Computer Communications 71 (2015) 119–128

Contents lists available at ScienceDirect

Computer Communications

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

DISIDE: Distributed strategy identification in opportunistic mobile networks

Sujata Pal, Sudip Misra*

School of Information Technology, Indian Institute of Technology, Kharagpur, West Bengal 721302, India

ARTICLE INFO

Article history:
Received 8 November 2014
Revised 3 June 2015
Accepted 30 August 2015
Available online 8 September 2015

Keywords:
Opportunistic mobile networks
Strategy identification
Cooperation

ABSTRACT

The distributed nature of routing protocols in Opportunistic Mobile Networks (OMNs) allows nodes to behave non-cooperatively for forwarding other nodes' messages. So, the identification of different behaviors of nodes is one of the important issues in OMNs. In this paper, we propose a *Distributed Strategy Identification Scheme* (DISIDE), using which a node identifies other nodes' strategies locally. In the proposed scheme, a node learns from its own observation, while receiving or forwarding messages to other nodes. In addition, it learns from other nodes by exchanging information. Based on these observations, each node identifies other nodes' strategies in a distributed manner. We implement DISIDE on different routing protocols with the existing cooperative strategy adaptation scheme, DISCUSS. Simulation results show that the detection efficiency of the network varies between 70–100% in real, map based and random entity mobility models.

1. Introduction

Opportunistic Mobile Networks (OMNs) are variants of Delay Tolerant Networks (DTNs), in which the mobility of nodes creates opportunities for transferring messages between any pair of source–destination nodes [1]. A node in an OMN not only receives and sends its own messages, but also does the same for the other nodes. So, cooperation plays an important role for transferring messages of other nodes in OMNs. However, not all nodes in an OMN are cooperative in their behavior. Some nodes do not want to receive and forward messages created by (or destined for) other nodes; some nodes may even receive and drop such messages. This non-cooperative behavior degrades the system's performance. The identification of such kind of behaviors is a pressing concern in OMNs, because the nodes are not under the control of any central authority. We detect nodes' behavior "on-the-fly", based on the receiving and forwarding actions on messages of other nodes.

The identification of behaviors of nodes is challenging in the absence of a central server. Unlike the existing works (such as, [2] and [3]) the proposed solution does not need any central server, judge node, or trusted authority. Our scheme is fully distributed and in this scheme, each node individually detects the behavior of the other nodes based on the observation history. Similarly, many other misbehavior detection schemes exist for mobile ad hoc networks [4–8], which detect routing misbehavior and mitigate them. However, these works are not suitable for OMNs due to the existence of strong intermittent inter-node connectivity.

In this paper, we consider three behaviors of nodes namely, cooperate, exploit, and isolate [9]. Some nodes, known as *cooperators*, are cooperative in receiving and forwarding the messages generated both locally and by other nodes in the network. Some of the other nodes, known as *exploiters*, take help from other cooperative nodes for forwarding their own messages without helping them in return. In addition, we consider a third kind of behavior *isolator*, where a node neither takes help nor provides so to the other nodes. In this work, we consider that although the nodes share meta data (such as, node identification address and routing information), they do not reveal their strategies (behaviors) to one another.

1.1. Motivation

In our earlier version of this work [10], we assumed that each node informs its node address, *as well as* its strategy to the other nodes. It may be noted that in DISCUSS [10], the nodes used such knowledge to evaluate the group-wise performance, based on which the nodes possibly changed their own strategies. Message delivery ratio of the network increases, if most of the nodes choose their strategies as cooperators. However, in practice, nodes in an OMN may not share information about their own strategy with others. For example, in real world, a selfish or malicious node would not inform others about its actual behavior. In fact, it is likely that a malicious node would falsely claim itself to be cooperative. This work, however, does not deal with the aspects of trust and malicious nodes. In this work, we consider three social strategies of the nodes namely, cooperate, exploit, and isolate. Even in such a scenario,

* Corresponding author. Tel.: +91 3222 282338.
E-mail address: sudip_misra@yahoo.com, smisra@sit.iitkgp.ernet.in (S. Misra).

http://dx.doi.org/10.1016/j.comcom.2015.08.020
0140-3664/© 2015 Elsevier B.V. All rights reserved.

the nodes – especially the exploiters – are unlikely to inform their non-cooperative behavior to others. Therefore, it is essential that a node is able to identify the strategy of other nodes based on the interactions with the other nodes. The terms "strategy" and "behavior" are used interchangeably throughout the manuscript.

In this work, we propose a DIstributed Strategy IDEntification (DISIDE) scheme, that detects other nodes' behaviors (strategies). A node detects the strategy of another node in two phases. In the first phase, a node (say, *B*) observes the behavior of another node (say, *C*) locally when it receives (forwards) messages from (to) *C*. In addition, *B* and *C* exchange their lists that contain information about other nodes. In the second phase, *B* identifies the strategy of *C* based on the information collected in the first phase.

1.2. Contributions

The specific *contributions* of this paper are as follows:

- We propose a distributed scheme, DISIDE, using which every node identifies the strategies of other nodes locally (i.e., without the help of any central authority).
- We study the compatibility of DISIDE with different routing protocols.
- Simulation based on synthetic map, random-way-point and several real-traces are conducted to evaluate the performance of the proposed scheme.
- We present a comparative performance analysis when DISCUSS [10] is used with and without DISIDE.

1.3. Organization

The remainder of this paper is structured as follows. Section 2 reviews the existing work. Section 3 introduces three types of node behavior. Section 4 describes the strategy identification scheme. Sections 5 evaluates the scheme 'DISIDE' and finally Section 6 concludes the work, while giving directions on how this work can be extended in the future.

2. Related work

Existing routing protocols, for instance, [11–16], assume that the nodes are well behaved and cooperative in forwarding messages created by (or destined for) other nodes. However, it is imperative that in different deployment scenarios (such as, in challenged environments) some nodes may exhibit non-cooperative behavior, which degrades the overall network performance. So, the detection of nodes' behavior in the presence of multiple such behaviors is an exigent problem of fundamental nature in these networks. In our earlier work, DISCUSS [10], we assumed that the nodes share their strategies with one another. In this work, we relax the assumption of sharing nodes' behaviors with one other, and propose a distributed strategy identification scheme that efficiently detects nodes' behavior. In the following, we review the state-of-the-art works in a closely related domain – misbehavior detection. Subsequently, we meticulously highlight how the current work differs from the existing works in the literature.

It may be noted that, the identification or detection of a misbehaving node is easier in the presence of a centralized server. In such case, the central server keeps track of behavior of all the nodes by collecting feedback from other nodes and accordingly, it (central server) blacklists the misbehaving nodes. However, the problem is challenging in a distributed environment. Ayday and Fekri [2] proposed 'ITRM', a graph-based iterative algorithm used for the detection of malicious nodes in DTNs. ITRM calculates the reputation of peers (who provide service to other peers) by collecting feedback from other peers (raters). Subsequently, it finds the trustworthiness of the raters themselves. ITRM selects an arbitrary node in the network as the *judge* node. The judge node collects feedback from others by using the rating tables formed by the other nodes (acting as judges themselves). After collecting sufficient feedback from the other nodes, the judge node calculates the reputation values of all the nodes using an iterative algorithm and detects the malicious nodes. For surviving in the network, the malicious nodes try to reduce packet drops. So, the judge node waits for longer time duration, when the packet drop rate of the malicious nodes is reduced. Ciobanu et al. [17] invented 'SENSE', a selfish node detection algorithm using incentive schemes that reduce the selfish behavior in opportunistic networks. When two nodes executing SENSE meet, they check their battery level and accordingly find their altruism values. Based on this, each node decides whether it should forward other nodes' data. Panos et al. [18] proposed 'SIDE', which monitors a node's behavior using a host-based detection engine and a remote attestation procedure for ensuring the integrity of the SIDE. Li and Cao [19] addressed routing misbehaviors and mitigated them in DTNs. They first detect packet dropping nodes and then mitigate misbehaving nodes in the routing process by limiting the traffic flowing through the misbehaving nodes. Li et al. [20] proposed another routing algorithm known as Social Selfishness Aware Routing (SSAR) that alleviates selfishness and provides an efficient routing in DTNs.

Costantino et al. [21] proposed a privacy-preserving friend proximity detection scheme for opportunistic networks, called interest-casting, that helps to deliver information to other users through multi-hop forwarding. Nicopolitidis et al. [22] proposed an adaptive artificial intelligence tool, in which, learning automata are used at the network nodes for detecting the routes least affected by licensed users. Zhu et al. [3] proposed 'iTrust' for detecting misbehavior in DTNs. They introduced the presence of a periodically available *trusted authority* (TA), which assesses each node's behavior. The TA collects the forwarding history evidence of a target node from its upstream and downstream nodes. Based on these evidences, the TA penalizes or rewards the node. In addition, 'iTrust' uses the concept of reputation system, in which the inspection probability varies according to the reputation of the target nodes.

In blackhole attack, malicious nodes may provide forged data to the encountered nodes. To overcome this, Li et al. [23] proposed the concept of encounter tickets that prevents blackhole attack in disruption-tolerant networks. An encounter ticket provides the evidence of contact between a pair of nodes. Whenever two nodes come in contact with each other, they generate an encounter ticket and sign the same with their respective private keys. They first submit their tickets and then reveal their contact history to one another. Similarly, Guo et al. [24,25] proposed Misbehavior Detection System (MDS) that helps in finding malicious nodes in vehicular DTNs. They also used the concept of encounter tickets similar to [23]. The schemes [23–25] detect the presence of malicious nodes in the network. However, these schemes would not be able to detect the isolator from the network because isolator neither drops nor forwards other nodes messages.

2.1. Synthesis

The current work differs from the existing works in three major aspects. First, when misbehavior of nodes is considered, there are two possibilities – either a node misbehaves or not. In some cases, however, intermittent or selective misbehavior can be observed. However, in our work, we consider that the nodes always exhibit one of the behaviors – cooperate, exploit, and isolate. The problem becomes highly challenging in dynamic scenarios in which the behaviors of the nodes may change with time (for example, see [10]). In this sense, our work is more about "identification" (i.e., what it is) rather than "detection" (i.e., whether it is). In fact, the term "misbehavior" would be rather inappropriate in our context. For example, does "exploitation" solely