Computer Communications 34 (2011) 548–555

Contents lists available at ScienceDirect

Computer Communications

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

A hierarchical architecture for detecting selfish behaviour in community wireless mesh networks

Nikhil Saxena *, Mieso Denko [1], Dilip Banerji

Department of Computing and Information Science, University of Guelph, Guelph, Ontario, Canada N1G 2W1

ARTICLE INFO

Article history:
Available online 5 May 2010

Keywords:
Wireless mesh networks
Reputation management
Wireless networks
Cooperative networks

ABSTRACT

Wireless mesh networks (WMNs) consist of dedicated nodes called mesh routers which relay the traffic generated by mesh clients over multi-hop paths. In a community WMN, all mesh routers may not be managed by an Internet Service Provider (ISP). Limited capacity of wireless channels and lack of a single trusted authority in such networks can motivate mesh routers to behave selfishly by dropping relay traffic in order to provide a higher throughput to their own users. Existing solutions for stimulating cooperation in multi-hop networks use promiscuous monitoring or exchange probe packets to detect selfish nodes and apply virtual currency mechanism to compensate the cooperating nodes. These schemes fail to operate well when applied to WMNs which have a multi-radio environment with a relatively static topology. In this paper we, propose architecture for a community WMN which can detect selfish behaviour in the network and enforce cooperation among mesh routers. The architecture adopts a decentralized detection scheme by dividing the mesh routers into manageable clusters. Monitoring agents hosted on managed mesh routers monitor the behaviour of mesh routers in their cluster by collecting periodic reports and sending them to the sink agents hosted at the mesh gateways. To make the detection more accurate we consider the quality of wireless links. We present experimental results that evaluate the performance of our scheme.

1. Introduction

Wireless mesh networks (WMNs) are emerging multi-hop wireless networks which provide a cost-effective solution to extend the coverage of existing wireless networks. The architectural components of a WMN include mesh clients, mesh routers and gateways. Mesh routers form the wireless backbone providing services to the mesh clients by relaying packets to and from the Internet. WMNs often have one or more mesh gateways which provide backhaul connectivity to the Internet. Nodes in WMNs have the capability for dynamic self-organization and self-configuration. These attributes provide WMNs many advantages such as reliability, scalability and low upfront cost [1]. Due to these properties, WMNs have found their application in various scenarios such as community networking, pervasive healthcare, office and home automation, emergency rescue operations and ubiquitous wireless network access.

In this paper, we have considered a community based-WMN which is used to provide Internet connectivity to community users. The mesh routers in the network can be managed by Internet Service Providers (ISP) or by independent users. Such networks can either be fully managed, semi-managed or unmanaged [2]. In fully managed networks, all mesh routers are managed by an ISP and there exists a prior trust relationship among them. In semi-managed network, part of mesh routers belong to the ISP while some mesh routers may belong to independent users which cannot assume each other to be trustworthy. An unmanaged network is formed by independent users in an ad hoc manner as it is not administered by any authority.

Since the unmanaged mesh routers in semi-managed networks may not share a priori trust relationship between each other, they may drop packets originating from other mesh routers to increase their share of available bandwidth. Mesh routers which show such behaviour exploit the network services without contributing to it, and hamper the performance of other users.

Existing solutions for stimulating cooperation in multi-hop networks have certain limitations. Reputation based schemes [3–5] use the idea of promiscuous overhearing which fails in a multi-channel environment of WMNs. Scheme based on the concept of virtual currency [9] fail with WMNs due to their static topology. The probe based schemes [7,8] incur communication overhead and congest the mesh gateway and therefore have limited scalability.

* Corresponding author. Address: Department of Computing and Information Science, University of Guelph, Room 312, Reynolds Guelph, Ontario, Canada N1G 2W1. Tel.: +1 519 824 3105.
E-mail address: nsaxena@uoguelph.ca (N. Saxena).
[1] IEEE senior member.

0140-3664/$ - see front matter © 2010 Published by Elsevier B.V.
doi:10.1016/j.comcom.2010.04.040

In this paper, we propose a hierarchical report based monitoring architecture which enforces cooperation by detecting and punishing selfish mesh routers in the network. The contribution of the proposed scheme are: (a) it detects presence of selfish mesh routers. (b) It uses a hierarchical reporting architecture which makes the scheme more scalable by reducing the communication overhead. (c) It makes use of link quality metric to differentiate between intentional packet drop and packet drop due to poor link quality.

The rest of this paper is organized as follows. Section 2 discusses the related work. Section 3 discusses the proposed scheme. Misbehaviour detection algorithm and reputation systems are presented. Section 4 provides performance evaluation using simulation experiments. Detailed discussions of the simulation results are presented in this section. Finally Section 5 provides conclusion and our future work.

2. Related work

Non-cooperation is a major problem in a multi-hop network due to its effect on protocol performance. Despite a large volume of work on cooperation in wireless ad hoc networks, relatively, not much research work has been conducted to enforce cooperation in wireless mesh networks. This section discusses some of the work done to avoid packet forwarding attacks in multi-hop wireless networks in general and their limitations when applied to Wireless mesh networks. We focus on schemes based on reputation computation, virtual currency, and exchange of periodic reports.

Reputation based schemes observe the behaviour of their neighbouring nodes through promiscuous overhearing and accordingly assign them a reputation rating which are used for identifying the selfish nodes. Nodes often have components such as watchdog [3] which buffers all packets before transmission and then overhears its neighbour's transmission to check whether it is forwarded or not. In schemes like CORE [4] and CONFIDANT [5] results from the watchdog component are fed to the reputation systems which update the reputation ratings on network nodes based on their cooperation and participation in packet forwarding. Reputation values can be periodically shared by different reputation components and nodes with low ratings are excluded or their packets denied forwarding. However, such schemes cannot be applied to wireless mesh networks due to their multi-radio and multi-channel characteristics. This is because a *watchdog* component tuned to a certain channel cannot observe communication on other channels. Moreover promiscuous monitoring cannot differentiate between intentional packet drop and packet drop due to a transmission collision.

In probing based schemes the sender and destination nodes of each flow exchange probe packets to detect and identify selfish nodes. Awerbuch et al. [6] proposed a scheme based on this idea which uses end-to-end acknowledgments for every successful packet received. If the number of acknowledgements lost in a time window exceeds a certain threshold, the source starts the search for selfish node. A set of intermediate nodes are specified as *probed* nodes such that they form non-overlapping intervals along the forwarding path. The probed nodes along with the destination must send back an acknowledgment for every packet. Once a fault is detected in an interval it is further sub-divided till the selfish node is localized. The limitation of this scheme is that selfish nodes can identify probe message and relay them to avoid detection. To counter this limitation Kargl et al. [7] proposed a mechanism called *iterative probing* in which each node shares a key with every other node in the network. Every packet header contains a field which contains the probe command to identify if the packet is a probe packet or random padding. This field is encrypted with the private key of the probed node hence none of the other nodes can identify a probe packet. In case of packet dropping the source probes each of the intermediate nodes iteratively and the first node to send an acknowledgement is detected as the selfish node. When the number of packets dropped by nodes increases beyond an acceptable threshold, they are excluded from the network. In the scheme proposed by Shila and Anjali [8] the *detection threshold* is calculating by considering the characteristics of each link forming the source–destination path, which helps in differentiating packet loss due to intentional dropping and loss due to collisions. Probe based schemes cause high overhead in the network due to exchange of large number of probe messages. Moreover since the main traffic in a WMN is uplink/downlink; the mesh gateway is involved in most of the traffic flows and hence has to initiate probing of each flow. This can cause creation of bottleneck near the mesh gateway.

Schemes like Nuglets [9] and Sprite [10] are based on virtual currency approach. The basic idea is to keep account for the forwarding services of the mesh routers. Buttyan and Hubaux [9] proposed a simple trading model using cryptographically secured virtual currency. This encourages cooperation among nodes since virtual currency enables them to forward their own packets in the network. However, this scheme relies on the presence of tamper proof hardware to verify the authenticity of virtual currency. Moreover such schemes are not effective in a WMN where the mesh routers at the periphery might not get a chance to forward packets and by earning any virtual currency. In Sprite [10] a central trusted auditing server detects selfish behaviour by collecting receipts of all delivered packets from the network nodes. This scheme incurs high communication overhead since network nodes have to submit a receipt for every received packet, and offers poor scalability due to presence of a single auditing server.

Santhanam et al., [11] proposed a scheme called Distributed-Self Policing Architecture for Fostering Node Cooperation (D-SAFNC). In the scheme every mesh router sends periodic traffic reports to the sink nodes.To enforce cooperation, selfish mesh routers are excluded from the network after a certain number of offences. Unlike the Sprite architecture, D-SAFNC does not require a central auditing server since it uses the mesh gateways to aggregate and process traffic reports from nodes. However one of its major assumptions is the presence of sufficient number of gateways in the network which ensures that every mesh router is within a two hop neighbourhood of a gateway. With the increase in the number of mesh routers, the traffic caused by reporting nodes can congest the gateways and hence hamper the network performance.

3. The proposed scheme

In this section we discuss our proposed scheme for detecting selfish behaviour in community wireless mesh networks. We aim at making the detection of selfish mesh routers more accurate and efficient by overcoming the limitations of existing schemes. One of the limitations of existing schemes is that they do not consider the quality of the wireless links, which makes it challenging to differentiate between packet loss due to selfish intent and packet loss due to the characteristics of the wireless medium. This can cause increase in false positives and decrease in the detection rate. To increase the accuracy of detection rate, our scheme takes the characteristics of individual links into account. Another limitation with most of the schemes is their huge dependence on the gateways. Due to the traffic pattern of WMN, the gateways are often congested with data and control packets transmitted to and from the gateways. In our scheme we reduce the involvement of gateways by delegating a set of managed mesh routers to assist in