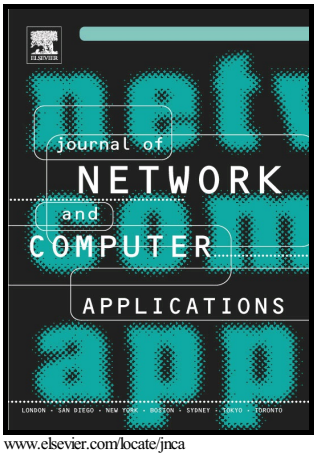
BDI2DoS: an Application using Collaborating BDI Agents to Combat DDoS Attacks

Ingrid Nunes, Frederico Schardong, Alberto Schaeffer-Filho



www.elsevier.com/locate/jnca

PII: S1084-8045(17)30057-7
DOI: http://dx.doi.org/10.1016/j.jnca.2017.01.035
Reference: YJNCA1851

To appear in: *Journal of Network and Computer Applications*

Received date: 9 August 2016
Revised date: 13 December 2016
Accepted date: 30 January 2017

Cite this article as: Ingrid Nunes, Frederico Schardong and Alberto Schaeffer Filho, BDI2DoS: an Application using Collaborating BDI Agents to Comba DDoS Attacks, *Journal of Network and Computer Applications* http://dx.doi.org/10.1016/j.jnca.2017.01.035

BDI2DoS: an Application using Collaborating BDI Agents to Combat DDoS Attacks

Ingrid Nunes[a,b], Frederico Schardong[a,*], Alberto Schaeffer-Filho[a]

[a] *Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre, Brazil*
[b] *Department of Computer Science, Technische Universität Dortmund, Dortmund, Germany*

Abstract

Computer networks are critical to many tasks in our daily lives. Therefore, mechanisms that guarantee the resilience of the network must be provided. Different approaches have been proposed to address potential challenges to network operation, but they rely on rigid solutions, which work only in anticipated scenarios. To address this issue, this paper presents BDI2DoS, which is a multi-agent innovative application that ensures the resilience of networks against the widely known Distributed Denial-of-Service (DDoS) attack. We take an existing network resilience strategy based on event-condition-action (ECA) policies to combat DDoS attacks, and use it as a requirement to specify the behaviour that must emerge from the interaction among agents, which together are capable of detecting and remediating anomalies that are considered a DDoS threat, in a flexible way. Agents in our multi-agent system follow the widely used BDI architecture, and were implemented with the BDI4JADE agent platform. In order to evaluate the effectiveness of BDI2DoS, we used the PReSET resilience simulator and BDI4JADE to build an integrated testbed. Our experiments compare the effectiveness of the ECA and the BDI-based resilience strategies and show that the latter is more flexible and able to cope with problems that occur during the execution of the anticipated behaviour.

Keywords: Network Resilience, Multi-agent Systems, BDI Architecture

1. Introduction

Network resilience is the key to provide reliable, robust and efficient network operation. Resilience is the ability of the network to maintain an acceptable level of operation when confronted with *challenges*, *e.g.,* equipment failures, device misconfiguration, or malicious attacks [1, 2, 3]. Ensuring network resilience has become critical nowadays given that many tasks in our daily lives rely on networked infrastructures.

Research on network resilience has combined contributions from different research areas, mainly machine learning [4] and autonomic computing [5, 6]. Some approaches provided agent-based solutions [7, 8, 9], in which agents collaborate in a sequential pre-defined way. An agent [10, 11] is a software component with autonomous and proactive behaviour, situated in an environment and with social ability. However, these approaches fall short of *emergent behaviour*, which is a key property of multi-agent systems. Moreover, there are many unexploited domain-neutral agent-based approaches, which can arguably provide flexible solutions to handle situations unpredicted at design time [12].

In this paper we exploit one particular agent-based approach to achieve network resilience: the belief-desire-intention (BDI) architecture [13], which separates the motivational state of a system from its deliberative state. Additionally, given that goals are explicitly represented, alternative ways of achieving them may be executed, when there is a failure in the execution. Using the BDI architecture, we developed BDI2DoS, an innovative application composed of a set of agents that combined form multi-agent collaborations comprising mechanisms capable of detecting and remediating *Distributed Denial-of-Service (DDoS)* attacks. In particular, we take an existing network resilience strategy based on event-condition-action (ECA) policies to combat DDoS attacks [14], and use it as a basis to specify the behaviour that must emerge from the interaction among agents. Traditionally, ECA policies have been used in network management as a means of specifying system behaviour [5, 15, 16, 17]. The decision-making process is purely reactive, and policy actions are performed when specific events occur and if certain conditions are met. Differently from the pre-specified interactions defined by ECA policies, a key issue associated with the BDI2DoS design is how to identify the possible local interactions that must occur between agents in order to make the application detect and contain the attack.

Our design consists of a set of capabilities that can be added to agents. Each capability has a set of rules used as part of the agent reasoning process together with a set of plans to achieve goals. Although plans are simple, they effectively provide agent coordination, and it is the interplay among decoupled agent parts (rules and plans) that

*Corresponding author.
Email addresses: ingridnunes@inf.ufrgs.br (Ingrid Nunes), fschardong@inf.ufrgs.br (Frederico Schardong), alberto@inf.ufrgs.br (Alberto Schaeffer-Filho)