Computer Networks 83 (2015) 149–166

Contents lists available at ScienceDirect

Computer Networks

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

Endeavouring to be in the good books. Awarding DTN network use for acknowledging the reception of bundles

Adrián Sánchez-Carmona *, Sergi Robles, Carlos Borrego

Department of Information and Communications Engineering (dEIC), Universitat Autónoma de Barcelona, 08193 Bellaterra, Spain

ARTICLE INFO

Article history:
Received 21 May 2014
Received in revised form 3 February 2015
Accepted 5 March 2015
Available online 18 March 2015

Keywords:
Incentive schemes
Delay Tolerant Networks
Nash equilibrium
Non-repudiation
Receipt exchange
Cooperation

ABSTRACT

This paper describes an incentive scheme for promoting the cooperation, and, therefore, avoiding selfish behaviours, in Delay Tolerant Networks (DTN) by rewarding participant nodes with cryptographic keys that will be required for sending bundles. DTN are normally sparse, and there are few opportunistic contacts, so forwarding of other's bundles can be left out. Moreover, it is difficult to determine the responsible nodes in case of bundle loss. The mechanism proposed in this paper contributes to both problems at the same time. On one hand, cryptographic receipts are generated using time-limited Identity Based Cryptography (IBC) keys to keep track of bundle transmissions. On the other hand, these receipts are used to reward altruistic behaviour by providing newer IBC keys. Finally, these nodes need these IBC keys to send their own bundles. When all nodes behave in a cooperative way, this incentive scheme works as a virtuous circle and achieves a Nash equilibrium, improving very much the network performance in terms of latency. The scheme is not difficult to implement, and it can use an already existing IBC infrastructure used for other purposes in a DTN.

1. Introduction

Delay Tolerant Networks (DTN) [1] are networks with low connectivity rates and high and variable delays. They support two main networking operations: (1) *to route* own traffic, to transmit a message from its origin to any intermediate node and (2) *to forward* other's traffic, to receive a message, store and carry [2] it for some time to transmit it when it is possible to its destination or to another intermediate node.

In these networks, all nodes are usually interested in routing and use their resources for their own benefit. On the other hand, all nodes demand that others forward their messages, but no one has a special interest in forwarding because it consumes energy and fills buffer space without any direct benefit. Therefore, it is necessary a mechanism to keep track of their behaviour: to know if they are forwarding, if they are refusing to forward or if they are losing or dropping messages. This knowledge about the performed actions of nodes must be used to encourage them to be cooperative and behave for the benefit of the network.

To solve this situation, we created an incentive scheme where nodes are required to forward if they want to route. The incentive scheme is based on a receipt exchange protocol. The receipt exchange protocol makes use of the principles of non-repudiation protocols to provides a way to discover which nodes are suspect of non-cooperative behaviour. The exchanged receipts are used by an incentive scheme that requires nodes to forward if they want to route, and punishes non-cooperative behaviours.

In the presented scheme, nodes need cryptographic keys, not only to forward messages and perform the receipt exchange protocol but also to route their own messages, because running out of keys means becoming isolated.

* Corresponding author.
E-mail addresses: adria.sanchez@deic.uab.cat (A. Sánchez-Carmona), Sergi.Robles@uab.cat (S. Robles), Carlos.Borrego@uab.cat (C. Borrego).

http://dx.doi.org/10.1016/j.comnet.2015.03.007
1389-1286/

When the incentive scheme detects suspicious nodes, it punishes them by delivering them lesser amounts of keys or even forcing these nodes to wait a while without keys. Therefore, Identity Based Cryptography (IBC) [3] keys act as an enforcing mechanism, because nodes are forced to forward messages to obtain keys, and they want the keys to route their messages.

Our main contributions can be summarised as follows.

- A receipt exchange protocol designed to overcome the limitations that the non-repudiations protocols present when applied in DTNs. The cryptographic receipts are generated by the incentive scheme using IBC keys that are used to track the actions of the nodes.
- An asynchronous incentive scheme for DTN that uses the policy "guilty until proven innocent" to punish and reward the cooperative nodes. This scheme uses the receipts generated by the receipt exchange protocol and rewards nodes by delivering IBC keys to the nodes.

In this article, we proof that, on the presented incentive scheme, node behaviours form a Nash equilibrium when all participants behave in a fully cooperative way. Besides, the simulations show that, even if nodes have low demand of keys and try to be as uncooperative as they can afford, our system improves the performance of the network in terms of latency.

The remainder of this paper is organised as follows: Section 2 presents the related work, in the field of incentive schemas and in the field of non-repudiation protocols and signature exchanges. Section 3 presents a receipt exchange protocol designed to overcome the limitations of non-repudiation protocols when applied to DTNs. Section 4 explains the incentive schema, its asynchronous operation and how we relate the amount of keys given to the nodes with their balances. Section 5 analyses the choices to be made by the network's participants and demonstrates that all nodes cooperating and being honest form a Nash equilibrium. Section 6 details the performance evaluation. Section 7 details the simulations and presents the obtained results. Finally, Section 8 concludes the article and provides some future lines of research.

2. Related work

In this section, we will present the state-of-the-art of incentive schemes. As our proposal relies not just on the incentive scheme but also on the receipt exchange protocol to build the chain of custody of every message, we will summarise how other incentive schemes keep track of the actions performed by the nodes to reward them. Finally, we will briefly summarise some non-repudiation protocols, a field that we used to develop the receipt exchange protocol presented in Section 3.

2.1. Incentive schemes

Incentive schemes have been an active research field; Mobile Ad Hoc Networks (MANET) [4] and DTN are usually the kinds of networks where this research is focused.

There are proposals that are heavily related to the concrete application they were designed to solve: dissemination of advertisements, special offers, discount coupons, and so on over a MANET. In [5], a central authority approves and marks each advertisement to track it, nodes that obtain the advertisements deliver receipts to the relaying node, and relaying nodes use these receipts to claim a reward for their work, but the central authority only rewards relaying nodes when the advertisement is used by an end user. *Coupons* [6] is based on the simple idea of adding the name of each relaying node to the transferred coupon, when the coupon is finally used a central authority rewards all nodes that had relayed it. *SMART* [7], is based on the same principles, but it is adapted for general purpose messages in DTN.

The incentive schema called *Pi* [8] includes the policy of payment-rewarding inside each message, giving to the relaying nodes the opportunity to choose, at every message, if the reward will be enough to compensate the usage of resources. As in almost all schemes, a central authority does the credit clearance after the message arrives at its final destination.

Other proposals, such as *Nuglets* [9], are based on the idea of a counter of virtual currency that every node maintains and updates when they send messages, subtracting the cost of sending a message or relaying others messages, adding a payment for relaying. Obviously, nodes are motivated to cheat and alter the content of the virtual currency counter, therefore these proposals are supported by a trusted and tamper resistant hardware module that provides security to the incentive schema.

In [10,11] the performance of the network is improved by forcing nodes to exchange messages one by one in a *Barter* manner, this way nodes are incentivised to accept and carry messages they are not interested in but they could exchange later by more interesting ones. In this proposal, nodes are restricted to exchange sets of messages of the same size, and no measures are taken against cheating, so in each transaction one party can deliver one message less than the other without being punished. Selfish nodes could benefit from this weakness to obtain all messages they are interested in without forwarding any other one, performing transactions where they receive one message and do not deliver one.

Several works present incentive schemes that, from a game theory perspective [12–14], grant that nodes should behave honestly and provide services to others because it is in its own interest. These kind of schemes, like *Sprite* [15], a scheme designed for Ad Hoc Networks, base their operation on the rationality of nodes. In *Sprite*, relaying nodes obtain a receipt of a message together with the message, and deliver the receipt to a central authority. The central authority re-builds the chain of custody of a message to charge the sender and reward the relay nodes when the message arrives at its final destination.

RAPID [16,17] is a DTNs incentive schema strongly related to a routing algorithm. This proposal, and many others, such as [18–21] are based on the Tit-for-tat principles: nodes reciprocate good or bad behaviour on part of the peer, they low service to a neighbour when they detect that a neighbour is misbehaving.