JNIC2017

III Jornadas Nacionales de Investigación en Ciberseguridad

Madrid, 31 de mayo y 1-2 de junio de 2017

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Universidad Rey Juan Carlos

A review of efficient network management to enhance the provision of attacks' network flows

Alberto Huertas Celdrán, Manuel Gil Pérez, Félix J. García Clemente, and Gregorio Martínez Pérez

Faculty of Computer Science, University of Murcia, 30071 Murcia, Spain
Email: alberto.huertas@um.es, mgilperez@um.es, fgarcia@um.es, gregorio@um.es

***Abstract*—Managing network resources in charge of monitoring network flows generated by potential attackers is a complex process that should be carried out in an automatic way. Self-Organizing Networks should be able to guarantee the provision of flow-based monitoring services to later detect cyber-attacks and react against them automatically. In this sense, we present a policy-based system oriented to the SDN paradigm in charge of managing automatically the network resources to ensure the provision of flow-based monitoring services. Using our proposal, network administrators define policies to switch-on/off, balance, or create/dismantle physical and virtual network resources considering the users' mobility, the network statistics, and the location of the infrastructure.**

***Index Terms*—Flow-based monitoring, Cyber-attacks, SDN, Virtualization, Location, Mobility**

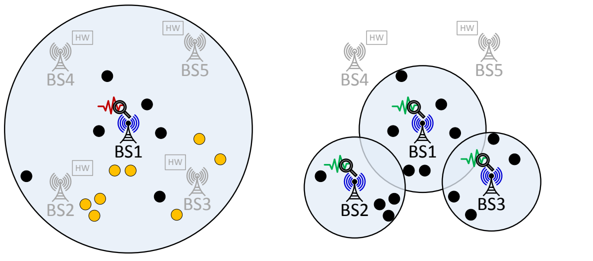
Tipo de contribución: *Investigación ya publicada*

I. Introduction

Administrators of traditional networks are characterized by managing and configuring manually their resources. The evolution of technologies has increased the complexity of the network management processes by including new heterogeneous information and resources. This new situation has required the automatization of the management processes performed by network administrators. In this sense, Self-Organizing Networks (SON) arose with the goal of moving from traditional manual management processes towards an automatic and dynamic perspective.

One of the most challenging tasks of SON is the automatic protection of the network resources and users against cyber-attacks. The first step of this self-protection consists in monitoring the network flows generated by active users to later analyze anomalies and detect potential cyber-attacks. In this sense, the provisioning of flow-based monitor services is an essential and complex process that should be carried out in an automatic way. Otherwise, it would be impossible to perform it, due to the huge number of users consuming network services, the high mobility of users, or the current bandwidth and latency of current communications, among others.

To reduce the complexity of the network management, virtualization techniques and the *Software Defined Networking* (SDN) paradigm can help to configure and manage automatically the network resources considering the network status. However, despite the facilities provided by the SDN paradigm, the mobility provided by current devices and the dynamic provision of services have hindered the management of the network infrastructure efficiently. Nowadays, SON should consider aspects like the network statistics, the users' mobility, or the infrastructure's location to ensure the provision of flow-based monitoring services.



(a) Concerned scenario (b) Managed scenario

Fig. 1. Network ensuring the provision of flow-based monitoring services.

In this sense, this paper is an extension of [1] oriented to manage efficiently the network infrastructure during the provision of flow-based monitoring services. Our mobility-aware solution can manage automatically the network infrastructure to ensure the provision of flow-based monitoring services, which are essential to later analyze the monitored information and detect cyber-attacks. To this end, network administrators define a set of policies which can switch on/off, balance, or create/dismantle at real-time physical or virtual network resources by considering aspects like the network statistics, the number of active users, or the users' mobility.

II. Proposal

To show the usefulness of our solution we define a dynamic scenario to illustrate the concerns that flow-based monitoring services can find in very crowded places. The proposed use case is composed of five base stations (BSs) distributed along a given area. Among them, one (BS1) is providing users with network services as well as monitoring the network flows, the rest of BSs are asleep (BS2, BS3, BS4, and BS5). Fig. 1a shows how the service running in BS1 is monitoring the network flows generated by the users located in the area (black points), and it is able to manage the whole flows ensuring the provision of service. In a given moment, some newcomers appear (yellow points) and the flow monitoring service is not able to gather the whole network flows. This fact implies that the subsequent processes of detection and reaction against cyber-attacks will not be performed properly.

To manage this situation, our proposal allows switch on/off new base stations located close the congested one (BS2 and BS3), create new virtual flow-based monitoring services from generic hardware allocated in the BSs, and balance the traffic between the existing base stations to distribute the flow monitoring work. Fig. 1b, depicts the situation managed by our solution. To perform automatically and at real-time the previous changes, our solution makes use of management oriented policies. Using our proposal, the network administrators can define three kinds of policies: switching, virtualization, and balancing. These policies will decide the list of potential actions to be taken by the network's resources in accordance with the provision of flow-based monitoring services. It is worthy to note that other policies could also be defined since the proposed solution is extensible.

1) Switching policies: Switching policies allow the SDN paradigm to switch on/off the network resources located at specific locations. Oriented to the use case, the network administrator can define the next policy indicating that when the flow monitoring service running in the BS1 is congested, that means that the number of monitored flows per second (MFPS) is over the *RedAlert* threshold (defined by the network administrator beforehand), the action of the policy consists in switching on the base stations located close to the congested one.

Type(#Switching) ∧ BaseStation(?bs) ∧ Location(?bs,?area) ∧
locatedBS(?area,?neighborBSs) ∧ hasMonitorServ(?bs,?serv) ∧
integer[MFPS in #RedAlert] hasMFPS(?serv)
→ switch(?neighborBSs,#ON)

2) Virtualization policies: Once BS2 and BS3 have been switched on, the next step consists in creating new virtual flow-based monitoring services in those base stations. To this end, virtualization policies allow creating and dismantling virtual network resources to ensure the provision of service. Regarding the use case, the next virtualization policy creates two virtual flow-based network monitoring services in BS2 and BS3 when these base stations have been switched on, and when the flow monitoring service of BS1 is congested.

Type(#Virtual) ∧ BaseStation(?bs) ∧ Location(?bs,?area) ∧
locatedBS(?area,?neighborBSs) ∧ hasMonitorServ(?bs,?serv) ∧
hasStatus(?neighborBSs,#ON) ∧
integer[MFPS in #RedAlert] hasMFPS(?serv)
→ createService(?neighborBSs,#FlowMonitor)

3) Balancing policies: Finally, the last step consists in balancing the network flows between the existing flow-based monitoring services allocated in BS1, BS2, and BS3. To this end, our solution defines balancing policies in charge of zoom in/out the cover areas of the base stations to balance the network traffic between close base stations. The next policy indicates that when the flow-based monitoring service of a BS is congested and the monitoring service deployed by the previous policy has been instantiated, the network should balance the traffic load.

Type(#Balancing) ∧ BaseStation(?bs) ∧ Location(?bs,?area) ∧
locatedBS(?area,?neighborBSs) ∧ hasMonitorServ(?bs,?serv) ∧
hasFlowMonitorStatus(?neighborBSs,#deployed) ∧
integer[FPS in #RedAlert] hasMFPS(?serv)
→ balance(?bs,?nearBs)

4) Architecture: To manage automatically the network resources with the goal of ensuring the provision of flow-based monitoring services, we have defined an architecture oriented to the SDN paradigm. Fig. 2 shows this architecture, where the *SDN plane* contains the layers of the SDN paradigm and the *SDN management plane* depicts the components of our solution.

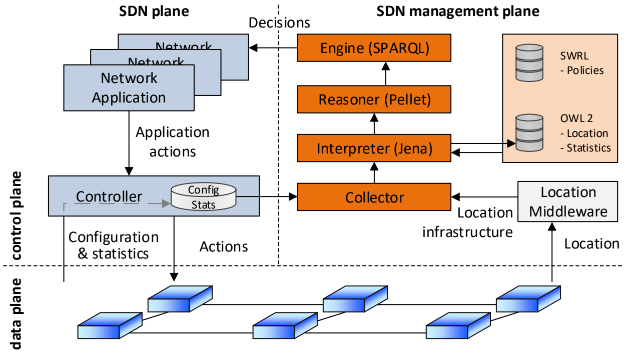


Fig. 2. Architecture to manage efficiently the network resources

From bottom to top, the *Collector* joins the infrastructure location, provided by *Location Middleware*, with the network configuration and statistics received from the *Controller*. The *Interpreter* component receives the previous information and stores all this information. The *Reasoner* component receives the stored information and the policies defined by the network administrators and generates new knowledge. Finally, the *Engine* is in charge of transferring the actions defined by the policies to the SDN applications, which will enforce the corresponding actions over the network.

III. Conclusions

In this paper, we have proposed an SDN-oriented system to manage at real-time the network resources to ensure the analysis of network flows generated by potential attackers. To manage automatically the network resources our proposal defines a set of policies that allow the network administrator to switch-on/off, balance, or create/dismantle physical and virtual network resources to guarantee the provision of service.

Acknowledgements

This work has been supported by a Séneca Foundation grant within the Human Resources Researching Training Program 2014, the European Commission Horizon 2020 Programme under grant agreement number H2020-ICT-2014-2/671672 - SELFNET (*Framework for Self-Organized Network Management in Virtualized and Software Defined Networks*), the Spanish MINECO (project DHARMA, *Dynamic Heterogeneous Threats Risk Management and Assessment*, with code TIN2014-59023-C2-1-R), and the European Commission (FEDER/ERDF).

References

[1] A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, G. Martínez Pérez. "Policy-based management for green mobile networks through Software-Defined Networking", Mobile Networks and Applications, Springer Mobile Networks and Applications, Published online 05 December 2016