Ad Hoc Networks 19 (2014) 142–155

Contents lists available at ScienceDirect

Ad Hoc Networks

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

An accurate and precise malicious node exclusion mechanism for ad hoc networks

Lyno Henrique G. Ferraz [a,*,1], Pedro B. Velloso [b], Otto Carlos M.B. Duarte [a]

[a] Universidade Federal do Rio de Janeiro – GTA/POLI-COPPE/UFRJ, Rio de Janeiro, Brazil
[b] Universidade Federal Fluminense – IC/UFF, Niterói, Brazil

ARTICLE INFO

Article history:
Received 21 March 2013
Received in revised form 18 February 2014
Accepted 2 March 2014
Available online 12 March 2014

Keywords:
MANET
Security
Access control
Trust model

ABSTRACT

Mobile ad hoc networks are attractive due to the wireless communication, infrastructureless design, and the self-organized mobile nodes. These features, however, introduce vulnerabilities, since there are no centralized control elements and the communication depends on cooperation of nodes. We propose a robust and distributed access control mechanism based on a trust model to secure the network and stimulate cooperation by excluding misbehaving nodes from the network. The mechanism divides the access control responsibility into two contexts: local and global. The local context responsibility is the neighborhood watch to notify the global context about suspicious behavior. In its turn, the global context analyzes the received information and decides whether it punishes the suspicious node using a voting scheme. We model the exclusion mechanism and perform a parameter analysis. Simulation results prove that the combination of voting and trust schemes provides an accurate and precise classification and node exclusion mechanism, even though in scenarios of limited monitoring.

1. Introduction

Mobile ad hoc networks (MANETs) lack physical infrastructure and centralized control. In this kind of network, the node itself plays the roles of router, server and client. However, nodes should perform these roles altruistically to assure proper network operation. Nevertheless, a node may misbehave and fail to cooperate, because it is overloaded, broken, or due to selfish and even malicious behavior. Thus, an access control mechanism that stimulates cooperation and also allows only well behaving nodes in the network is crucial for the correct operation of the network.

Security in ad hoc networks is often accomplished with the use of an access control mechanism in conjunction with an authentication scheme to validate users identities, hence only authenticated nodes can participate and use network capabilities. Authentication assures the correct node identification but does not ensure that it will cooperate and behave as expected, as nodes still can change their conduct and misbehave intentionally or due to resource constraints. Likewise, an altruist node that experiences an occasional communication failure and fail to cooperate should still be part of the network. Therefore, the adoption of a naive protocol or mechanism, which does not consider the existence of misbehaving nodes degrades the performance of the network [1]. A mechanism that distinguishes altruist nodes from the misbehaving ones, and limits the misbehaving access to resources is essential to secure and improve the network performance [2].

[*] Corresponding author. Tel.: +55 21 2562 8635.
E-mail addresses: lyno@gta.ufrj.br (L.H.G. Ferraz), velloso@ic.uff.br (P.B. Velloso), otto@gta.ufrj.br (O.C.M.B. Duarte).

[1] Grupo de Teleinformática e Automação – GTA, Universidade Federal do Rio de Janeiro (UFRJ), P.O. Box 68504, 21945-972 Ilha do Fundão, Rio de Janeiro, RJ, Brazil.

http://dx.doi.org/10.1016/j.adhoc.2014.03.001
1570-8705/© 2014 Elsevier B.V. All rights reserved.

In this paper, we propose the Trust-based Exclusion Access-control Mechanism (TEAM), a robust node exclusion mechanism that allows an accurate and precise access control. TEAM uses a distributed and self-organized two-level trust and reputation system inspired by a jury trial. The system controls node access to the network, monitors node behavior, and excludes misbehaving nodes. Using the jury trial model, the access control is achieved by a combination of witnesses and juries. The witnesses use an accurate and scalable trust model based on local interactions to identify the nature of the defendants, their one-hop neighbors. Then, the witnesses rate the defendants a trust level and notify the jury of each defendant about their behavior. The local trust model produces more accurate information to be sent to the juries and avoids multihop communication overhead. When the jury receives the notification about selfish/malicious defendant behavior, it votes for the exclusion of that defendant. The voting mechanism is important because it requires the majority of the jury agreement, validating the local behavior analysis securely in a global context. For each defendant, our mechanism randomly selects a set of nodes in the network to compose the jury. We present a simple analytical model of TEAM, which represents its basic behavior and allows us to understand the impact of the main parameters in the control access efficiency. We also evaluate TEAM, through simulations, under different configurations and scenarios, comparing to the closest related work in literature. Results show that the proposed TEAM mechanism excludes nodes accurately and precisely with a low message overhead.

The paper is structured as follows. In Section 2, we describe the main related works. In Section 3, we present the architecture of the access control mechanism and, in Section 4 we analyze the reputation model used. In Section 5 we present the simulations and results. Finally, we conclude this paper in Section 6.

2. Related work

Misbehaving and selfish behavior nodes degrade the performance of routing [3], address allocation [4], and access control mechanisms [5]. Several proposals focus on selfish behavior prevention to enforce cooperation and embed the cooperation in routing protocols [6–8]. These approaches, however, do not focus on network security and, consequently, they do not have means to detect and punish malicious behavior.

Other proposals use a mechanism to monitor the environment to identify and exclude misbehaving, malicious, and selfish nodes.

Non-centralized schemes are mandatory for securing ad hoc networks a distributed secure approach consists of using threshold cryptography [9–11], but the need for an administrator to manage membership or select and configure a group of nodes persists. Arboit et al. [12] propose an accusation-based scheme in which nodes monitor their neighbors to send accusations whenever they detect misbehavior from the vicinity. Nodes use the received accusations to assign a trustworthiness value to all other nodes in the network, and revoke their certificate when the sum of accusations is greater than a configurable threshold. In order to improve the accuracy of the certificate revocation mechanism, the accusations have variable weights that depend on the node reliability, which are calculated based on the past behavior. The nodes in this mechanism, however, maintain data and receive accusations from all other nodes to assign the trustworthiness value. Martignon et al. propose a complete scheme to detect selfish behavior in Wireless Mesh Network based on both direct observations of neighbors and indirect information provided by other mesh routers. The scheme is incorporated in Ad hoc On-Demand Distance Vector (AODV) routing protocol, so routers exchange recommendations to assign a trustworthiness value. The routers also consider the trustworthiness of others to weight the recommendations, but they also have to maintain data and receive trustworthiness information from all other nodes.

Assure a fast and efficient certification revocation to exclude a node is actually a challenge in ad hoc networks. Kato et al. [13] propose a cluster-based approach in which only the cluster head node sends a revocation message. Thus, one message is enough to revoke a certificate, which reduces the exclusion delay, in contrast to the voting schemes. However, the accuracy and efficiency of the exclusion mechanism is not addressed.

Lai et al. [9] use self-organized and self-generated public keys to propose a key revocation and renewal scheme. In their proposal, an outside trusted entity issues keys, which authorize the node participation in the network. The key revocation of misbehaving nodes uses an accusation mechanism based on a neighborhood watch a controlled flooding, in which nodes propagate an accusation in a limited range. The propagation of the accusations is secured against forging via unicast authenticated messages. However, in order to the key revocation be globally known, each accusation must be propagated to the entire network, which causes processing and control message overhead.

Fernandes et al. proposed A Controller-node-based Access-Control mechanIsm for Ad hoc networks, called ACACIA [14], a distributed access control and authentication system without the need of a centralized Certification Authority. ACACIA is a self-organized monitoring and certificate management system, which controls the admittance of nodes and purges misbehaving nodes. The proposal avoids the use of a central administrator to control node access, using of the relationship of users to control network access. This proposal uses randomly chosen sets of nodes to control the admittance of nodes in the network and the exclusion of misbehaving nodes. Furthermore, the system uses a neighborhood watch mechanism, which constantly generates accusation messages to the random controller sets. Then, these controller sets appraise a reputation to the nodes depending on the incoming rate of accusation messages, and exclude the nodes with low reputation. Therefore, the system drawback is the high control-message overhead, and the low reputation accuracy on different network conditions, such as number of neighbors that generate different reputation values.

In this paper, we propose TEAM, an access control mechanism to cope with node misbehavior in ad hoc networks.