Journal of Network and Computer Applications 36 (2013) 744–755

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

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

A multipath routing strategy to prevent flooding disruption attacks in link state routing protocols for MANETs

Gimer Cervera [a], Michel Barbeau [b], Joaquin Garcia-Alfaro [c,*], Evangelos Kranakis [b]

[a] Universidad Tecnológica Metropolitana, 97279 Mérida, Yucatán, Mexico
[b] School of Computer Science, Carleton University, K1S 5B6 Ottawa, Ontario, Canada
[c] Telecom SudParis, CNRS Samovar UMR 5157, 91000 Evry, France

ARTICLE INFO

Article history:
Received 22 June 2012
Received in revised form
20 October 2012
Accepted 12 December 2012
Available online 3 January 2013

Keywords:
MANETs
Multipath routing
Wireless security
Network security

ABSTRACT

Multipath routing has been proposed to increase resilience against network failures or improve security in Mobile Ad Hoc Networks (MANETs). The Optimized Link State Routing (OLSR) protocol has been adopted by several multipath routing strategies. They implement Multipoint Relay (MPR) nodes as a flooding mechanism for distributing control information. Ideally, the construction of multiple disjoint paths helps to increase resilience against network failures or malicious attacks. However, this is not always possible. In OLSR networks, partial link-state information is generated and flooded exclusively by the MPRs. Therefore, the nodes only obtain a partial view of the network topology. Additionally, flooding disruption attacks may affect either the selection of the MPRs or the propagation of control traffic information. As a consequence, the chances of constructing multiple disjoint paths are reduced. We present a strategy to compute multiple strictly disjoint paths between any two nodes in OLSR-based networks. We provide mechanisms to improve the view of the network topology by the nodes, as well as handling potential flooding disruption attacks to the multipath construction mechanism in OLSR-based networks. We conduct simulations that confirm our claims.

1. Introduction

The design of an efficient routing protocol in Mobile Ad Hoc Networks (MANETs) has become a challenging problem. This kind of networks are more prone to both link and node failures due to restricted energy or mobility. Additionally, when a node misbehaves during the execution of the routing protocol the connectivity of the network is compromised. Multipath routing has been proposed in MANETs to improve scalability, fault tolerance, security, load-balancing, energy-conservation and Quality-of-Service (QoS) (Mueller et al., 2004). Unlike the single path strategy, in a multipath approach different paths are computed between a source and a destination to increase the routing resilience against failures. According to Tarique et al. (2009), in multipath routing protocols there are three major challenges to be addressed: (a) discovery multiple routes, i.e., disjoint routes or routes with nodes or links in common, (b) path selection, i.e., multiple paths can be used as backups or simultaneously for parallel data transmission, and (c) load distribution, i.e., how data is transmitted through the multiple routes. In our work, we address security issues that affect either the discovery or selection of routes in link-state multipath routing protocols.

OLSR is a proactive link-state routing protocol designed exclusively for MANETs. The core optimization of the protocol is the selection of MPRs as an improved flooding mechanism for generating and distributing Topology Control (TC) messages in the network. As a second optimization, only partial link-state information is diffused in the network to create optimal routes from a given node to any destination. An MPR reports, in every TC message, only its selector nodes, i.e., the nodes that have selected it as an MPR. These optimizations limit the size and number of control traffic messages. As a result, several OLSR-based multipath routing strategies have been proposed. In general, OLSR-based multipath protocols have two phases: *Topology Discovery* and *Route Computation*. In the first phase, the nodes obtain information about the network topology through the exchange of Hello and TC messages. In the second phase, the nodes compute multiple paths to a particular destination in the network based on the information gathered during the first phase.

Ideally, to increase the resilience against failures or to cope with security threats, a node may construct disjoint paths, i.e., none of the computed routes share links or nodes. However, the optimizations in OLSR reduce the chances of constructing strictly disjoint paths. In the first optimization, TC messages are generated exclusively by the MPRs. In the second optimization,

* Corresponding author. Tel.: +33 160 76 47 55.
E-mail address: joaquin.garcia-alfaro@acm.org (J. Garcia-Alfaro).

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2012.12.013

the MPRs report only their selector set. Additionally, the original algorithm defined in RFC3626 (Clausen and Jacquet, 2003) to compute MPR sets minimizes the number of nodes selected as MPRs to reduce the overhead generated by control traffic messages. Thus, only a subset of nodes generate partial link-state information. Hence, some important links to the construction of disjoint paths are unannounced.

The flooding of link-state information is also affected by misbehaving nodes in the network. Cervera et al. (2011) present a taxonomy of flooding disruption attacks that affect either the flooding of control traffic information or the selection of the MPRs in OLSR-based networks. All the multipath routing strategies based on the selection of MPRs as a flooding mechanism are susceptible to these attacks. The attacks have impact either in the *topology discovery* or *route computation* phases. Yi et al. (2008, 2009a,b, 2011) proposed a multipath extension to OLSR, Multipath OLSR (MP-OLSR). MP-OLSR is a hybrid multipath routing protocol with multiple description coding for data transfer. In MP-OLSR, the construction of multiple paths leverages on Dijkstra's algorithm to find optimal routes in terms of hops. MP-OLSR uses TC messages with redundant information to increase the chances of constructing disjoint routes. MP-OLSR comprises the TC_redundancy (TCR) parameter defined in RFC3626 (Clausen and Jacquet, 2003) to include more information in every TC message. However, in some cases, TC messages with redundant information are not enough. As many other routing protocols based on OLSR, MP-OLSR has been proposed without security measures. MP-OLSR does not consider nodes with partial views of the network nor flooding disruption attacks. Additionally, the computed routes are not necessarily disjoint. The algorithm computes several routes but it is not possible to know how many of them are disjoint. We selected it as an example to present drawbacks and security risks in multipath routing protocols based on OLSR.

To address these constrains, we propose to compute MPR sets with additional coverage during the network topology discovery phase and a mechanism to obtain, if possible, $t+1$ disjoint paths during the *route computation* phase, where t is a positive integer. Additional coverage in the selection of the MPRs is defined in RFC3626 (Clausen and Jacquet, 2003), as the ability of a node to select redundant MPRs to advertise its presence to more nodes in the network. In this manner, extra coverage helps to maintain the integrity of the network in spite of the presence of misbehaving nodes during the network topology map acquisition. We named this approach a k-Covered-MPR selection. However, the overhead due to the excessive number of TC messages reduces the performance of the network. This problem is addressed by the k-Robust-MPR selection presented in Cervera et al. (2010), which balances security and traffic overhead. In OLSR networks, the MPRs form a Connected Dominating Set (CDS). A CDS is a subset of connected nodes such that if a node in the network is not part of the CDS, then it has a link to a node in the CDS. We define an MPRCDS as a CDS such that every node in the CDS has been selected as an MPR. When the nodes select their MPRs following a k-Covered-MPR selection we obtain a k-CCDS. When the nodes compute their MPRs following a k-Robust-MPR selection we obtain a k-RCDS. These variation on the selection of MPRCDS are formally defined in Section 4.1. We propose the function Disjoint Multipath OLSR (DM-OLSR) to construct multiple node-disjoint paths. The objective of our function DM-OLSR, is to construct a set P of $t+1$ node-disjoint paths between a source node s and a destination node d. To improve the network topology view, our improved mechanism utilizes additional coverage in the selection of MPRs during the *topology discovery* phase. The network topology can be abstracted as a graph of static nodes and is represented by a graph $G=(V,E,c)$, where V is the set of vertices v (i.e., nodes), $E \subset V \times V$ is the set of arcs e (i.e., links between nodes) and c a strictly positive cost function.

1.1. Contributions of the paper

In this paper, our function DM-OLSR aims to address a partial view of the network topology, flooding disruption attacks and load balancing in multipath OLSR-based networks. In our function DM-OLSR, nodes select their MPRs with additional coverage during the *topology discovery* phase and compute, when possible, $t+1$ disjoint paths during *the route computation* phase. Our mechanism privileges the nodes with the smallest number of nodes in their selector set to be included in the computed paths. Clearly, in sparse networks it is not always possible to compute disjoint paths. Nevertheless, multipath routing takes advantage of large and dense networks. Then, we focus on the cases where the construction of multiple disjoint paths is affected either by an incomplete view of the network topology or by the presence of a misbehaving node that perpetrates a flooding disruption attack.

Organization of the paper—OLSR and MP-OLSR are reviewed in Section 2. In Section 3, we show vulnerabilities in MP-OLSR. We present our proposed countermeasures in Section 4. Our experiments and results are presented in Section 5. Related work is presented in Section 6. Finally, Section 7 concludes the paper.

2. Background

This section presents an overview of the original OLSR protocol and the MP-OLSR extension.

2.1. Optimized link state routing protocol

OLSR is a proactive routing protocol designed exclusively for MANETs. The core of the protocol is the selection, by every node, of Multipoint Relay (MPR) sets among their one-hop symmetric neighbors as a mechanism to flood the network with partial link-state information. This technique minimizes the number of traffic control messages flooded in the network, reduces the size of the messages and allows to construct optimal routes to every destination in the network. The link-state information is constructed by every node and involves periodically sending Hello and TC messages. The OLSR protocol is hop-by-hop routing, i.e., each routing table lists, for every reachable destination, the address of the next node along the path to that destination. Every node learns about its one and two-hop neighbors by periodically generating and receiving Hello messages. Hello messages are not retransmitted further. The MPR set is selected so that every two-hop neighbor is reachable through, at least, one MPR. Every node reports the nodes it has selected as MPRs in its Hello messages. With this information, the nodes build their MPR selector set, i.e., the set of nodes that have selected a given node as an MPR. TC messages are generated exclusively by the MPRs. A node that has an empty MPR selector set does not send or retransmit any TC message. The originator of a TC message advertises itself as the last hop to reach all nodes included in its selector table. The information contained in TC messages is determined by a TCR parameter. This parameter is defined in the RFC3626 (Clausen and Jacquet, 2003) and has three possible values:

- If TCR is equal to zero, then MPRs report its selector table.
- If TCR is equal to one, then MPRs report its selector table and its MPR set.
- If TCR is equal to two, then MPRs report its one-hop neighbors.