available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Toward cost-sensitive self-optimizing anomaly detection and response in autonomic networks☆

Zonghua Zhang[a,*], Farid Naït-Abdesselam[b], Pin-Han Ho[c], Youki Kadobayashi[d]

[a] Institut Telecom/Telecom Lille1, France
[b] Universite Paris Descartes, Paris V, France
[c] University of Waterloo, Canada
[d] NICT, Japan

ARTICLE INFO

Article history:
Received 24 February 2011
Received in revised form
10 May 2011
Accepted 5 June 2011

Keywords:
Autonomic network
Auto defense
Anomaly detection and response
Reputation management
MANET

ABSTRACT

While anomaly detection and response play a significant role in attaining auto defense, one of core functionalities of autonomic networks, the design and deployment of Anomaly Detection and Response Systems (ADRS) herein is a non-trivial issue because of the special network characteristic, namely self-managing, which requires candidate ADRS to automatically and optimally balance performance objectives and potential negative consequence. In this paper, we propose a decision-theoretic framework to systematically analyze ADRS in autonomic networks, with an objective to achieve its cost-sensitive and self-optimizing operation. In particular, each ADRS agent is viewed as an autonomous entity, making decision as its local operating environment. A global reward signal is then used to quantify the performance of ADRS as a whole in terms of those identified metrics. Furthermore, the analytical framework serves as a basis for developing an adaptive, robust, and near-optimal prototype termed ARSoS, along with a reinforcement learning algorithm for approximately inferring the optimal behavior of a reputation-based ADRS in a specific autonomic network variant, mobile ad-hoc network. The performance of ARSoS is validated through extensive simulations.

1. Introduction

The rapid development of computer network and communication technology has significantly enhanced the accessibility to Internet services, providing versatile ubiquitous computing that enables high-speed and high-quality information exchange between mobile devices located anywhere in the globe. As one of the most promising network technology, autonomic networks aim to overcome the rapidly growing complexity of computing systems management, and to reduce the barrier that complexity poses to the further growth of the Internet and other networks. This type of network is composed of flexible, dynamic, and fully autonomous network entities, which can (re)organize the network in accordance with the working, economical, and social needs of the users and organizations by the means of either wired or wireless communication. In practice, the emerging autonomic network variants include Mobile ad-hoc networks (MANET), vehicular ad-hoc network (VANET), and wireless sensor networks (WSN).

☆ This work was supported by Nano fund of Information Security Research Center of NICT, Japan. It was done when the author was with NICT.

* *Corresponding author.*
E-mail address: zonghua.zhang@telecom-lille1.eu (Z. Zhang).

0167-4048/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2011.06.002

Despite the promising features of autonomic network, its application and performance would be dramatically impeded if security cannot be preserved. Like other network counterparts, some proactive security mechanisms relying on cryptographic primitives such as authentication, authorization, and access control can be adopted, but the unique network characteristics deter the construction of a clear in-depth defense line since novel vulnerabilities are continuously introduced, exposing the network to sophisticated attackers (Chess et al., 2003; Dobson et al., 2006; Huebscher & McCann, 2008). Auto defense is therefore a fundamental property that must be ensured, representing a dynamic and adaptive mechanism that reacts to attacks on the network infrastructure. To enable that, anomaly detection and response is one of the key approaches, which aims at discerning anomalous events from system normalities that are characterized by legitimate event samples and dealing with the negative consequence.

While a large variety of anomaly detection and response systems (ADRS)[1] have been developed and expected to be self-managing, distributed, scalable, and light-weight, the minority can be readily applied to autonomic networks due to several facts: (1) since autonomic networks are self-managing and network nodes are autonomous and possibly mobile, there is neither a well-defined network boundary for perimeter defense nor a fixed infrastructure for supporting the deployment of ADRS; (2) it becomes more complex in wireless context where data delivery and collaborative service rely on a shared medium, thereby suffering reliability issues on communication links, introducing novel vulnerabilities that are different from those of traditional network paradigms; (3) it lacks a formal way that can assist ADRS in automatically taking appropriate response to handle the identified anomalous events, meanwhile optimally balancing its performance objectives and potential negative consequence. For instance, ADRS developed for MANETs cannot be solely evaluated in terms of detection accuracy and false positive rate, while the operational cost regarding detection and response should be examined as well, since an ADRS with non-negligible overhead is always undesirable. From a systematic perspective, it is significant to identify the trade-off between detection performance and operational cost of an ADRS in MANET in order to achieve the best detection performance with the minimum operational cost.

Motivated by those key observations, we make three contributions. First, we consider a set of performance metrics for specifically evaluating ADRS in autonomic networks, and formulate the self-optimizing operation of ADRS as a distributed optimization problem with some practical constrains. Second, the cooperative behavior of anomaly detectors (ADs) is characterized as Multi-agent Partially Observable Markov Decision Process (MPO-MDP), allowing us to examine the fundamental trade-off between the key performance metrics in a formal way, ultimately leading to the self-optimizing operation of ADRS; Third, we develop an adaptive, robust and near-optimal deployment strategy, termed ARSoS, along with a reinforcement learning algorithm to automatically infer the behavior of reputation-based ADRSs in a specific autonomic network variant, MANET, in terms of the identified performance metrics.

The remainder of this paper is organized as follows. Related work is given in Section 2. We discuss anomaly detection and response in autonomic networks in Section 3. We then present an analytical framework to formally analyze the behavior of ARDS in Section 4. In Section 5, a prototype, which is called ARSoS, is developed in a MANET scenario. Section 6 reports the simulation results. The paper is concluded in Section 7.

2. Related work

Our work intersects with three research tracks: anomaly detection and response in autonomic networks, performance evaluation of ADRS, and optimal deployment of anomaly detectors in distributed environments.

2.1. *Anomaly detection and response in autonomic networks*

Anomaly detection plays a vital role in autonomic networks, diagnosing both accidental system errors and intentional attacks for ensuring dependable and secure networking operations (Huebscher & McCann, 2008). Due to the self-managing nature of autonomic networks, anomaly detection is always tightly integrated with automated response, achieving auto defense functionality. In particular, incentive-based mechanisms, which are classified into reputation-based system (Buchegger & Le Boudec, 2002; He et al., 2004; Zhang et al., 2008) and credit-based systems (Zhong et al., 2003), can be regarded as a special variant of ADRS. Such systems associate reputation or credit with node behavior for encouraging the nodes to cooperatively fulfill network functionalities. In addition, anomaly detection systems in wired networks have also been modified for autonomic networks by exploring particular network characteristics. For instance, ADRS reported in (Huang & Lee, 2003; Mishra et al., 2004; Tseng et al., 2006) are fully distributed, adaptive and light-weight, considering the fact that nodes in MANETs are mobile and resource-constrained. In this paper, we exemplify and examine reputation-based ADRS, particularly a reputation-based ADRS proposed in (Zhang et al., 2008).

2.2. *Performance evaluation of ADRS*

Unlike those ADRS in wired networks, the performance evaluation of ADRS in autonomic networks primarily relies on simulations. Neither a benchmark experimental dataset such as the MIT DARPA Intrusion Detection Evaluation Data Sets (Mit Darpa) nor a solid analytical framework like information-theoretic measures (Lee and Xiang, 2001) (along with commonly recognized evaluation metrics) has been developed. In the studies by Baras et al. (2007), Radosavac et al. (2007), Radosavac et al. (2008), a set of game-theoretic techniques was applied for analyzing the performance of intrusion

[1] We generally assume that anomaly detection and response are integrated together even though they are always treated independently in wireline networks. We also assume that an ADRS consists of distributed anomaly detectors, or AD for short.