Dynamic Reconfiguration in 5G Mobile Networks to Proactively Detect and Mitigater Botnets

Gil Pérez, Manuel ; Huertas Celdrán, Alberto ; Ippoliti, Fabrizio ; Giardina, Pietro G. ; Bernini, Giacomo ; Marco Alaez, Ricardo; Chirivella Pérez, Enrique; García Clemente, Félix J. ; Martínez Pérez, Gregorio; Kraja , Elian ; Carrozzo, Gino ; Alcaraz Calero, Jose M.; Wang, Qi

Published in:
IEEE Internet Computing

DOI:
10.1109/MIC.2017.3481345

Published: 18/09/2017

Document Version
Peer reviewed version

5G

Dynamic Reconfiguration in 5G Mobile Networks to Proactively Detect and Mitigate Botnets

Manuel Gil Pérez, Alberto Huertas Celdrán, and Fabrizio Ippoliti
University of Murcia, Spain

Pietro G. Giardina and Giacomo Bernini
Nextworks

Ricardo Marco Alaez and Enrique Chirivella-Perez
University of the West of Scotland

Félix J. García Clemente and Gregorio Martínez Pérez
University of Murcia, Spain

Elian Kraja and Gino Carrozzo
Nextworks

Jose M. Alcaraz Calero and Qi Wang
University of the West of Scotland

//I abridged your abstract so that it will fit into the layout template. Feel free to revise, keeping the abstract under 100 words.//

*Botnets are one of the most powerful cyberthreats affecting continuity and delivery of existing network services. Detecting and mitigating attacks promoted by botnets become a greater challenge with the advent of 5G networks, as the number of connected devices with high mobility capabilities, the volume of exchange data, and the transmission rates increase significantly. Here, a 5G-oriented solution is proposed for proactively detecting and mitigating botnets in a highly dynamic 5G network. 5G subscribers' **mobility** requires dynamic network reconfiguration, which is handled by combining software-defined network and network function virtualization techniques.*

Internet/Web technologies, botnet, 5G, mobility, SDN, NFV

The incoming fifth-generation (5G) mobile technology aims to offer huge data bandwidth and high networking capabilities to bring superb users' experiences on mobile communications. Meeting the demands of 5G is more than merely increasing the computational and bandwidth resources of the infrastructure, although these improvements still represent a crucial driver.[1] Although not every detail of 5G has been disclosed yet, new security challenges will arise (as discussed in other work[2]).

The announced number and heterogeneity of 5G devices, with high mobility capabilities,

entail an ever-evolving threats landscape. One of the most powerful threats in 5G will remain the malicious actions led by botnets, as in existing networks. A botnet is a network of thousands, millions of compromised devices known as bots, infected by an unconsciously installed malware, going on to be controlled by a command and control (C&C) server remotely. Typically, recruited bots ask from time to time to the C&C if they should trigger actions. How botnets behave, their architecture, and communication patterns among bots and C&C servers are widely reviewed elsewhere.[3]

Among the potential malicious actions that a botnet owner can request, DDoS attacks are often the most commonly used today. Kaspersky Lab reported for the third quarter of 2016 that the botnet-assisted DDoS attacks comprised **//correct?//** 78.9 percent of all detected attacks, where the largest number was observed on 3 August 2016 with 1,746 attacks.[4] As real examples, the Mirai and Leet botnets launched crippling DDoS attacks in 2016, reaching up to 650 gigabits per second (Gbps) of network traffic to disrupt services of Amazon and Netflix, among others.

Detecting and mitigating botnets have been addressed by many works,[5] among which we can highlight BotHunter[6,7] as a popular detector. BotHunter focuses on detecting specific stages of the malware infection process, conducted during the first recruitment phase, while BotMiner consists of a network anomaly-based botnet detection system that clusters similar traffic to identify C&C communication patterns. Yet, they focus on inspecting network packet payloads, which isn't a feasible choice in 5G because of the large volumes of data generated from 5G subscribers' User Equipment (UE), causing Deep Packet Inspection (DPI) tools to be overloaded. To address this drawback, many works move toward higher levels of detection to analyze swiftly the basic information of network flows. Rodrigo Braga and colleagues,[8] for example, proposed an unsupervised artificial neural network based on self-organizing maps that uses a set of low-level metrics to characterize the traffic and thus detect DDoS botnet attacks. In a real network environment, Daniël van der Steeg and colleagues presented a prototype to detect these DDoS botnet attacks using NetFlow.[9]

In addition to the aforementioned concerns, the large number of 5G subscribers' UEs with high mobility skills will require researchers **//or who?//** to adapt the existing detection and reaction algorithms to face botnets.[10] When bots move, the detection and reaction capabilities also have to be moved, "following" the bots, to continue performing their procedures accordingly. To address this issue, software-defined network (SDN) and network function virtualization (NFV) technologies could be used to enhance the flexibility of the network functions' (NFs') provisioning and update. Deployment of NFs as software elements is key for 5G networks, leveraging on common abstractions for their monitoring, configuration, control, and management. In this context, BotGuard[11] is a botnet detection framework based on SDN to identify botnets promptly, analyzing the topology characteristics to detect C&C communication patterns when depicting traffic in convex lens imaging graphs. Recently, Cristian Machado and colleagues presented an architecture called ANSwer,[12] where SDN and NFV features are combined to create network resilience strategies. ANSwer discusses the need for maintaining network resilience and demonstrates how to deploy and reconfigure SDN and NFV applications in real time to achieve satisfactory levels of resilience.

In this article, we present the design and implementation of an architecture oriented to the SDN and NFV technologies with new components to conduct the detection and

mitigation of botnets in 5G networks. The main novelty of this approach comes from the conduction of two control loops, with two different levels of abstraction for detection, because of the large number of expected 5G subscribers' UEs: a light, high-level detection to analyze network flows and identify suspicious bots very quickly; and, once possible bots are observed, conducting a heavy low-level DPI to confirm that the botnet is in place. For its mitigation, we propose the deployment of a virtualized and personalized honeynet to isolate the botnet communications through bots' behavior emulation. In this scenario, the bots' mobility is also considered and properly addressed, managing and detecting UEs' movements to dynamically deploy and/or reconfigure NFs in the 5G network infrastructure at runtime.

Motivating Use Case for a 5G Scenario

Here, we detail the mobile-aware 5G-oriented solution with a set of steps describing a use case, depicting several requirements that should be considered to detect and mitigate botnets in 5G networks. Figure 1 shows a given scenario composed of two 5G network operators that provide certain services in two different countries. They separate the Radio Access Network (RAN) from the non-radio aspects considered as an Evolved Packet Core (EPC) network.

Figure 1. Proactive scenario to detect and mitigate botnets. The scenario is composed of two 5G network operators that provide certain services in two different countries. They separate the Radio Access Network (RAN) from the non-radio aspects considered as an Evolved Packet Core (EPC) network. UE stands for User Equipment, and areas labeled a through f indicate the key architectural points where the architecture needs to face functional requirements (referred to in the main body text as Requirements a, b, and so forth). **//More descriptive caption okay?//**

Users in this scenario can move along the different RANs, consuming services at will. The UE of a given *User* is shown who moves requesting services to two servers, *Server1* and *Server2*. In this scenario, both EPCs belong to the same multitenant service provider, with roaming capabilities configured to allow mobility between them. In Figure 1, areas labeled a through f indicate the key architectural points where our architecture needs to face some functional requirements, so as to allow the discovery of the UE's purposes: whether it's a real bot contacting a C&C server or it's a legitimate UE.

The UE initially connects to RAN1, marked as Point 1 in Figure 1, and starts a communication with Server1. This network flow should be analyzed to determine whether the UE is a bot and Server1 is a real C&C. This raises *Requirement a*. A *Detection* process must be deployed in that RAN to perform the required detection.

As indicated in Point 2 of Figure 1, the user and his or her UE moves to another location of Country1. The Detection process should continue its tasks for determining whether the UE is a real bot, which began in Requirement a. Because RAN1 and RAN2 belong to EPC1, the UE's IP address doesn't change and the established connections aren't interrupted. This intra-EPC mobility raises *Requirement b*. Therefore, the previous Detection process must be reconfigured, now taking into consideration the new UE's location. Once this process confirms that the UE is actually a real bot, a *Reaction* process should be triggered so as to hijack the communications between the UE and Server1 and

thus prevent the execution of future attacks. This Reaction process is highlighted as *Requirement c* in Figure 1. This reaction will only hijack the network flows between the UE and Server1, leaving intact the UE's other communications.

As a next step, Point 3 of Figure 1 depicts when the UE moves to Country2, connecting now to RAN3 belonging to EPC2. This inter-EPC mobility causes the change of its IP address, giving rise to *Requirement d*. Because of this, a reconfiguration of the Reaction process deployed in Requirement c needs to be performed, considering the information of two different network operators. As a result, the traffic between the UE and Server1 should still be hijacked as before in RAN2.

As any UE is likely to be recruited by a botnet, consider that the UE of the use case establishes a new connection with another target, Server2. This is Point 4 in Figure 1. In this case, the new *Requirement e* indicates that another Detection process should be deployed and started to determine whether Server2 is actually a C&C. If so, *Requirement f* consists in performing a reconfiguration of the Reaction process running in Requirement d, adding the mitigation of the communication between the UE and Server2.

Proactively Detecting and Mitigating Botnets in 5G

This section details how the 5G-oriented botnet detection and mitigation proposal addresses the aforementioned requirements. This solution uses NFV techniques to deploy and/or reconfigure dynamically the virtualized network functions (VNF) needed to detect and mitigate botnets, adapting them when UEs move between RANs. Moreover, this proposal also leverages the SDN paradigm to modify at runtime the forwarding of packets during the detection and mitigation processes. Both technologies are perfectly integrated into this solution with the components of 5G networks.

The proposed solution relies on a Detection process, shown in Figure 1's use case, with two different phases at two complementary levels of abstraction. The first one refers to a high-level detection phase, where the network flows between the UEs and Servers are monitored and analyzed quickly. It's worth noting that this phase is always up and running to search new suspicious bots. In 5G scenarios, this first phase is mandatory. The huge number of UEs and the expected high-bandwidth rates make it impossible to perform a deep analysis of all the information flowing through 5G networks.

To perform this first high-level detection procedure, a *Flow Monitoring* (FM) function is being used, which lets us extract network flows encapsulated into general packet radio service (GPRS) Tunneling Protocol (GTP) packets that travel between RANs and EPCs in 5G mobile networks. As this needs to be always running to analyze all the network flows in search of suspicious bots and C&C servers, an FM is initially deployed in every RAN. Once a given UE is detected as a suspicious bot, a dedicated VNF providing DPI functionalities is deployed and configured (in the RAN in which the UE was detected) by following the European Telecommunications Standards Institute (ETSI) Management and Orchestration (MANO) NFV principles and procedures.[13] Using a DPI tool, **//the VNF?//** seeks specific highly distinctive patterns of particular botnet types, or a change in the normal behavior of the UE. As a result of this phase, we can confirm that UEs and Servers are real bots and C&C servers, respectively.

A fine-granularity analysis through a DPI tool can also be seen as Requirement a in Figure 1. That is, both detection procedures are conducted in the same RAN1: the first phase analyzes the network flows of all peers, while the second one is exclusively focused

on a much smaller pool of (suspicious) peers. So, the proposed double loop of detection allows facing the analysis of large volumes of information generated from the immense range of 5G subscribers' UEs.

Following the use case of Section 2, our solution relies on software switches such as Open Virtual Switch (OVS), deployed in RAN locations, so that the DPI tool can analyze the traffic between the UE and Server1. With an SDN Controller, we can control the network flows between the components (RAN and EPC components, VNFs, network nodes, and so on) of the use case. Specifically, we must add a *network flow mirroring* rule in the OVS flow table to mirror the traffic between the UE and Server1 to the DPI tool deployed for its analysis.

Before the UE can be thoroughly analyzed by the DPI tool of RAN1, the UE moves to RAN2. This corresponds to Point 2 of Figure 1, which is depicted in Figure 2 to represent the same scenario of Figure 1, but zooming Country1's components to detail the elements of a 5G network. This intra-EPC mobility of the UE is detected by a Long-Term Evolution Topology Manager (LTE TM) element. This is a new API provided by the Serving Gateway (S-GW) to notify mobility changes in a 5G topology. Thanks to the LTE TM, we can know that the UE is now connected to RAN2, and its IP address doesn't change in that transit because RAN1 and RAN2 belong to the same EPC.

As the UE hasn't been confirmed yet as a real bot, it's only suspicious for now, and the detection capabilities imposed on RAN1 also have to be moved to RAN2, the new placement of the UE. To this end, the actions performed by our solution are as follows, indicated as Requirement b in Figure 2:

- Deploy a DPI VNF in RAN2, similar to the RAN1 one, and configure it with the same detection rule to continue analyzing the traffic between the UE and Server1. If a DPI tool exists in RAN2, only the detection rule is added without deploying more VNFs.
- Add a network flow mirroring rule in the OVS flow table allocated in RAN2 to allow the DPI tool to receive the network flows between the UE and Server1.

Figure 2. Proposed 5G-oriented solution for the mobile use case. C&C = command and control; DPI = Deep Packet Inspection; FM = Flow Monitoring; HLTE TM = Long-Term Evolution Topology Manager; HSS = Home Subscriber Server; P-GW = Packet Data Network (PDN) Gateway; S-GW = Serving Gateway; SDN = software-defined network. **//Did I spell out the acronyms correctly? Or please correct as needed.//**

Once the previous actions have been successfully completed in RAN2, the detection rule in the RAN1's DPI tool to analyze the traffic between the UE and Server1 should be taken down. Also, the DPI VNF can be de-provisioned still following the ETSI MANO NFV procedures for VNFs termination, in case there are no other suspicious bots to be analyzed in RAN1.

If the DPI VNF deployed in RAN2 detects that the UE is a real bot, our solution initiates a Reaction process, indicated as Requirement c in Figure 2, which consists in the following:

- Deploying a new VNF implementing a honeynet that provides the same functionality of the UE detected, emulating its behavior through a cloned fake bot. Server1 won't be aware of that change, as it will continue to receive requests asking

for actions to be executed, but they will be sent by the cloned fake bot.

- Adding a network flow diversion rule in the OVS flow table of RAN2 to block the traffic flow between the UE and Server1, and divert it to the new cloned fake bot. This will prevent the UE from executing future attacks, as its functionality has been disabled by our deception-based solution through a honeynet.

As a next step, the UE moves between two countries, per Requirement d. This inter-EPC mobility is observed by our solution, taking into account information from the LTE TM belonging to each EPC. Specifically, the UE's IP address changes when moving from RAN2 to RAN3, but its stored identifier as an International Mobile Subscriber Identity (IMSI) is a unique value that doesn't change. By correlating this information, our solution is capable of discovering the UE mobility. The reconfiguration of the honeynet consists in also moving the VNF from RAN2 to RAN3, as well as updating the configuration of the honeynet with the new IP of the UE to maintain the emulation features required. To this end, we still apply ETSI MANO NFV procedures to deploy the honeynet VNF in the new location and update its configuration accordingly. Furthermore, a new diversion rule is required in the OVS's flow table allocated in RAN3.

As the last step, the UE starts a new communication with another target, Server2. As the first detection phase is always running, it identifies that the UE and Server2 are maintaining a potential malicious flow. A second detection phase is needed to confirm the botnet, for which the deployment of a new DPI VNF is triggered and includes a network flow mirroring configuration. This is aligned with Requirement e in Figure 1. Once Server2 is confirmed as another C&C, Requirement f finishes reconfiguring the honeynet previously deployed. The instantiation of a new honeynet VNF isn't necessary, as the UE's behavior is being emulated already to manage another botnet. Therefore, a reconfiguration of the existing honeynet consists in adding a new functionality that also emulates the new UE's behavior with Server2. Then, another network flow diversion rule must be added to the RAN3's OVS for blocking the link between the UE and Server2, as well as forwarding their flows to the already running cloned fake bot.

Proposed Architecture

Our architecture uses the four well-known processes for detection and reaction purposes — known as the Monitor, Analyze, Plan, and Execute (MAPE) approach — to present a functional decomposition of the proposed 5G botnet detection and mitigation architecture. This will "close the loop" from monitoring GTP flows and packet (analysis) to the orchestrated deployment of new VNFs in real time. As we mentioned, our proposal follows an approach of two detection phases with different levels of abstraction (see Figure 3).

Figure 3. Workflows of the two control loops of detection from (a) a high-level and (b) a fine-granularity level perspective. ABf = average of bytes per flow; ADf = average of duration per flow; ANPPF = average number of packets per flow; HNet = honeynet; and OVS = Open Virtual Switch. **//Did I spell out the acronyms correctly? Or please correct as needed.//**

Figure 3a shows the complete workflow for the first detection phase so as to identify suspicious bots, as well as the information exchanged between them. The Monitor process

is the first one executed for gathering network data from the FM and the LTE TM elements, and correlating and aggregating it for a subsequent analysis. The FM extracts metrics associated with the network flows of the UEs and Servers — for example, average number of packets per flow (ANPPF), average of bytes per flow (ABf), and average of duration per flow (ADf).

On the other hand, the LTE TM provides the UEs' location: media access control (MAC), IP addresses, and tunnel identifiers of the eNodeBs at which UEs are connected. With this, the Analyze process is in charge of analyzing it to decide whether UEs are suspicious bots and each target is a C&C server. If so, the Analyze process sends to the Plan one of the IP addresses of the UEs and Servers, and the botnet type is identified.

During the first detection phase, the Plan process decides to deploy a DPI VNF to analyze in detail the exchanged network packets, and modify the OVS flow table to mirror the traffic between the suspicious peers to the DPI tool. These decisions are sent to the Execute process, which is able to deploy and enforce the required actions to make it possible. The Execute process is composed of several components, starting from two Orchestrators. The *NFV Orchestrator* (NFVO) is capable of automatizing the process of applying the decisions made by the Plan process regarding the deployment and configuration of the VNFs. Following the ETSI MANO NFV procedures, the NFVO interacts with the *VNF Manager* (VNFM) to instantiate and dynamically configure the DPI VNF (as a combination of virtualized network and compute resources) in the virtualized infrastructure that's managed by the *Virtualized Infrastructure Manager* (VIM). Finally, the *SDN Orchestrator* (SDNO) is in charge of automatizing the configuration of the SDN plane, thereby configuring the OVS flow table through the *SDN Controller* to apply the network traffic mirroring rule.

Figure 3b depicts the processes conducted during the second detection phase. First, the Monitor process gathers, aggregates, and correlates the single alerts produced by the DPI VNF, as well as gathering the location information from the LTE TM. Note that these alerts carry the botnet type and the IP addresses of the suspicious bots and C&C servers, which are sent to the Analyze process. The system **//or what, specifically?//** then decides if they're actually bots and C&C servers. If so, the botnet type and the IP addresses are sent to the Plan process, which decides to deploy a honeynet per bot so as to hijack its network flows with a C&C server. These decisions are applied by the Execute process. To this end, the NFVO automatizes deploying honeynets as VNFs through the VNFM, on top of the VIM; configures them with the botnet type and the IP addresses of the bots and C&C servers, through the VNFM; and the SDN Controller is requested by the SDNO to add the network flow diversion rule for managing the network flows between such peers.

Implementing the 5G-Oriented Solution

This section details how the implementation of our proposed architecture combines free and open source SDN/NFV technologies in a fully virtualized environment, together with certain custom 5G software components to address the requirements highlighted in the use case.

Following the MAPE architecture, the Execute process is built integrating three existing SDN/NFV platforms running in a VNF per each **//module or component, or what, specifically? A word is missing here.//**. The role of the NFVO is covered by the OpenBaton framework (http://openbaton.github.io) that's fully compliant with the ETSI

MANO specification[14] and supports different types of VNFMs and VIMs. In our implementation, we make use of the version 3.0.1 that supports autoscaling, fault management, and the possibility of configuring the VNF external networks through the VIM command interface. OpenBaton also provides a generic VNFM component that we customized to meet the reconfiguration requirement of a VNF at runtime, as indicated by Requirements b and f in the use case.

We use OpenStack Liberty (see www.openstack.org) to cover the role of the VIM, basically for the following reasons: it's the de facto open source cloud management platform; it's compliant with OpenBaton; it's possible to integrate it with OpenDaylight (www.opendaylight.org) version 0.4.2, chosen as the SDN Controller; and it uses OVS as a software switch for VNF instances. In our proposal, VNFs are virtual machines (VM) that execute certain components required to perform the detection and reaction procedures. Specifically, during the detection process, the DPI VNF is a VM executing an instance of Snort IDS tool version 2.9.7.0 (www.snort.org), supporting GTP, while during the reaction process the honeynet VNF runs a generic application acting as a bot to cheat the C&C.

In the SDN/NFV integrated environment, OpenDaylight and OpenStack are both in charge of network management. In particular, while OpenStack controls the networking at layer 3, OpenDaylight controls the OpenStack internal OVS instances to be capable of installing OpenFlow rules received from SDNO in their flow tables. SDNO is a custom-developed software that interacts with the SDN Controller through the OpenDaylight REST API interfaces and generates the proper OpenFlow rules when network flow mirroring and network flow diversion actions are required. When the Plan process decides to install a rule in OVS, SDNO queries the controller's inner datastores to retrieve all needed network topology information. This procedure is necessary to identify the involved switches and hosts (UEs, VNFs, C&C, and so on) connected to them. Once the targets (that is, bots, the C&C, and Snort when generating the network flow mirroring rule) are identified in the network, SDNO generates the flow rule as a JavaScript Object Notation (JSON) payload of a REST query to send to OpenDaylight.

To replicate a 5G environment as realistically as possible, we consider the Open Air Interface (OAI; www.openairinterface.org) wireless platform, which provides a software-based implementation of EPC and RAN compatibles with the Third-Generation Partnership Project (3GPP) LTE standard. Both the radio and core packet facilities must be considered as part of the solution infrastructure. Thus, in our implementation, they're deployed as VNFs outside the NFVO/VNFM, and can be considered as part of the infrastructure.

The FM component is a 5G-oriented software, developed to extend the OVS monitoring features. Indeed, although OVS supports different types of monitoring protocols, it isn't able to extract information encapsulated into GTP flows. The FM extracts information and generates network statistics about the IP, TCP/UDP, and application-level packets encapsulated in GTP. The FM is integrated into the virtualized infrastructure as part of the RAN, and belongs to the Monitor process.

Finally, the LTE TM element is a customized part of the OAI that's located at the EPC, holding information related to UEs' movements and triggering mobility events. When a given event regarding the UE mobility happens, the LTE TM produces a message that's stored in a repository. Three kinds of messages are considered: create, update, and delete. Each message brings an information payload related to the UEs and mobile infrastructures:

eNodeB, P-GW, S-GW, and so forth. In this way, we're able to know the first time that a UE is connected to a specific RAN (create), the moment when UE changes the RAN (update), and when a UE is no longer connected to the RAN (delete). Hence, actions from the LTE TM let us track UE's mobility, and therefore reconfigure the detection and reaction processes of our solution.

The high mobility capabilities of UEs, as well as the large volumes of data generated in emerging 5G networks, require developing innovative solutions to address cyberattacks conducted by botnets. With our 5G-oriented solution, the 5G network infrastructure is dynamically reconfigured to detect and mitigate botnets proactively, using a double control loop of detection and deploying a virtualized and personalized honeynet, respectively. Detection and reaction functionalities will maintain their capabilities even when subscribers move in a highly dynamic 5G network. This solution uses innovative features enabled by combining SDN/NFV techniques.

In future work, we'll explore ways of moving detection and reaction between network operators in interprovider scenarios, where new security and privacy conditions will arise. In addition, we also plan to evaluate our architecture and the current implementation we have running in our internal lab environment — which properly detects and mitigates Zeus-based botnets — as well as addressing other types of botnets.

Acknowledgments

This work was supported by a Séneca Foundation grant within the Human Resources Researching Training Program 2014, the European Commission Horizon 2020 Programme under grant agreement H2020-ICT-2014-2/671672 — SELFNET (Framework for Self-Organized Network Management in Virtualized and Software Defined Networks), and the European Commission (FEDER/ERDF).

References

1. *5G Security: Forward Thinking*, white paper, Huawei Technologies, Dec. 2015.
2. A.B. Martin et al., *Threat Landscape and Good Practice Guide for Software Defined Networks/5G*, tech. report, European Union Agency for Network and Information Security (ENISA), Dec. 2015; www.enisa.europa.eu/publications/sdn-threat-landscape.
3. R.A. Rodríguez-Gómez, G. Maciá-Fernández, and P. García-Teodoro, "Survey and Taxonomy of Botnet Research through Life-Cycle," *ACM Comp. Surv.*, vol. 45, no. 4, 2013, pp. 45:1–45:33; doi:10.1145/2501654.2501659.
4. O. Kupreev, J. Strohschneider, and A. Khalimonenko, *Kaspersky DDOS Intelligence Report for Q3 2016*, tech. report, *SecureList*, 31 Oct. 2016; https://securelist.com/kaspersky-ddos-intelligence-report-for-q3-2016/76464.
5. M. Mahmoud, M. Nir, and A. Matrawy, "A Survey on Botnet Architectures, Detection and Defences," *Int'l J. Network Security*, vol. 17, no. 3, 2015, pp. 272–289.
6. G. Gu et al., "BotHunter: Detecting Malware Infection through IDS-Driven Dialog Correlation," *Proc. 16th Usenix Security Symp.*, 2007, pp. 12:1–12:16.
7. G. Gu et al., "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection," *Proc. 17th Usenix Security Symp.*, 2008, pp. 139–154.
8. R. Braga, E. Mota, and A. Passito, "Lightweight DDoS Flooding Attack Detection using NOX/OpenFlow," *Proc. 35th Local Computer Networks*, 2010, pp. 408–415; doi:10.1109/LCN.2010.5735752.
9. D. van der Steeg et al., "Real-Time DDoS Attack Detection for Cisco IOS Using NetFlow," *Proc. 2015 IFIP/IEEE Int'l Symp. Integrated Network Management*, 2015, pp. 972–977; doi:10.1109/INM.2015.7140420.

10. N. Yang et al., "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security," *IEEE Comm.*, vol. 53, no. 4, 2015, pp. 20–27; doi:10.1109/MCOM.2015.7081071.
11. J. Chen et al., "BotGuard: Lightweight Real-Time Botnet Detection in Software Defined Networks," *Wuhan Univ. J. of Natural Sciences*, vol. 22, no. 2, 2017, pp. 103–113; doi:10.1007/s11859-017-1223-8.
12. C.C. Machado, L.Z. Granville, and A. Schaeffer-Filho, "ANSwer: Combining NFV and SDN Features for Network Resilience Strategies," *Proc. IEEE Symp. Computers and Comm.*, 2016, pp. 391–396; doi:10.1109/ISCC.2016.7543771.
13. European Telecomm. Standards Inst. Network Function Virtualization Industry Specification Group (ETSI NFV ISG), *Network Functions Virtualisation (NFV); Management and Orchestration*, specification, ETSI GS NFV-MAN 001 V1.1.1, Dec. 2014.
14. ETSI NFV ISG, *Network Functions Virtualisation (NFV); Infrastructure Overview*, specification, ETSI GS NFV-INF 001 V1.1.1, Jan. 2015.

Manuel Gil Pérez is a research associate in the Department of Information and Communication Engineering of the University of Murcia, Spain. His research primarily focuses on security infrastructures, trust management, and intrusion detection systems. Gil Pérez has a PhD in computer science from the University of Murcia. Contact him at mgilperez@um.es.

Alberto Huertas Celdrán is a research associate in the Department of Information and Communication Engineering of the University of Murcia, Spain. His scientific interests include security, software-defined networking, semantic technology, and policy-based context-aware systems. Huertas Celdrán has a PhD in computer science from the University of Murcia. Contact him at alberto.huertas@um.es.

Fabrizio Ippoliti is a PhD candidate in a double-degree program between the Department of Information and Communications Engineering at the University of Murcia, Spain, and the Department of Computer Science at the University of Camerino, Italia. His research interests include future network architectures and services. Ippolitic has an MSc in computer science from the University of Camerino. Contact him at fabrizio.ippoliti@um.es.

Pietro G. Giardina is a software engineer in R&D department at Nextworks. His research interests and development activities mainly focus on software-defined networks (SDN), network function virtualization (NFV), OpenFlow, and Netconf. Giardina has an MSc in computer engineering from **//which university?//**. Contact him at p.giardina@nextworks.it.

Giacomo Bernini is an R&D project manager at Nextworks. His main responsibilities include the coordination and management of both research and industrial projects, including consultancies and third-party software developments for European telecommunications vendors and providers for network control and orchestration solutions. His background and expertise mostly focuses on NFV, SDN, 5G network architectures, and cloud computing. Bernini has a **//highest degree achieved?//** in **//which subject area?//** from **//which university?//**. Contact him at g.bernini@nextworks.it.

Ricardo Marco Alaez is a researcher **//or what is his current position?//** at the University of the West of Scotland, United Kingdom, where he's involved in the H2020 5G-PPP Phase 1 SELFNET project. His main interests include network management, mobile networks in cloud computing, and 5G networks. Marco Alaez has a PhD in tTelecommunications from the University of Valencia. Contact him at Ricardo.MarcoAlaez@uws.ac.uk.

Enrique Chirivella-Perez is a PhD student at the University of the West of Scotland, United Kingdom, where he's involved in the H2020 5G-PPP Phase 1 SELFNET project. His main interests includes infrastructure

monitoring, network management, automatic deployment of services, and software-defined networks in cloud computing and 5G networks. Contact him at Enrique.Chirivella-Perez@uws.ac.uk.

Félix J. García Clemente is an associate professor in the Department of Computer Engineering of the University of Murcia. His research interests include security and management of distributed communication networks. Garcia Clemente has a PhD in computer science from the University of Murcia. Contact him at fgarcia@um.es.

Gregorio Martínez Pérez is a full professor at the University of Murcia. His research interests include security and management of distributed communication networks. Martínez Pérez has PhD in computer science from the University of Murcia. Contact him at gregorio@um.es.

Elian Kraja is a software engineer and Openstack architect at Nextworks, where he's active in 5G-PPP projects (SELFNET, 5G-CROSSHAUL, 5G-MEDIA, and 5G-Transformer), industrial projects on NFV technologies, and is a member of an ETSI Task Force (STF 530) working on gap analysis between IFA005/006 and OpenStack APIs. His research interests include cloud computing, SDN, and NFV. Kraja has a **//highest degree achieved?//** in computer science **//which university?//**. Contact him at e.kraja@nextworks.it.

Gino Carrozzo is the deputy head of R&D and senior network architect at Nextworks. He is research focuses on telecommunication networks, with deep knowledge of architectures and protocols for 5G, SDN/NFV, IoT, GMPLS/ASON, MPLS-TP, and PBB-TE. Carrozzo has a PhD in **//which subject area?//** from **//which university?//**. Contact him at g.carrozzo@nextworks.it.

Jose M. Alcaraz Calero is a professor in networks and security at the University of the West of Scotland, and he's the technical co-manager of the EU H2020 5G-PPP projects SELFNET and SliceNet. His professional interests include network cognition, management, security and control, service deployment, automation and orchestration, and 5G mobile networks. Alcarez Calero has a PhD in **//which subject area?//** from **//which university?//**. Contact him at Jose.Alcaraz-Calero@uws.ac.uk.

Qi Wang is a full professor with the University of the West of Scotland, and he's the technical co-manager of EU H2020 5G-PPP projects SELFNET and SliceNet. His research primarily focuses on 5G mobile networks. Wang has a PhD in **//which subject area?//** from the University of Plymouth, UK. Contact him at Qi.Wang@uws.ac.uk.