for the different contiki versions. On the other hand, the compilation and load times are greater in the second case, since the contiki 3.1 operating system version is heavier, what lengthens the final start of the simulation. In both cases, the most expensive time is the compilation time.

According to the physical scenarios proposed, in the first case (20 sky motes), the IoT honeynet is ready in less than 15 seconds, and in the second case (50 wismote motes) it is up and running in less than 45 seconds. Depending on the grade of the similitude needed, we can replicate not only the IoT devices with their configurations, but also the physical network topology. Indeed, we could generate a different topology in order to obtain some network benefits such as for instance,



(a) Sky Contiki 2.7 startup



(b) Wismote Contiki 3.1 startup

Fig. 11: IoT Honeynet Startup time

improving the convergence time in case we are not using static IP assignment. Since we are using RPL as routing protocol and the convergence time could be a handicap, the translator plugin allows to replicate the physical environment, and specify a concrete network topology.

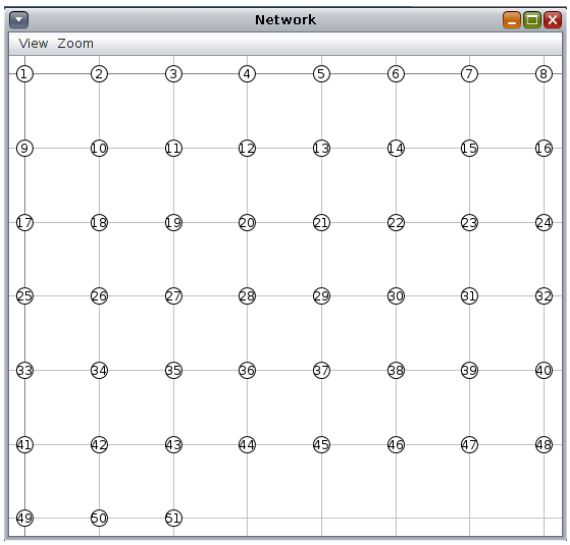


Fig. 12: Mesh Topology

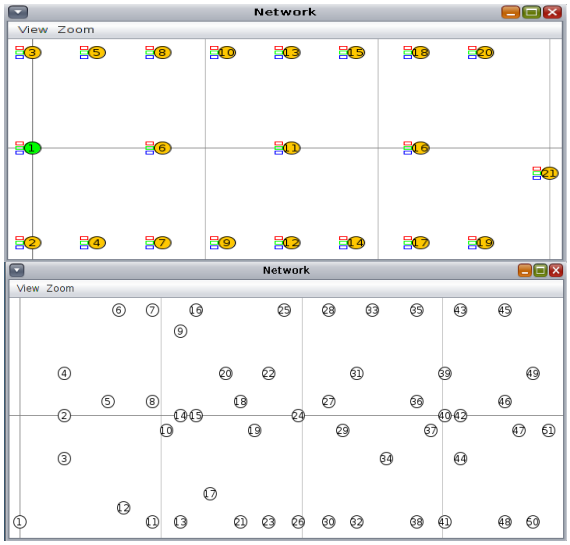
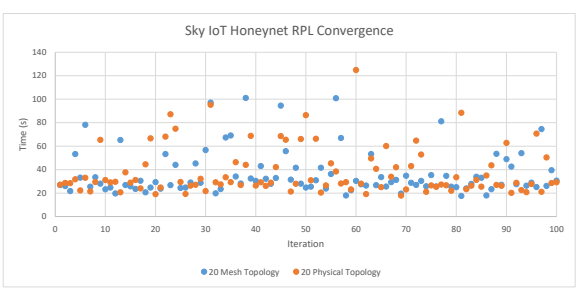


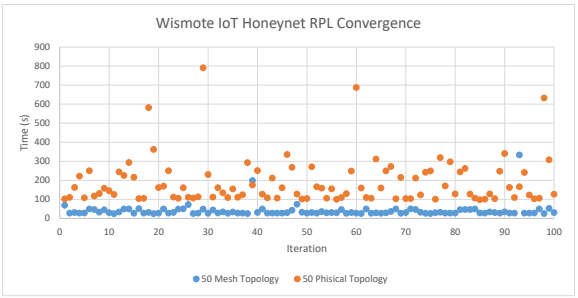
Fig. 13: Physical Topology

Figure 12 shows a vIoTHoneyNet mesh topology while figure 13 shows the IoT honeynet virtualization by replicating the physical positions for each use case. The mote marked as 1 represents the router and each square of the grid is 10 meters large. The system is considered converged when the router learns through RPL routing protocol at least one route for each device in the virtual IoT honeynet, i.e., when all nodes are fully reachable from outside. Since the topology is determinant in this process we compare the results of the physical topology

deployment emulation with the results of a classical mesh topology deployment emulation.



(a) Sky Contiki 2.7 convergence



(b) Wismote Contiki 3.1 convergence

Fig. 14: IoT Honeynet RPL Convergence

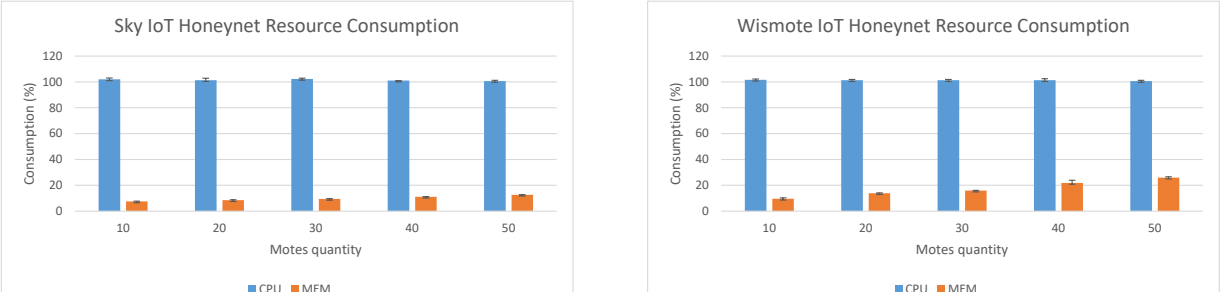
Figures 14a and 14b show the convergence time for both use cases by virtualizing the physical topology and a mesh topology. For the first floor use case, results are quite similar since the physical topology is close to a mesh topology. The best results are near to 17 seconds, while the worse results are close to 100 and 125 seconds respectively, being the vast majority comprised between 20 and 40 seconds. On the other hand, in the second floor use case, since the physical distribution is more random, we can observe the mesh topology obtains significant better results, being the majority of the results close to 35 seconds with a maximum of 334 seconds and a minimum of 24 seconds. It should be noted that IoT deployments devices are sleeping as much as they can in order to save energy, thereby generating a great dispersion in the results. The average values are close to 40 and 191 seconds, respectively.

Regarding filtering and forwarding policies enforcement, the performance evaluation accomplished measures the time taken since the filtering/forwarding policy enforcement has been requested, until them have been enforced in the vSwitch. Since in the experiments the networking policies are applied for a whole IoT subnet, the time taken by policies is independent of the number of the IoT devices. In this regard, the translation filtering and forwarding processes are independent of the use case, and the lightest steps in terms of time consumption.

Table II shows the performance time in the IoT honeynet policy enforcement process. For the first use case the virtual IoT honeynet are deployed in less than 60s, while in the second use case the average time is close to 4 minutes. These times might be improved through the use of static IP addresses or a more detailed study of the simulator parameters for the convergence times (out of the scope of this paper).

Use case	Translation X10	Simulation start	Convergence	Filtering	Forwarding	Total (s)
20-mesh	2.88	13.26	36.48	0.37	0.36	53.35
20-phy	2.88	13.26	37.89	0.37	0.36	54.76
50-mesh	5.3	43.41	39.93	0.37	0.36	89.37
50-phy	5.3	43.41	191.57	0.37	0.36	241.01

TABLE II: Policy enforcement timing



(a) Sky Contiki 2.7 resource consumption

(b) Wismote Contiki 3.1 resource consumption

Fig. 15: Resource usage performance

In addition, different tests were conducted to analyze the CPU and RAM memory usages of the our vIoTHoneynet manager. Figures 15a and 15b show the resource consumption measured for the different use cases. The CPU metrics are almost use case independent and the simulation is using completely one CPU at a 100%, regardless of the number of devices. Finally, as it was predictable, RAM memory grows according to the incremental number of devices, being bigger in the second use case, since the nodes are more complex.

VII. Conclusions

This paper has exposed a novel solution to manage dynamically virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-enabled IoT networks. The proposal allows administrators to deploy IoT Honeynets as a service through high level security policies over IoT infrastructures such as Smart Buildings. The approach adopted enables to replicate the physical IoT architecture on a virtual environment, by translating the physical architecture model to common interoperable IoTHoneyNet data model, and in turn, translating it to a virtualized environment deployed as VNFs. The whole process is driven by network security policies defined over the SDN controller and NFV MANO, whereby filtering, dropping and diverting the network traffic dynamically, and adapting the network behavior according to the new deployed vIoTHoneyNets needs.

The performance evaluation accomplished has demonstrated the feasibility of the proposed solution. Results has shown the successful deployment of IoT Honeynets with full connectivity. The deployment times behaves as expected, following a linear increasing trend as the number of nodes grows. Besides, the proposal has demonstrated that the virtual IoT Honeynets can be deployed on demand in a totally transparent way to the attacker, since the network behavior modification is performed fast, once the IoT Honeynet has been deployed.

As future work, we envisage to investigate on virtual IoTHoneynet for 5G-enabled IoT devices to reach broader and WAN scenarios. Finally, we also expect to design and implement, in the scope of ANASTACIA cognitive approaches (e.g. based on AI), in order to counter cyber-attacks in IoT.

ACKNOWLEDGMENTS

This work is the result of the stay (20177/EE/17) funded by "Fundacion Seneca-Agencia de Ciencia y Tecnologa de la Region de Murcia", under the program "Jimenez de la Espada de Movilidad Investigadora, Cooperacion e Internacionalizacion". The research has been also supported by a postdoctoral INCIBE grant within the "Ayudas para la Excelencia de los Equipos de Investigacin Avanzada en Ciberseguridad" Program, with code INCIBEI-2015-27363, as well as by the H2020 EU project ANASTACIA project, Grant Agreement N 731558.

REFERENCES

[1] Y. Gao, Y. Peng, F. Xie, W. Zhao, D. Wang, X. Han, T. Lu, and Z. Li, "Analysis of security threats and vulnerability for cyber-physical systems," in *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology*, Oct 2013, pp. 50–55.

[2] 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.

[3] A. Dunkels, B. Gronvall, and T. Voigt, "Contiki - a lightweight and flexible operating system for tiny networked sensors," in *29th Annual IEEE International Conference on Local Computer Networks*, Nov 2004, pp. 455–462.

[4] D. R. J. V. A. S. S. B. A. Z. Alejandro Molina Zarca, Jorge Bernal Bernabe and P. Gouvas, "Security by design architecture for softwarized and virtualized iot scenarios," *IEEE Internet of Things Journal*, pp. 1–1, 2019.

[5] J. P. Santos, R. Alheiro, L. Andrade, V. Caraguay, Á. Leonardo, L. I. Barona López, M. A. Sotelo Monge, L. J. Garcia Villalba, W. Jiang, H. Schotten *et al.*, "Selfnet framework self-healing capabilities for 5g mobile networks," *Transactions on Emerging Telecommunications Technologies*, vol. 27, no. 9, pp. 1225–1232, 2016.

[6] S. Ziegler, A. Skarmeta, J. Bernal, E. Kim, and S. Bianchi, "Anastacia: Advanced networked agents for security and trust assessment in cps iot architectures," in *2017 Global Internet of Things Summit (GIoTS)*, June 2017, pp. 1–6.

[7] V. Varadharajan and U. Tupakula, "Security as a service model for cloud environment," *IEEE Transactions on Network and Service Management*, vol. 11, no. 1, pp. 60–75, 2014.

[8] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things," in *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*. ACM, 2015, p. 5.

[9] A. Furfaro, A. Garro, and A. Tundis, "Towards security as a service (secaas): On the modeling of security services for cloud computing," in *Security Technology (ICCST), 2014 International Carnahan Conference on*. IEEE, 2014, pp. 1–6.

[10] S. Shin, L. Xu, S. Hong, and G. Gu, "Enhancing network security through software defined networking (sdn)," in *2016 25th International Conference on Computer Communication and Networks (ICCCN)*, Aug 2016, pp. 1–9.

[11] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin, and Z. Zhang, "Enabling security functions with sdn: A feasibility study," *Computer Networks*, vol. 85, pp. 19 – 35, 2015.

[12] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 602–622, Firstquarter 2016.

[13] Y. Choi, "Implementation of content-oriented networking architecture (cona): a focus on ddos countermeasure," in *Proceedings of European NetFPGA developers workshop*, 2010.

[14] T. Xu, D. Gao, P. Dong, H. Zhang, C. H. Foh, and H. C. Chao, "Defending against new-flow attack in sdn-based internet of things," *IEEE Access*, vol. 5, pp. 3431–3443, 2017.

[15] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the Internet of Things," in *Mobile Ad Hoc and Sensor Systems (MASS), 2015 IEEE 12th International Conference on*. IEEE, 2015, pp. 190–198.

[16] P. Bull, R. Austin, E. Popov, M. Sharma, and R. Watson, "Flow based security for iot devices using an sdn gateway," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug 2016, pp. 157–163.

[17] S. Choi and J. Kwak, "Enhanced sdiot security framework models," *International Journal of Distributed Sensor Networks*, vol. 12, no. 5, 2016.

[18] I. Farris, J. Bernabe, N. Toumi, D. Garcia-Carrillo, T. Taleb, A. Skarmeta, and B. Sahlin., "Towards Provisioning of SDN/NFV-based Security Enablers for Integrated Protection of IoT Systems," in *IEEE Conference on Standards for Communications and Networking (CSCN-2017)*, 2017.

[19] C. Hecker and B. Hay, "Automated honeynet deployment for dynamic network environment," in *2013 46th Hawaii International Conference on System Sciences*, Jan 2013, pp. 4880–4889.

[20] A. Guerra Manzanares, "Honeyio4: the construction of a virtual, low-interaction iot honeypot," B.S. thesis, Universitat Politècnica de Catalunya, 2017.

[21] P. Krishnaprasad, "Capturing attacks on iot devices with a multi-purpose iot honeypot," Ph.D. dissertation, 2017.

[22] J. D. Guarnizo, A. Tambe, S. S. Bhunia, M. Ochoa, N. O. Tippenhauer, A. Shabtai, and Y. Elovici, "Siphon: Towards scalable high-interaction physical honeypots," in *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*. ACM, 2017, pp. 57–68.

[23] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "Iotpot: analysing the rise of iot compromises," *EMU*, vol. 9, p. 1, 2015.

[24] W. Han, Z. Zhao, A. Doupé, and G.-J. Ahn, "Honeymix: Toward sdn-based intelligent honeynet," in *Proceedings of the 2016 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization*, ser. SDN-NFV Security '16. New York, NY, USA: ACM, 2016, pp. 1–6.

[25] N. Provos *et al.*, "A virtual honeypot framework." in *USENIX Security Symposium*, vol. 173, 2004, pp. 1–14.

[26] N. Memari, S. J. B. Hashim, and K. B. Samsudin, "Towards virtual honeynet based on lxc virtualization," in *2014 IEEE REGION 10 SYMPOSIUM*, April 2014, pp. 496–501.

[27] W. Fan, D. Fernndez, and Z. Du, "Versatile virtual honeynet management framework," *IET Information Security*, vol. 11, no. 1, pp. 38–45, 2017.

[28] F. H. Abbasi and R. J. Harris, "Experiences with a generation iii virtual honeynet," in *2009 Australasian Telecommunication Networks and Applications Conference (ATNAC)*, Nov 2009, pp. 1–6.

[29] W. Fan and D. F. Cambronero, "A novel sdn based stealthy tcp connection handover mechanism for hybrid honeypot systems," in *Proceedings of 2017 3rd IEEE Conference on Network Softwarization*, July 2017. [Online]. Available: http://oa.upm.es/45524/

[30] W. Fan, D. Fernández, and V. A. Villagrá, "Technology independent honeynet description language," in *Model-Driven Engineering and Software Development (MODELSWARD), 2015 3rd International Conference on*. IEEE, 2015, pp. 303–311.

[31] "Common Information Model (CIM), DMTF." http://www.dmtf.org/standards/cim.

[32] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Proceedings. 2006 31st IEEE Conference on Local Computer Networks*, Nov 2006, pp. 641–648.

[33] C. Basile, "D4.2 Policy transformation and optimization techniques, Secured EU project."

[34] R. Danyliw, J. Meijer, and Y. Demchenko, "The incident object description exchange format (iodef)," *Internet Engineering Task Force (IETF), RFC-5070*, 2007.

[35] O. Forum, "Open command and control (openc2)," https://openc2.org/members.html.