Ad Hoc Networks 9 (2011) 687–697

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Trust management for multimedia P2P applications in autonomic networking

Florina Almenárez *, Andrés Marín, Daniel Díaz, Alberto Cortés, Celeste Campo, Carlos García-Rubio

Telematic Engineering Dept., University Carlos III of Madrid, Avda. Universidad, 30, 28911 Leganés, Madrid, Spain

ARTICLE INFO

Article history:
Available online 1 October 2010

Keywords:
Trust management
Trust attacks
Multimedia P2P applications
Autonomic networking

ABSTRACT

In the last years, trust management has become a fundamental basis for facilitating the cooperation between different users in peer-to-peer (P2P) multimedia applications within autonomic networks. In these networks and applications, trust management should fulfill certain requirements (i.e. decentralisation, dynamism, simplicity, interoperability, etc.) for being functional. In this paper, we propose an evolutionary model of trust management that captures dynamic entities' behaviour over time. Likewise, we explain protection mechanisms against several attacks, which are based on the cooperative behaviour of the entities, trust relationship properties, and trust rules. Finally, we successfully validate our model from several scenarios and compare it with other proposals in this field.

1. Introduction

Autonomic networking requires networks can learn and reason to provide self-mechanisms that enable a user to accomplish securely her tasks without regarding device, media, and/or technology [32]. These networks emerge due to the proliferation of mobile devices such as smartphones, PDAs, networked audio and video equipment and game consoles, that interact to provide multimedia and interactive content such as photos, video, online gaming, and the convergence of these and wired networks in order to supply seamless services to the end user, guaranting freedom of movement while maintaining continuity of applications. Today there is a strong need for receiving multimedia content through mobile handheld devices [22].

Such services in autonomic networking are characterized by lacking of: (a) an administrator dedicated to the configuration, management, and maintenance of the system; (b) a fixed infrastructure to control all the relationships (ad-hoc) that are formed; and (c) a space with heterogeneous peers regarding capabilities and behaviour. Thus, management and security of these networks are a critical issue considered by a wide range of researchers. For that, trust management has recovered a big interest as basis of the security solutions, and Digital Rights Management (DRM) approaches, etc. Nevertheless, little effort has so far been put into the investigation of multimedia distributed applications using autonomic networks.

Trust is a measure that describes the trustworthiness of individual entities based on previous knowledge, common knowledge, and monitoring schemes. Thus, trust management requires a constant feedback, because trust is not static; on the contrary, trust changes over time. So, one of the main challenges in trust management is to model the trust evolution in a suitable way. So, we propose a novel evolutionary model, that unlike other models proposed, contributes to:

- addressing the evolution beyond a posteriori probabilities from previous behaviour. We also take into account negative behaviour for penalizing it. This attempts to

* Corresponding author. Tel.: +34 916248799.
E-mail addresses: florina@it.uc3m.es (F. Almenárez), amarin@it.uc3m.es (A. Marín), dds@it.uc3m.es (D. Díaz), acortes@it.uc3m.es (A. Cortés), celeste@it.uc3m.es (C. Campo), cgr@it.uc3m.es (C. García-Rubio).
URL: http://pervasive.gast.it.uc3m.es/ (F. Almenárez).

1570-8705/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2010.09.005

model it like real life. The curve of positive behaviour is different from usual logarithmic curve.
- capturing the subjective nature of trust by using fuzzy logic as well as probabilities.
- including parameters easily measured mathematically. In addition it uses simple mathematical operations to be executed by limited devices reducing the overhead added. Only it requires actions configured by the service developers, for instance Apache server.
- formalizing trust properties and added more properties until now.
- changing the perspective of using trust management like reputation systems. In this case, the model is mainly focused on supporting the service.

This article is organized as follows. Section 2 identifies the main challenges of trust management for autonomic networking and P2P multimedia applications. Section 3 describes our approach, including the formal trust relationship properties and the evolutionary model. Section 4 describes the mechanisms used to defend evidence-based trust management against several attacks. Section 5 successfully validates the evolutionary trust model whose behaviour is a good representation of trust management in the real life. Section 6 contains the evaluation of the trust management model using OMNET++ 4.1 and an the implementation of a prototype. Section 7 briefly explains the related work, comparing the approaches in accordance with the requirements identified previously. Finally, Section 8 presents conclusions and issues to be addressed in future work.

2. Requirements of trust management

(a) *Decentralized management*. Each entity manages its own security. They are autonomous agents to make individual decisions on configuration, management, trust, etc. Due to open dynamic environments, trust relationships are established in an ad-hoc and peer-to-peer way. The dependence on a central device should be avoided.

(b) *Simplicity as regards usability and performance*. The model is oriented to final users, therefore, it must be very simple to manage. It introduces parameters that can be mathematically obtained, instead of abstract and subjective parameters that often require human intervention. In the other direction, the performance requirements should be low enough that it can be included in any device, in order that any entity can use it anytime, anywhere, and in any network.

(c) *Cooperation between participant nodes*. Making use of the common knowledge is allowed by the cooperation between trusted entities. Information could be locally distributed among different entities. In this way, entities cooperate to manage the network.

(d) *Adapt to dynamic situations*. Both trust establishment and support should be dynamic. Firstly, trust relationship establishment between unknown entities should be permitted. Secondly, trust is not static; this might gain or lose over time. For this, entity's behaviour should be monitored to get feedback during each interaction.

(e) *Support context-awareness*. An entity can vary its rules according to the environment where is roaming, for example, to participate in an online game is different from to offer personal videos. In general, traditional applications work in static environments with fixed infrastructure.

(f) *Interoperable with deployed security solutions*. All devices support traditional security mechanisms such as X.509 certificates, SSL, and cryptographic algorithms, in order to establish secure communications with remote servers; therefore, trust management must be compliance with these mechanisms.

(g) *Modelling distrust and uncertainty*. Distrust is as important as trust, so malicious entities should be identified to avoid any interaction with them. Besides, in open environments, imperfect knowledge about other entities is an inherent property of trust relationships.

(h) *Granularity for the trust assessment*. Although it is not an essential requirement, granularity provides a more accurate assessment than deterministic values. For example, Is the marginal trust degree (in PGP [37]) more towards up or towards down?

(i) *Prevention of attacks*. Due to the fact that pervasive devices are more exposed to receive attacks and the critical role of trust management systems, the model should be able to auto-defend against attacks and warn user of them. For that, threats should be detected and identified to define effective defensive responses.

3. Pervasive Trust Management (PTM) model

In this section, we give an overview about our trust management model, called *Pervasive Trust Management* (PTM) [4,6], which considers trust as a general concept instead of a situational concept. Although it has been defined, in this paper we focus on to formalize trust properties using temporal logic, and define and validate mathematical trust evolution mechanism. It – based on Luhmman's ideas [23] – attempts to take the trust management in the real world to the digital world. PTM has been designed under the principle: *"trust comes on foot and goes by horse"*, just as Nielsen states: *"It [trust] is hard to build and easy to lose"* [26].

3.1. Trust relationship properties

Trust relationships can be – generally – established in two ways: direct (DTR) and indirect (ITR). The Fig. 1 depicts it. A direct trust relationship is established without intervention of third parties, for example, the trust relationship A has in B ($T(A \rightarrow B)$). On the contrary, indirect trust relationships are established with the help of third parties, for instance, the trust relationship A has in C, and in D through B. This last one is also known as *derived trust relationship*. Third parties can be persons or a specific system.