Towards an Agent-based NOX/OpenFlow Platform for the Internet

Alexandre Passito, Edjard Mota, Rodrigo Braga

[1]Laboratório de Computação Inteligente e Autônoma (LabCIA)
Departamento de Ciência da Computação (DCC)
Universidade Federal do Amazonas (UFAM)
Manaus – AM – Brazil

{passito,edjard,rodrigo.braga}@dcc.ufam.edu.br

Abstract. *Concerns about security, mobility, routing, quality-of-service, middle-boxes led to revisions in the basic architectural framework of the Internet, such as new schemes for addressing, new features for switching/forwarding equipment and deployment of new services using overlay networks. Some of these revisions depend on network domains to cooperating in order to achieve scalability. For example, [Liu et al. 2008] proposes a filter-based DDoS defense system which depends on an infrastructure service to be deployed for each network domain in order to block attack traffic. Somewhat solution seems hard to be applied at large scale because each network has its own administrative boundaries and internal policies, and incentives to cooperation can be hard to achieve.*

To tackle the highly distributed nature of the Internet and such increasingly complex interactions, each administrative domain should be modeled as an autonomous society of agents (or a multiagent system). A multiagent system, [Wooldridge 2009], is one that consists of a number of agents, which interact with one another on behalf of owners with different goal and motivations. In order to successfully interact, these agents will thus require the ability to cooperate, coordinate and negotiate with each other.

This ongoing research aims to enhance network operating systems [Gude et al. 2008] with agent capabilities, such as reactivity, pro-activity and social ability. This approach will enable the building of artifacts for the autonomous control of networks, allowing networks to self-govern their behavior, but only within the constraints of the goals that the system as whole seeks to achieve. To tackle large scale Internet problems, social abilities like cooperation and negotiation is being used to make agents interact with other network domains. Using such high-level and centralized abstraction of the network will reduce the complexity of building agents in a too complex and often uncertain environment. This feature expressively reduces the burden to construct a translation layer into each agent to cope with different network vendors. From the network operating system viewpoint, agents are used as an efficient manner to build autonomous network control artifacts. Applications, now characterized as agents, can be used to build self-managed networks and exploring autonomous solutions for configuration, optimization, recuperation and protection.

The implementation/experimentation of the agent-based network operating system uses the NOX/OpenFlow [Gude et al. 2008] platform and is under development by LabCIA. Our preliminary result using the platform under construction

is self-protecting networks against flooding DDoS attacks [Braga et al. 2010]. The detection method uses Self Organizing Maps, an unsupervised artificial neural network, trained with features of the network traffic. Taking advantage of the abstraction layer, it is possible to extract flow-based information from all OF switches registered by NOX. Furthermore, there is great flexibility to add/remove OF switches into/from the detection loop. The benefit of this possibility is that if there is a change in the network topology, it is possible to autonomously adapt to it adding switches more relevant to detection or removing those less important. This new method also yielded low rates of false alarms and high rates of attack detections using flow information instead of per-packet information.

For mitigating detected attacks, we plan to allow the cooperation between agents from different network domains. For example, if network A detects that an attack has been launched, it could inform B that is under attack and ask B to filter the packets in the origin. After negotiation, B uses network biddings of NOX/OpenFlow to block the attack source.

We stand on the assumption that OpenFlow will gradually be adopted by network domains. OpenFlow is not a toy protocol. It makes part of a world-wide consortium trying to innovate in networks research and its deployment is reaching large scale infra-structures like GENI and Internet2. Additionally, a new proposal of IP and Transport unification through OpenFlow increases its possibility to future large scale adoption. As soon this assumption holds, our research will be valuable to show how intelligent scalable architectures can be used to build the future Internet.

References

Braga, R., Mota, E., and Passito, A. (2010). Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow. In *Under submisstion to IEEE Conference on Local Computer Networks (LCN)*.

Gude, N., Koponen, T., Pettit, J., Pfaff, B., Casado, M., McKeown, N., and Shenker, S. (2008). NOX: Towards an Operating System for Networks. *ACM SIGCOMM Computer Communication Review*, 38(3):105–110.

Liu, X., Yang, X., and Lu, Y. (2008). To filter or to authorize: Network-layer DoS defense against multimillion-node botnets. In *ACM SIGCOMM*, pages 195–206. ACM.

Wooldridge, M. (2009). *An Introduction to MultiAgent Systems*. John Wiley & Sons, 2 edition.

Biographies

Alexandre Passito is M.Sc. (2008) and Ph.D. student in Informatics (UFAM).

Edjard Mota is Ph.D in Artificial Intelligence (The University of Edinburgh, 1998).

Rodrigo Braga is M.Sc. student in Informatics (UFAM).