Ad Hoc Networks 7 (2009) 1243–1258

Contents lists available at ScienceDirect

Ad Hoc Networks

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

On eliminating packet droppers in MANET: A modular solution

Djamel Djenouri *, Nadjib Badache

CERIST Center of Research, Ben-Aknoun, BP 143, Algiers 16030, Algeria

ARTICLE INFO

Article history:
Received 2 May 2007
Received in revised form 9 October 2008
Accepted 26 November 2008
Available online 6 December 2008

Keywords:
Mobile ad hoc networks
Security
Packet forwarding
Routing
Selfish misbehavior

ABSTRACT

In this paper we deal with misbehaving nodes in mobile ad hoc networks (MANETs) that drop packets supposed to be relayed, whose purpose may be either saving their resources or launching a DoS attack. We propose a new solution to monitor, detect, and safely isolate such misbehaving nodes, structured around five modules: (i) The monitor, responsible for controlling the forwarding of packets, (ii) the detector, which is in charge of detecting the misbehaving of monitored nodes, (iii) the isolator, basically responsible for isolating misbehaving nodes detected by the detector, (iv) the investigator, which investigates accusations before testifying when the node has not enough experience with the accused, and (v) finally the witness module that responds to witness requests of the isolator. These modules are based on new approaches, aiming at improving the efficiency in detecting and isolating misbehaving nodes with a minimum overhead. We describe these modules in details, and their interactions as well. We also mathematically analyze our solution and assess its performance by simulation, and compare it with the watchdog, which is a monitoring technique employed by almost all the current solutions.

1. Introduction

Mobile Ad hoc Networks (MANET) are dynamic and self-organized networks able to operate without depending on fixed or pre-installed infrastructure, using only wireless devices that act both as hosts and routers, and thus cooperatively provide multi-hop communications. The infrastructureless multi-hop nature of MANETs causes vulnerabilities to DoS packet dropping attack and selfish misbehavior. A node can launch a DoS attack by simply participating in the routing protocol to include itself in routes then dropping data packets it is asked to forward. Contrary to DoS attack, selfishness is an *unaggressive* motivation for dropping packets in self-organized MANETs, which merely aims at preserving resources. To save its battery a node might behave *selfishly* by not forwarding packets originated from other nodes, while using their resources to relay its own packets towards remote recipients. Regardless of whether the motivation is aggressive or not the packet dropping misbehavior harms the forwarding service in the network, and thus represents a big problem in MANETs.

In this paper we provide a full modular solution dealing with the packet dropping misbehavior and attempting to solve the complete problem, unlike the current solutions that just focus on some sub-problems. Our contribution can be summarized as follows:

- *For the monitoring*: we use the random two hops ACKs approach [1], which overcomes the watchdog's problems in detection effectiveness (presented in the following section) with reasonable overhead. Note that the watchdog [2] is a basic technique on which rely all the current sophisticated solutions that employ monitoring.
- *For the accusation*: we propose a Bayesian approach enabling redemption before judgment. The unique feature of our approach compared to the existing reputation-based ones is that each node *separately* monitors and evaluates the behavior of its successor, with no exchange (overhead) of the estimated behavior as long as the monitored node is considered to behave correctly (does not drop packets). As soon as a node considers another as misbehaving, it will proceed to its isolation

[*] Corresponding author. Tel.: +213 554 68 93 72; fax: +213 21 91 21 26.
E-mail addresses: ddjenouri@mail.cerist.dz (D. Djenouri), badache@mail.cerist.dz (N. Badache).

1570-8705/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2008.11.003

cooperatively with others. The current solutions based on the Bayesian approach, like [3], or generally speaking based on reputation like [4] require nodes to continuously exchange with each other their estimation of reputations. Therefore, our solution is low-cost in terms of overhead with respect to reputation evaluation.

- *For the accusation approval and isolation*: finally we suggest a social-based approach to approve detections and isolate guilty nodes. This approach's aim is to consider the vulnerability of false accusation attack (rumors), and to decrease false positives caused by channel conditions and nodes mobility. In summary, each node monitors and evaluates the behavior of its successors by itself, and as soon as it accuses a node it launches a procedure to approve this accusation and collaboratively isolate the node in the network. Compared to the current solutions, which use cooperation in the behavior estimation and perform the isolation unilaterally at every node, the collaborative isolation gives our solution many advantages in terms of reducing false positives as we will see later.

All these approaches are structured around five interacting modules, we will illustrate later. Our solution allows benign nodes running it to detect and isolate misbehaving nodes that drop data packets in many cases. It deals with both continuous and selective dropping, but the detection is inevitably slower for the second case due to the tolerance we use to prevent false detections in case of packet collision and node mobility that causes unintentional packet loss. Our isolation mechanism is global, contrary to many current solutions that perform the isolation locally in neighborhoods. In this case, a misbehaving node can simply move away from the region where it was isolated to rejoin the network. Our solution is not vulnerable to this misbehavior. As noted earlier, the rumor vulnerability that may arise from the global isolation strategy is taken into account by our social-based isolation approach. However, we do not consider reintegration of isolated nodes, which can be rational and required in some cases to make the solution fault tolerant. When adding such a reintegration mechanism the effectiveness of the solution should be reconsidered by preventing nodes from abusing the mechanism, which is problematic and presents one of our perspectives. We also do not consider collusive misbehavior where two successive nodes cooperatively misbehave, which also represents a very difficult problem to deal with. The rest of this paper is organized as follows: in the following section the related work is sketched, followed by a detailed presentation of the components of our solution in the third section. Section 4 is devoted to a mathematical analysis and discussion on our solution and its security features, and Section 5 to a simulation study where we compare our solution with the watchdog approach. Finally, the last section concludes the paper and summarizes the perspectives.

2. Related work

The first solution dealing with the problem of misbehavior on packet forwarding is the watchdog [2]. It is implemented with DSR [5], and relies on monitoring neighbors in the promiscuous mode. Each node in the source route monitors its successor after it sends it a packet to forward, by overhearing the channel and checking whether it relays or drops the packet. A monitoring node accuses a monitored node for misbehaving as soon as it detects that the latter drops more than a given number (threshold) of packets. This basic technique has been used by almost all the subsequent solutions. Nonetheless, it suffers from some problems of efficiency in detection, especially when using the power control technique employed by some new power-aware routing protocols following the watchdog's proposal [6] [7]. It may wrongly accuse innocents, or ineffectively miss the detection of misbehaving nodes. This is because the solution supposes that packets transmitted by any node can be received by all the nodes in its neighborhood, which cannot be ensured in all transmissions when using dynamic transmission powers. In addition to the problems related to detections the watchdog does not prevent nodes from misbehaving, since it does not provide any mechanism allowing nodes to exchange their experience, and does not apply any punishment against the detected nodes. More recent solutions [8] deal with this problem, and propose punishment policies together with methods to exchange information on misbehaving nodes.

Yang et al. [9] describe a unified network layer solution to protect both routing and data forwarding in the context of AODV. This solution is based on the approach of mutually according admission in neighborhood through signed tokens, issued using threshold cryptography-based signatures. The token has a period of expiration, whose value depends on how long the holder has been behaving well, and every node has to renew its token before its expatriation by collecting at least K different signatures of the token from its neighbors. Nodes in a neighborhood collaboratively monitor each other to detect any misbehavior using the watchdog, and decide about the delivery of requested token signatures according to the outcome of this monitoring. Compared to the basic solution of the watchdog, this one has the advantage of dealing with punishment policy, and preventing misbehaving nodes from accessing the network. However, it has some drawbacks. First, all the watchdog's problems described previously remain untreated, since the neighbor monitoring component completely relies on it. The second disadvantage of this solution is that it prevents a node which has less than K neighbors from communicating, and poses a critical issue on the choice of the parameter (threshold) K for the sharing of the secret key. The choice of low K weakens the key (It will be breakable), whereas the choice of high values requires high connectivity, which is not always ensured in MANET.

Michiardi and Molva [4] suggest a generic reputation-based mechanism that can be easily integrated with any network function, termed CORE. In this paper the authors give rigorous definitions to the notion of reputation, by defining three types of reputations: (i) *subjective reputation* that is calculated directly from a node observations, (ii) *indirect reputation*, which is calculated basing on the information (observations) provided from other nodes, and (iii)