Ad Hoc Networks 24 (2015) 250–263

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme

Auxeeliya Jesudoss [a,*], S.V. Kasmir Raja [b,1], Ashraph Sulaiman [a,2]

[a] University of Rwanda, Huye, Rwanda
[b] SRM University, Chennai, India

ARTICLE INFO

Article history:
Received 6 January 2014
Received in revised form 31 July 2014
Accepted 14 August 2014
Available online 16 September 2014

Keywords:
VANET
Cooperative nodes
Selfish nodes
Payment
Punishment
Watchdogs

ABSTRACT

This paper proposes a Payment Punishment Scheme (PPS) working along with various established models to encourage truth telling during election process of the nodes in a cluster, motivate individual nodes in a cluster to cooperate and stimulate the nodes to monitor and acknowledge the successful information interchanges between nodes and/or clusters. To prompt the creation of a robust cluster in a Vehicular Ad-hoc Network (VANET), vehicles with greater resources (weights) are elected as Cluster Heads after scrutinizing their advertised weights (using the VCG model). The vehicles are discouraged to provide willful wrong information by awarding them incentives called reputation, which upon accumulation secure a higher priority of information interchange for the vehicle. Each vehicle can increase their reputation by participating in election process, forwarding the data packets and monitoring and reporting the performance of other nodes by acting as watchdogs. A modified Extended Dempster–Shafer model is used to discourage one or more selfish and/or malicious nodes to effectively implement the PPS by using watchdogs, gateway nodes, etc. The proposed scheme has been analyzed with extensive experiments. The effectiveness of this method is compared with state-of-the-art QoS-OLSR protocol.

© 2014 Elsevier B.V. All rights reserved.

1. Introduction

A successful information interchange in a VANET hinges on active cooperation among various vehicles that form small one-hop units called clusters. It being a voluntary action, the vehicles need to be motivated to cooperate, communicate and use the network to improve the robustness of the VANET. Incentive based motivation is encouraged in a VANET due to the minimal availability/absence of Road Side Units (RSU)/Infrastructure. In order to provide an active and continuous monitoring on the performance of a VANET, the vehicles/nodes (moving in the same direction) are divided into clusters. All participating nodes belong to one cluster and all the nodes in one cluster vote one of the nodes inside the cluster to be a Cluster-Head (CH). A Cluster Head is elected based on the weight which depends on a various mobility parameters. The second best node is elected as an Auxiliary Cluster-Head (ACH). The system uses Vickrey, Clarke and Groves (VCG) model [14] in order to enable truth telling behavior by every node. Once the election process is completed, all the nodes that have participated in the election process are given a payment called reputation, which is a numeric value that acts as the parameter for routing priority and building a trusting environment. A node can gain reputation by participating in election process, successful packet transmission and by monitoring the performance

* Corresponding author. Tel.: +250 788600011.
E-mail addresses: auxeeliya@gmail.com (A. Jesudoss), dean.research@srmuniv.ac.in (S.V. Kasmir Raja), ashraph@gmail.com (A. Sulaiman).
[1] Tel.: +91 9940036006.
[2] Tel.: +250 788549930.

http://dx.doi.org/10.1016/j.adhoc.2014.08.018
1570-8705/© 2014 Elsevier B.V. All rights reserved.

of other nodes and/or CHs. A Tamper Proof Device in the On-Board Unit (OBU) which keeps track of the incremented or decremented reputation values.

In order to generate a truth based environment, the system must verify and/or authenticate each and every information interchange among nodes and/or clusters. A Combined trust on Importance Factor (CIF) rule is proposed to monitor the performance of a relay node with the help of nodes acting as watchdogs. The watchdog system is implemented where in every packet transmission is approved by a minimum of three nodes that includes one node from the cluster through the packet has already passed, Cluster Head of the current cluster and any other node in the cluster. This enables to identify false positives. A reputation table (*RTable*) that contains the reputation values of all nodes in a cluster is broadcasted by the CH. This table is continuously updated with the changing reputation values of the nodes by the CH. The reputation value of a node broadcasted by a CH is always synchronized with that of the reputation table in the OBU of every node in the cluster. The communication overhead is reduced for sharing such reputation tables through Delta Encoding techniques discussed in the Section 4.1.1. The ACH becomes the Cluster Head when the Cluster Head moves away from the cluster there by ensuring maximum cluster stability.

The rest of this paper is organized in the following sections: Section 2 briefs the related work. Section 3 formulates the proposed payment and punishment scheme using the VCG and modified EDS models. Section 4 analyzes the proposed mechanisms for performance evaluation. Finally, Section 5 reviews the conclusion and discusses the future work.

2. Related works

This section presents the related works on reputation based node cooperation in VANET. Selfishness and malicious behavior of nodes affect the VANET communication. To deal with such behavior, several studies propose that cooperative nodes should be rewarded with positive reputations and non-cooperative nodes should be punished with negative reputations. Buttyan and Habaux proposed a virtual currency called NUGLETS [1], which is paid for intermediate nodes for forwarding the packets between sender and destination. In another work [2], the same authors improved their results by introducing a NUGLET counter that increases or decreases based on successful and unsuccessful packet forwards respectively. The value of NUGLET counter must remain positive for a node that wants to send its own packets.

Marti et al. [3] proposed a watchdog mechanism, in which a node that act as a watchdog overhears the forwarding behaviors of neighbor nodes within its transmission range and identifies the cooperative nodes. However, this technique does not penalize the non-cooperative nodes. Buchegger and Le Boudec [4] proposed CONFIDENT protocol to detect and isolate the misbehaving nodes. Though this approach punishes the low reputation (selfish) nodes by not forwarding their data packets, each node has to perform different evaluations such as key validation and trust manager certificate verification to detect the selfish nodes.

Authors of CORE protocol, Michiardi and Molva [5] addressed the false reputation propagation problem by not spreading the negative reputation between nodes. Thus, this protocol prevents the DOS attacks and it is impossible for a node to maliciously decrease another nodes reputation. Bansal and Baker [6] proposed OCEAN protocol as an extension to the DSR protocol. Though, OCEAN protocol is able to distinguish selfish and misbehaving nodes it fails to punish the misbehaving nodes. Rather a second chance is provided to misbehaving nodes to operate as normal nodes.

SORI protocol was proposed by He et al. [7] to encourage packet forwarding and discipline selfish behavior using reputation based punishment system. Despite SORI is computationally efficient because of One-way Hash Chain authentication, it fails to differentiate between selfish and misbehaving nodes. Vehicle Adhoc Reputation System (VARS) [8] introduced opinions that are appended with message protocol and every forwarder make use of these opinions to calculate the reputations.

Hu and Burmester [9] proposed LARS to mitigate misbehavior and enforce cooperation using reputation values. Misbehaving nodes are identified based on the reputation values, which were directly observed and stored by the neighbor nodes. Though LARS protocol stimulates the misbehaving node to improve its reputation value, this protocol subject to routing attacks. Zhang et al. [10] introduced RADAR, a reputation based protocol to quantify the behavior of each node and to observe local and global trust of all neighbors. RADAR protocol quickly detects malicious nodes but does not support high mobile networks.

Omar et al. [29] proposed a watchdog based cooperative clustering scheme for VANETs called QOS-OLSR, where relay nodes are monitored by watchdogs and payments are given by their combined trust calculated through Dempster–Shafer (DS) theory. However, this scheme has the following flaws. (i) nodes are expected to reveal their available bandwidth, connectivity and vehicle mobility information to participate in election. However, revealing such information depends on the node's behavior. (ii) One common result produced by DS theory may result in uncertain decisions. (iii) All watchdogs are treated uniformly, which may lead to unreliable result.

3. Payment and punishment scheme

The main focus of this paper is to encourage the nodes/vehicles in the network to actively participate in various network activities, such as message forwarding and monitoring and reporting, which are considered as the major responsibilities of the nodes[3] to achieve a successful VANET. We believe that such encouragement could be effectively done when the nodes work together as a team (clusters in VANET). Moreover, a cluster-based message forwarding can have more control over sending and receiving data and monitoring the behavior of the fellow

[3] Hereinafter, we use the terms nodes and vehicles interchangeably.

Download English Version:

https://daneshyari.com/en/article/444380

Download Persian Version:

https://daneshyari.com/article/444380

Daneshyari.com