ARTICLE IN PRESS

Ad Hoc Networks xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks

M.P. Salamanca [a], N. Peña [a], N.L.S. da Fonseca [b,*]

[a] Electronics and Telecommunication Systems Group (GEST), Department of Electrical and Electronic Engineering, Universidad de los Andes, Cra. 1E No. 19A 40, Bogota 111711, Colombia

[b] Institute of Computing, Campinas State University, Av. Albert Einstein, 1251, Cidade Universitaria, Campinas, SP 13083-852, Brazil

ARTICLE INFO

Article history:
Received 10 September 2014
Accepted 20 March 2015
Available online xxxx

Keywords:
Admission control
Envelopes
Routing protocols

ABSTRACT

Envelope-Based Admission Control (EBAC) is an admission control scheme independent of the routing protocol, designed for ad hoc networks with the aim of supporting delay bounds. During the admission of users, EBAC evaluates a known route to determine whether it has enough bandwidth to support the new flow. To do this, the incoming node sends probing packets along a route so that the receiving node computes the envelope of the incoming flow, as well as the service envelope that models the service provided by the network. Based on these envelopes, the receiving node decides whether to admit the new flow. Admission control schemes that are decoupled from the routing protocol can work with any routing protocol. However, characteristics such as the way the underlying protocol deals with link failures or the speed of the route discovery process impact the admission control operation. This paper analyzes the performance of the EBAC scheme when used jointly with four different routing protocols: AODV, DSR, OLSR and DYMO. Results show that in both static and mobile scenarios, joint operation with the AODV protocol achieved the best performance of those evaluated.

1. Introduction

In ad hoc networks, nodes can move and are allowed to join and leave the network at any time. Such dynamic behavior can lead traffic flows to be switched to new routes, thus affecting other ongoing transmissions. Moreover, given that network links are wireless, ad hoc networks are also affected by the typical problems of wireless communications: fading, higher packet loss rate, interference between traffic flows, and even interference between packets of a single flow when these are sent along multihop routes. Providing Quality of Service (QoS) in ad hoc networks is thus a challenging task.

Admission control is a strategy designed to provide QoS guarantees by limiting the number of admitted flows into a network. A new flow is admitted into the network only if the QoS requirements of the incoming flow and that of previously admitted flows can be satisfied. In ad hoc networks, one of the most important design features of admission control is whether or not the control mechanism is coupled with the routing protocol, since the choice of route can impact on QoS provisioning [1]. Admission control schemes decoupled from the routing protocol use routes previously discovered by such protocols and determine whether or not a route has enough resources for the new flow. Two types of such schemes are known: *stateful*, in which intermediate nodes store state information, and *stateless*, in which only source and destination nodes participate in the admission process. Stateless admission control is the simplest scheme, since the burden of the process

* Corresponding author.
E-mail addresses: marsalam@uniandes.edu.co (M.P. Salamanca), npena@uniandes.edu.co (N. Peña), nfonseca@ic.unicamp.br (N.L.S. da Fonseca).

http://dx.doi.org/10.1016/j.adhoc.2015.03.008
1570-8705/

relies only on the source and destination nodes. In these schemes, traffic flows can be switched to a new route when the available bandwidth is insufficient.

Envelope-Based Admission Control (EBAC) [2] is a distributed stateless admission control scheme that requires neither network nor MAC level feedback; moreover, it is able to provide delay bounds to more than one class of traffic. EBAC was designed for pedestrian networks and for density of nodes that avoids network partitioning. The EBAC scheme sends a sequence of probing packets to the destination node, which are used to infer the available bandwidth on the network route between source and destination. The destination node decides on the admission of a flow based on both the envelope of the probing traffic and the service envelope. The envelopes are calculated according to the algorithm proposed by Cetinkaya et al. [3], which was applied to chains of wireless nodes [4]. EBAC has been shown to guarantee delay bounds for two classes of traffic in networks with static nodes [2]. Moreover, EBAC operation was also evaluated in scenarios with mobile nodes.

Although admission control schemes that are decoupled from the routing protocol can work with any routing protocol, the impact of this routing protocol on their operation should always be assessed. Routing protocol performance depends on characteristics of specific scenarios, such as node speed and node density which, in turn, can affect the admission control operation. This paper provides a detailed assessment of the impact that routing protocols have on the performance of EBAC. Four widely known routing protocols were employed in the evaluation: AODV, DSR, OLSR and DYMO. This group includes both reactive and proactive protocols, which allows the evaluation of the performance of the EBAC scheme for different types of routing protocol operation. It is our best knowledge that such investigation has not been carried out before.

The structure of the paper is the following. Section 2 describes the operation of EBAC. Section 3 explains the four routing protocols used in the evaluation. Section 4 *summarizes* the simulation scenario. Section 5 explains the results obtained, and finally, Section 6 concludes the paper.

2. Description of EBAC

EBAC is an admission control scheme designed for ad hoc networks that guarantees delay bounds. The EBAC scheme decides on the admission of an incoming flow by measuring both the arrival and service envelopes of a flow of probing packets. This section describes the operation of EBAC, the estimation of the envelopes of the probing flow and the criteria to decide whether an incoming flow should be admitted or not.

The EBAC algorithm employs the characterization of *envelope processes* to make admission decisions. Given $A(t)$ the cumulative amount of traffic that arrived during the interval $(0,t)$, the process $\hat{A}$ is the envelope of A if, for all t and $\tau,\ 0 \leqslant \tau \leqslant t$

$$A(t) - A(\tau) \leqslant \hat{A}(t-\tau) \tag{1}$$

Cetinkaya et al. introduced algorithms to calculate measurement-based arrival and service envelopes. The algorithm calculates the arrival envelope as the maximum traffic rate generated by the source node, and the service envelope as the worst service provided by the network.

The admission process of a flow begins when the incoming node starts a flow of probing packets transmitting it at a constant bit rate (CBR) equal to the peak rate of the incoming flow. Relevant information such as the peak rate of the incoming flow, the traffic class it belongs to and the time instant when the probe was sent (*transmission time*) is appended to each probing packet. The destination node stores the transmission and the arrival time of each probing packet and, after a predefined number of probes (or *window size*) received, the arrival and the service envelopes are estimated [5].

2.1. Computation of the arrival envelope

Arrival envelopes characterize the incoming traffic by estimating the aggregate peak-rate envelopes. Let $A[s, s+I_k]$ be the arrivals during the interval $[s, s+I_k]$, then $A[s, s+I_k]/I_k$ is the rate for that particular interval. The peak rate over any interval of length I_k is given by $R_k = \max_s A[s, s+I_k]/I_k$. Thus, the peak-rate envelope is the set of rates R_k that bound the flow rate over intervals of length I_k, and it is described by the pairs (R_k, I_k).

Consider that time is slotted and that slots are I_1 seconds long, which is the minimum interval of the measured rate envelope. Each window consists of T time slots. The peak-rate envelope over the past T time slots, being t the current time, is defined as

$$R_k^1 = \frac{1}{k\tau} \max_{t-T+k \leqslant s \leqslant t} A[(s-k+1)\tau, s\tau] \tag{2}$$

for $k = 1, \ldots, T$. Thus, $R_k^1,\ k = 1, \ldots, T$ describes the aggregate peak-rate envelope in time intervals of duration $I_k = k\tau$ contained in the most recent $T\tau$ seconds. The superscript in R_k^m denotes the envelope calculation window, being $m = 1$ the most recent one.

Every T time slots, the arrival envelope is computed using (2). At each iteration, the oldest time window is discarded and the envelopes of the past M windows are retained, including the most recent one, thus $R_k^m \leftarrow R_k^{(m-1)}$, for $k = 1, \ldots, T$ and $m = 2, \ldots, M$.

The variance of the past M measured envelopes is calculated as

$$\sigma_k^2 = \frac{1}{M-1} \sum_{m=1}^{M} (R_k^m - \overline{R_k})^2 \tag{3}$$

where $\overline{R_k} = \sum_m R_k^m / M$.

2.2. Computation of the service envelope

The service envelope is calculated by measuring the service received by a traffic flow when its packets are backlogged. When the packets are not queued, only their individual delays are considered.

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

Suppose that only one traffic class exists, where a_j denotes the arrival time of the jth packet, and d_j its departure time. A flow is considered backlogged when it has, at least, one packet in the system. In particular, a flow is continuously backlogged for k packet transmissions during the interval $[a_j, d_{j+k-1}]$, if

$$d_{j+m} > a_{j+m+1} \quad \text{for all} \quad 0 \leqslant m \leqslant k-2 \tag{4}$$

for $k \geqslant 2$. Notice that all packet transmissions are backlogged for $k = 1$ and it corresponds to the packet delay along the path.

Fig. 1 shows an arrival and departure sequence. Consider the first packet. Given that the second packet arrives after the first one has departed, the backlogging condition for the first packet is satisfied only for $k = 1$. For the second packet, the flow is backlogged for $k = 2$ consecutive packets since $d_2 > a_3$. The service envelope is expressed as a vector of time values $\vec{U}$ such that U_i is the maximum time required to serve $i \cdot L$ bits, where L is the smallest packet size. Initially, $\vec{U} = \vec{0}$ and the service envelope is iteratively calculated considering each one of the n received packets during the window.

For packet j, the envelope is updated as

$$U_i = \max(U_i, d_{j+k-1} - a_j) \tag{5}$$

where

$$i = \sum_{m=0}^{k-1} l_{j+m} \tag{6}$$

and l_{j+m} is the size of packet $j + m$ expressed in units L. For a particular packet j, all $k \geqslant 1$ that satisfy the inequality (4) are iteratively considered. Similarly to the arrival envelope, the mean and variance of the service envelope over successive windows is computed.

2.3. Admission control

When an incoming flow requests admission, the egress node verifies if its admission is feasible or not. Consider a traffic class that has an arrival envelope with mean $\overline{R}(t)$ and variance $\sigma^2(t)$. The mean and the variance of the minimum service envelope of that traffic class are respectively given by $\overline{S}(t)$ and $\psi^2(t)$, and the incoming flow peak-rate envelope is given by $r(t)$. The flow is admissible with delay bound D and a confidence level $\Phi(\alpha)$ if

$$t\overline{R}(t) + tr(t) - \overline{S}(t+D) + \alpha\sqrt{t^2\sigma^2(t) + \psi^2(t+D)} < 0 \tag{7}$$

for all the interval durations of $0 \leqslant t \leqslant T$. The confidence level characterizes the variations of the past measurements and the uncertainty of the prediction of future service and arrivals, and is determined by using the Extreme Value Theory [6]. Once the admission test is performed, the egress node sends a notification to the source node.

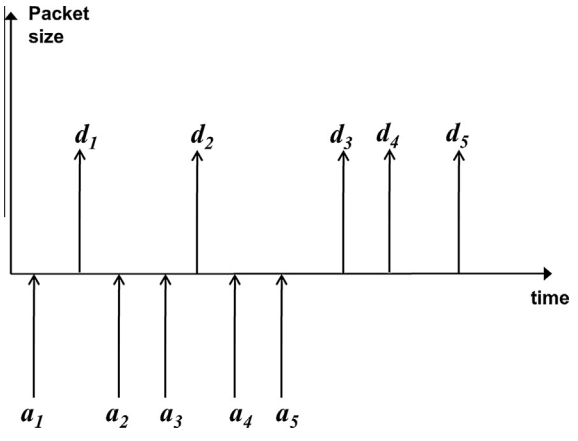


Fig. 1. Example of an arrival and departure sequence.

3. Routing protocols

Routing protocols for ad hoc networks are generally classified as *reactive* or *proactive*. Reactive protocols, also called *on-demand* protocols, discover routes only when they are needed. When a node has a packet to send and there is no route to the destination, the node starts a route discovery process by flooding the network with a query. A route is created either when the destination node or an intermediate node, responds to the query. Since packets must wait in a buffer while the route is being discovered, the delays experienced by initial packets increase. In spite of this increase, however, reactive schemes demand fewer resources since the routing tables store only the set of routes needed by the node. Reactive protocols demand a certain amount of bandwidth for the discovery process, however.

Proactive routing protocols store a table with routes to all other nodes in the network at each node. Routing tables are built and updated by exchanging periodic control messages between the nodes. A node that has a packet to send only needs to find the corresponding entry in the routing table. Proactive schemes demand more bandwidth than reactive schemes, since the nodes need to send the periodic control packets to update the information about available routes.

This section describes the four routing protocols used jointly with EBAC in this investigation. Three of them are reactive (AODV, DSR, and DYMO) while the fourth is proactive (OLSR). The processes of route discovery and maintenance of these protocols will be described next.

3.1. AODV

The Ad hoc On Demand Distance Vector (AODV) protocol [7] is a distance-vector routing protocol that uses sequence numbers to avoid the typical problem of distance vector protocols, known as *count to infinity*.

To discover a route, the AODV protocol implements a mechanism known as *expanding ring search technique*. If a node has a packet to send and a route to the destination of the packet is unknown, it sends a Route Request (RREQ) message. The first RREQ message is sent with a value of the Time To Live (TTL) field equal to one. If a time out occurs after sending an RREQ, the node broadcasts another RREQ message with an increased value for the

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

TTL field in the header. When a node receives an RREQ message, both the route to the previous hop and that to the originator of the message, are either created or updated. The route is updated if the sequence number of the RREQ is higher than a previous value or if the sequence number is the same, but the new route has fewer hops. If the node is the destination itself or if it knows a new route to the destination, it sends a Route Reply (RREP) message back to the source node. The nodes that receive the RREP message create a forwarding route by adding/updating the route to the previous hop and to the destination.

In the AODV protocol, there are two mechanisms for route maintenance. The first extends the route lifetime every time a packet is successfully forwarded. The second mechanism makes a node to keep information of its active next-hop nodes, either by using link-layer notifications or by listening to the channel to determine the transmission attempts from the next hops, a technique called *passive acknowledgement*. If a transmission attempt is not detected during a specific interval, its connectivity is determined by receiving a packet (even a HELLO message, if enabled) from the next hop, by sending an RREQ message to the next hop, or by sending an ICMP echo request to the next hop.

If the next-hop link cannot be detected, the node assumes that the link has been interrupted and generates a Route Error (RERR) message. Nevertheless, if the destination node is no further than a certain number of hops, the node that detected the broken link attempts to repair the route locally by sending an RREQ message. If this new discovery process fails, the node transmits an RERR message which can either be broadcasted or iteratively unicasted to the neighbor nodes that had been originally forwarding packets on the broken route. An RERR message can also be sent when a node gets a data packet destined to a node to which it does not have an active route. When the source node receives an RERR message, a new process of route discovery begins.

3.2. DSR

The Distance Source Routing (DSR) protocol [8] is another reactive protocol; it discovers multiple routes to a destination node in a single discovery cycle. If an active route fails, the source node can choose an alternative cached route. The DSR protocol was designed for ad hoc networks of up to two hundred nodes, as well as for mobile networks with a small diameter of 5–10 hops. In the DSR protocol, the complete sequence of hops between source and destination is carried in each data packet sent (*source routing*).

The DSR protocol also uses RREQ and RREP messages to discover a new route. The source node that requires a route to the destination node, broadcasts an RREQ message to all nodes within its transmission range. Intermediate nodes append their address to the RREQ message and propagate it. This procedure is repeated until the RREQ message reaches the destination node. At this time, the node responds to the initiator of the discovery process with an RREP message that includes the whole route from source to destination. The source node may find multiple routes to the destination because it adds the new route to its cache each time an RREP message is received. According to [8], each implementation of the DSR protocol "may choose any appropriate strategy and algorithm for searching its route cache and selecting the best route from among those found".

To maintain a route when using the DSR protocol, each node that transmits a data packet must confirm that it has been correctly delivered to the next hop. This confirmation can be either a simple acknowledgement (ACK) provided by the link-layer, a passive one or one generated by a DSR-specific software. However, if the MAC protocol provides feedback that a packet has been correctly delivered, no other type of confirmation is necessary.

The DSR protocol has a *maintenance buffer*, where the packets that are awaiting for next-hop confirmation are stored. If the confirmation is not received after a certain number of retransmission attempts, all packets in the maintenance buffer awaiting the unreachable next hop are removed. The node that detected the broken link then generates an RERR message and sends it to the source node of the removed packet. If the node has another route to the destination of that removed packet, this node will replace the original source route in the packet with this route from its route cache (*packet salvaging*) as soon as the RERR message is sent. Then, this node forwards the packet to the next-hop, indicating the alternative route. Each packet can only be salvaged a certain maximum number of times, otherwise the process could be repeated indefinitely.

When the source node receives an RERR message, the broken link is removed from its cache and, if there is another route to the same destination, it will be used. However, if the broken route was the only path to that destination, the originator must start a new cycle of discovery.

3.3. DYMO

The Dynamic MANET On-Demand Routing (DYMO) protocol [9] is a revised version of the AODV protocol, also known as AODVv2. The DYMO protocol adds some of the features of DSR to that of AODV. It is "best suited for relatively sparse traffic scenarios where any particular router forwards packets to only a small percentage of AODVv2 routers in the network" [9]. The default metric of the DYMO protocol is hop count, but route selection can be also based on other metrics, such as delay and energy.

In order to discover a new route, the originator multicasts an RREQ message. The format of the RREQ and RREP messages is defined in RFC 5444 [10]; it allows the inclusion of multiple routing protocol messages in a single packet. With this message format, intermediate nodes that receive either an RREP or an RREQ message can append this route from itself to the originator of the packet. This feature is called *path accumulation function* and it allows each node receiving an RREP or RREQ message to update its own routing table with the information from other intermediate nodes, thus eliminating certain route discovery attempts since this information will already be available. The routes of the DYMO protocol also have a sequence number and the criteria for updating them is the same as that of the AODV protocol. Upon receiving an RREQ

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

message, the destination node sends an RREP message in the direction of the source node.

The DYMO protocol provides route maintenance similar to that of the AODV protocol. RERR messages include a list of unreachable nodes with the sequence numbers of the corresponding routes, and the RERR messages inform upstream nodes about the routes that are no longer available. Nodes that receive RERR messages use that information to invalidate reported routes.

3.4. OLSR

Optimized Link State Routing (OLSR) [11,12] is a proactive routing protocol designed mainly to reduce message overhead produced by traditional link-state protocols. In the OLSR protocol, route discovery and route maintenance are not different procedures. The routing table is updated constantly by the reception of periodical control messages of the types HELLO and TC messages. The OLSR protocol "does not generate extra traffic in response to link failures and additions" [12]. The routing table is re-calculated locally each time there is a change, either in the neighbor set or in the network topology. According to [11], this protocol is suitable for "large and dense networks, as the technique of Multipoint Relays (MPRs) works well in this context".

Instead of flooding the whole network with routing information, in the OLSR protocol each node selects a set of nodes, located in its 1-hop neighborhood, which will be the MPRs of that node. The neighbors of a node that do not belong to the MPR set, receive broadcast packets but do not retransmit them. Fig. 2 shows a source node transmitting a broadcast packet and its selected MPR set.

Neighbor detection in the OLSR protocol is a fundamental task. In order to perform it, each node periodically broadcasts HELLO messages to all its immediate neighbors informing them of its link status. In this way, HELLO messages allow each node to identify its neighbors up to two hops away. These messages are received by all one-hop neighbors, but they are not necessarily forwarded. Based on the information received, a node selects its MPRs and constructs a table with the corresponding addresses.

The other type of control packets, *Topology Control* (TC) messages, which are broadcasted at regular intervals by every MPR, and contain the list of network nodes that have selected that MPR as a relay node. Each TC message is broadcasted through the whole network by the MPRs, and will allow each node to construct its own routing table. In the OLSR protocol, a route between two hosts is essentially a sequence of hops through the MPRs between source and destination nodes.

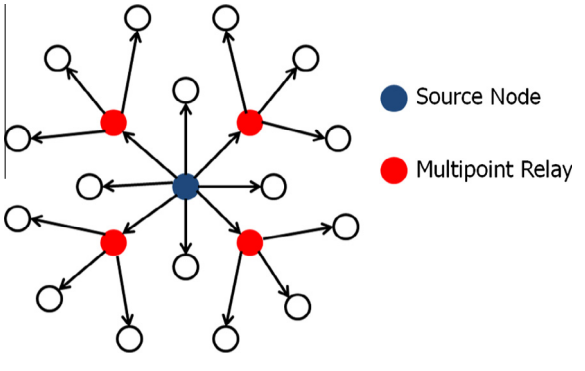


Fig. 2. A source node using the OLSR protocol and its corresponding set of Multipoint Relays.

4. Simulation description

Simulation using the Qualnet Simulator version 5.02 [13] was employed to assess the impact of the routing protocol on the performance of EBAC. The scenario consisted of 50 nodes, randomly placed in an area of 1500 m × 400 m, a size chosen to avoid network partitioning due to node mobility. The DCF MAC option of IEEE 802.11b at a speed of 2 Mbps was used with the transmission range of each node was set to 250 m.

The simulation involved both voice and data sources. Voice calls were modeled as two ON–OFF sources, one at each end, while data sources were modeled as a single ON–OFF at the source node. The duration of each flow was exponentially distributed with a mean value of 5 min. Source and destination nodes of each flow were randomly selected from the 50 nodes. Voice calls used the G.723.1 codec with a configuration based on the voice traffic characterization derived in [14]. The parameters of each source type with the corresponding delay bounds, are shown in Table 1. Traffic flows were generated alternately, i.e. a voice flow was followed by a data flow. Each simulation lasted 1800s. The admission algorithm sent 7 windows of 16 probing packets each. These values were chosen according to the results presented in [15].

EBAC implementation includes a timer to control the time that the incoming node should wait for the reception of a response packet sent by the destination node. This response packet is necessary to inform the incoming node whether the flow has been accepted or rejected. The time is set to 2.5 s by the incoming node immediately after the last probing packet has been sent. If, during that time period, a response packet is received, the timer is ignored; otherwise, the incoming node assumes that either a probing packet or a response packet has been lost, and the flow is rejected. The duration was determined by several tests; it is shorter than the route timeout or the route cache timeout values that were set for the routing protocols. In this way, EBAC guarantees that the route tested will be the same one used by the traffic flow if it is accepted.

5. Simulation results

This section presents the results of the simulation experiments for the routing protocols. In the first part,

Table 1
Simulation traffic parameters.

Parameter	Voice	Data
Distribution	Exponential	Pareto
Mean ON time	1.49 s	250 ms
Mean OFF time	1.722 s	250 ms
Packet size (Bytes)	48	1024
Delay bound	100 ms	500 ms
Max. bit rate (bps)	7875	400,000

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

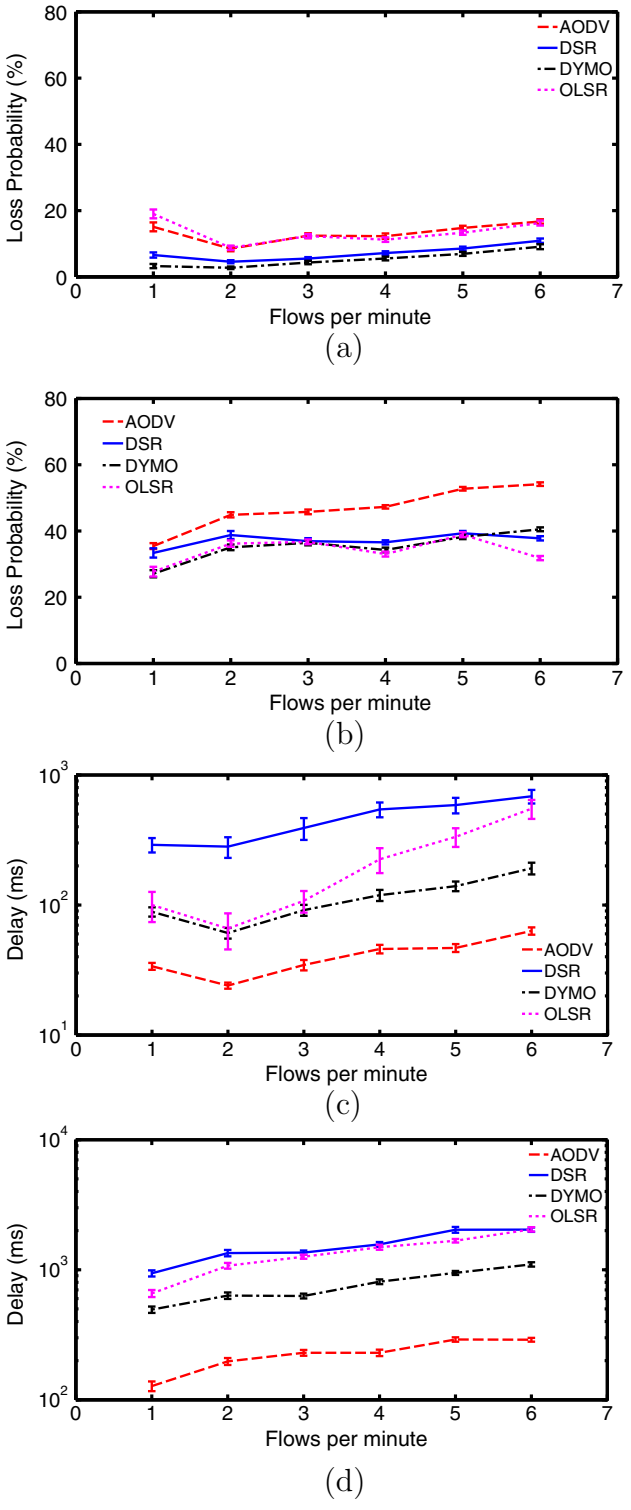


Fig. 3. Statistics of probing packets with AODV, DYMO, DSR and OLSR protocols for static nodes. Figures (a) (voice) and (b) (data) depict loss probability of probing packets; (c) (voice) and (d) (data) illustrate average delay.

the probing packets are analyzed to understand the decisions made by EBAC based on the operation of each routing protocol. Then, EBAC is evaluated in a scenario with static nodes and different rates of incoming traffic to find the maximum rate which can be supported by EBAC operating jointly with each routing protocol. The EBAC scheme is

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

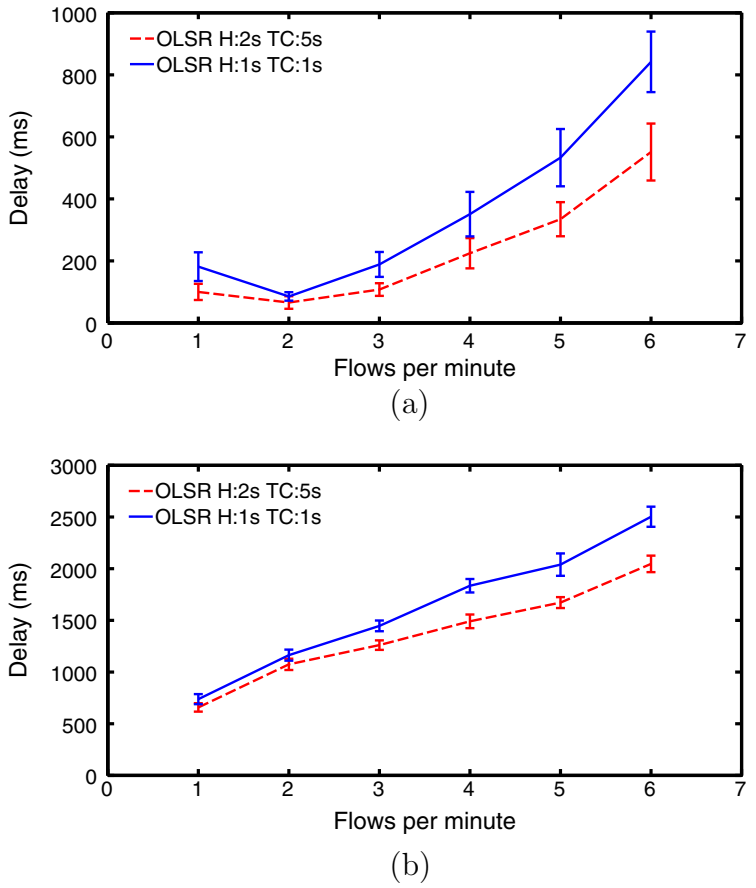


Fig. 4. Statistics of probing packets with the OLSR protocol and two different time intervals between consecutive control packets. Figures (a) corresponds to voice traffic and (b) to data traffic. The letter H corresponds to Hello messages and TC to Topology Control messages.

tested again in the same scenario but with low mobility, to determine its operation limits. The analysis focused on finding the routing protocol that provides the best performance in terms of average delay, packet losses and acceptance probability.

Experiments were performed under exactly the same conditions in order to guarantee a fair comparison. All figures show confidence intervals with 95% confidence level, derived with independent replication method (up to 100 repetitions were employed).

5.1. Analysis of probing packets

The decisions made by the EBAC scheme depend on measurements based on probing packets. These packets gather valuable information that shows the way that the underlying routing protocol operates, specifically on how it deals with link failures. To assess these operations, simulation scenarios involved static conditions so that the results would not be influenced by anything other than the routing protocols.

Fig. 3 shows the delay and loss probability of probing packets for each routing protocol as a function of incoming flows per minute (fpm). Fig. 3(a) and (b) show that the percentage of lost probes is greater for data traffic. This is a result of the fact that since data probes are much larger than voice probes, and, during the transmission between nodes in wireless networks, large packets are more prone to error than small packets. Additionally, the sending rate of data probes is much higher than that of voice probes, thus causing higher contention in multihop paths and increasing the loss probability of data probes. In a multihop network, the decisions that routing protocols make when a node loses its connection to the next hop are crucial for the performance of any user application.

Neither RFC 3561 (the AODV protocol) [16] nor the Draft 26 (the DYMO protocol) [9] mentions what should be done with the outbound packets present in network queues when a link fails. Qualnet implementation addresses the issue differently for each protocol. For the AODV protocol, buffered packets are discarded when the MAC layer reports a failure in transmission to the next-hop node of a route, while for the DYMO protocol, packets remain in the queue until the link is restored. As a consequence, the AODV protocol produces short packet delays but a high packet loss probability, while the DYMO protocol causes long packet delays and low packet loss probability. This behavior can be seen in Fig. 3. The AODV protocol produces the highest loss probability of the protocols analyzed.

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

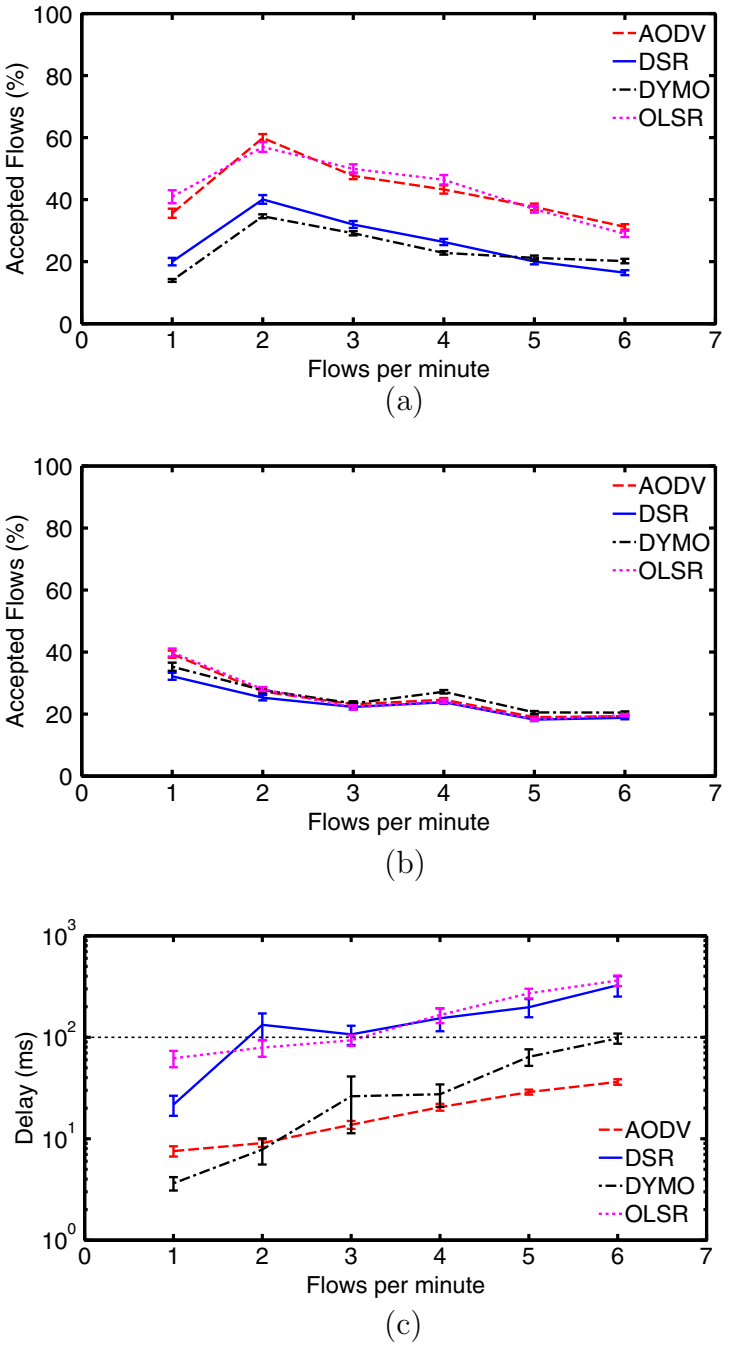
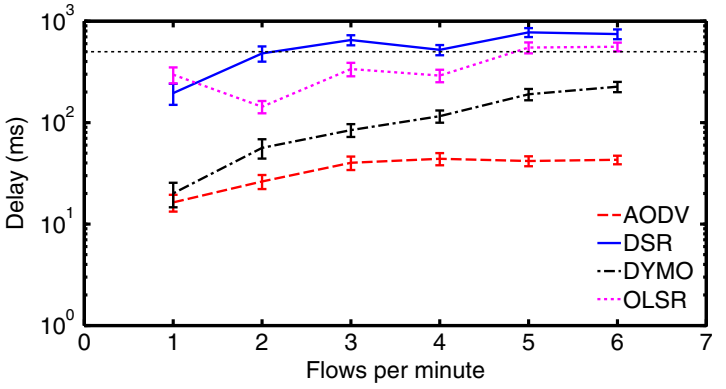


Fig. 5. Statistics of EBAC in a scenario with static nodes. Figures (a) (voice) and (b) (data) show accepted flows, (c) (voice) and (d) (data) illustrate average packet delay, (e) (voice) and (f) (data) depict lost packets.

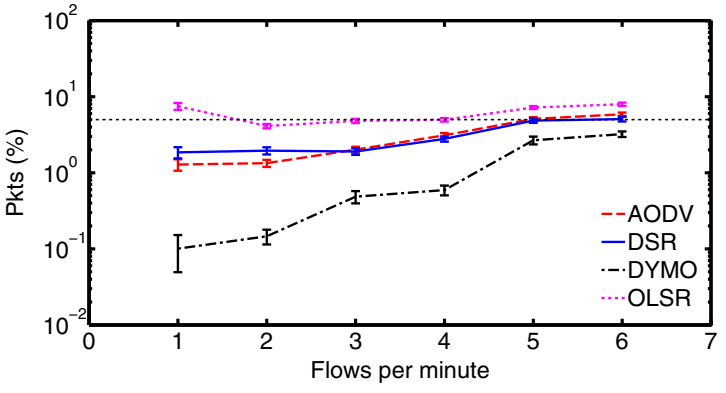
In the DSR protocol, long delays are due to the retransmission mechanism. If the link to the next hop is broken, the MAC layer returns the packet to the network layer. When this happens, the number of retransmissions is increased and the packet sent back to the MAC layer for a new attempt. Then, the MAC layer re-initiates the whole process transmitting the packet. The number of times the packet can be returned to the MAC layer can be set, in the simulation experiments in this paper this number was set to 2. If the packet cannot be delivered after the maximum number of attempts, it is dropped from the maintenance buffer.

The proactive OLSR protocol behaves in a completely different way. RFC 3626 [11] only mentions that a packet should be dropped when $TTL \leqslant 0$. "OLSR itself does not perform packet forwarding. Rather, it maintains the

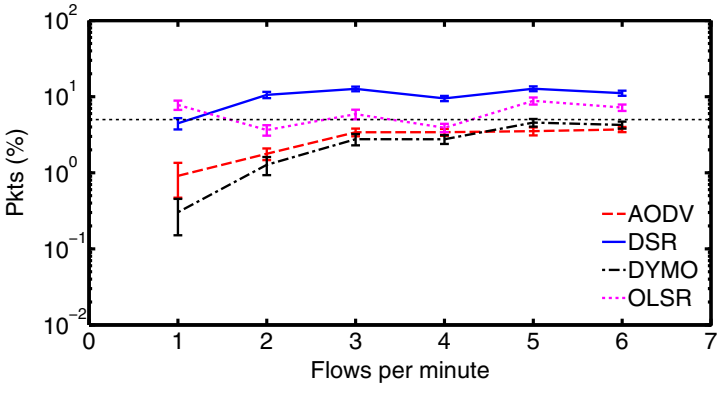
Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008



(d)



(e)



(f)

Fig. 5 (*continued*)

routing table in the underlying operating system, which is assumed to be forwarding packets as specified in RFC 1812". Indeed, RFC 1812 [17] explains that a packet is dropped when the node has no routes to the destination. Therefore, the packet dropping policy in the OLSR protocol is transferred to IP and MAC layers. The consequences of this operation scheme are that with voice probes, the losses are similar to those when using the AODV protocol, while for data probes they behave similarly to those of the DYMO protocol. Moreover, the OLSR protocol is highly sensitive to network congestion, as reflected in the delay experienced.

Since the OLSR protocol uses control packets to calculate and update routes, a set of simulations was designed to evaluate whether the protocol performance could be improved by increasing the frequency of control packets. The new simulations were configured to reduce the interval between consecutive HELLO packets from 2 s to 1 s and between TC packets from 5 s to 1 s. Fig. 4 shows that the delay for both classes of probing packets increases when

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

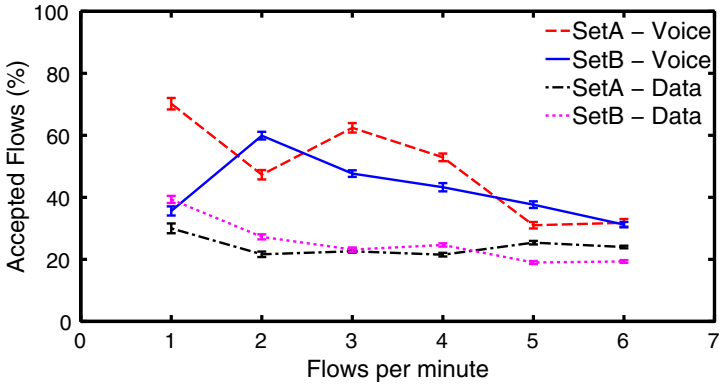


Fig. 6. Percentage of accepted flows with two different sets of incoming flows and the AODV protocol.

Table 2
Limits for operation for each routing protocol in a mobile scenario.

Protocol	Flow rate (fpm)	Mobility factor (%)
AODV	1	40
	2	10
DSR	1	10
OLSR	No mobility supported	
DYMO	1	50
	2	10

control packets are sent more frequently. Thus, introducing more control packets to the network would not improve the performance.

5.2. Performance involving static nodes only

In the static scenario, the EBAC scheme was tested with incoming flow rates increasing from 1 to 6 flows per minute (fpm). Fig. 5 shows the percentage of accepted flows,

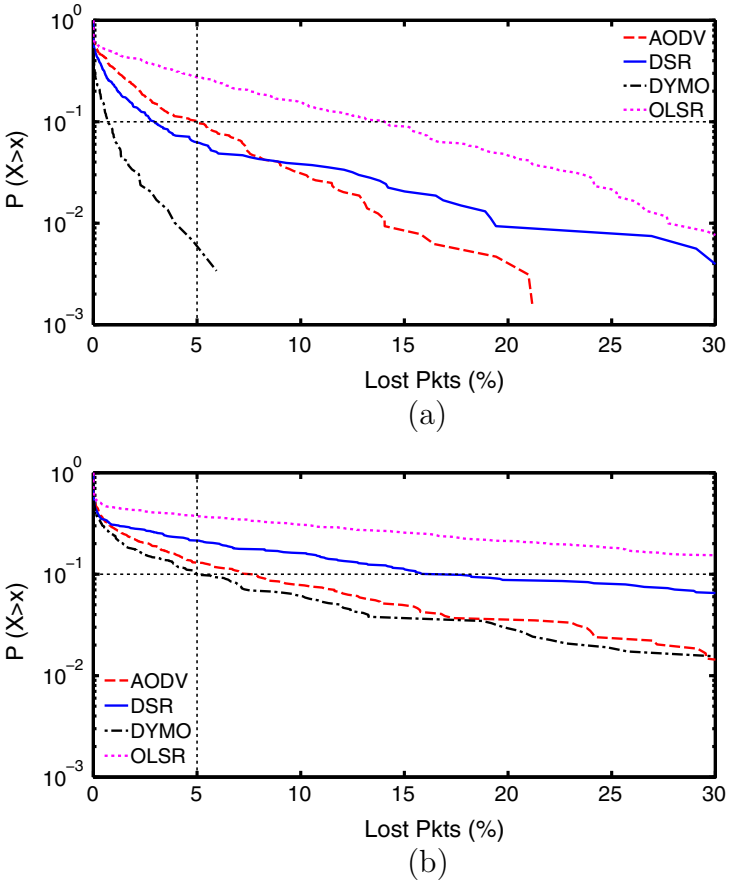


Fig. 7. Empirical complementary distribution of packet losses with incoming flow rate of 1 fpm and mobility factor equal to 50%. (a) and (b) correspond to voice and data traffic, respectively.

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

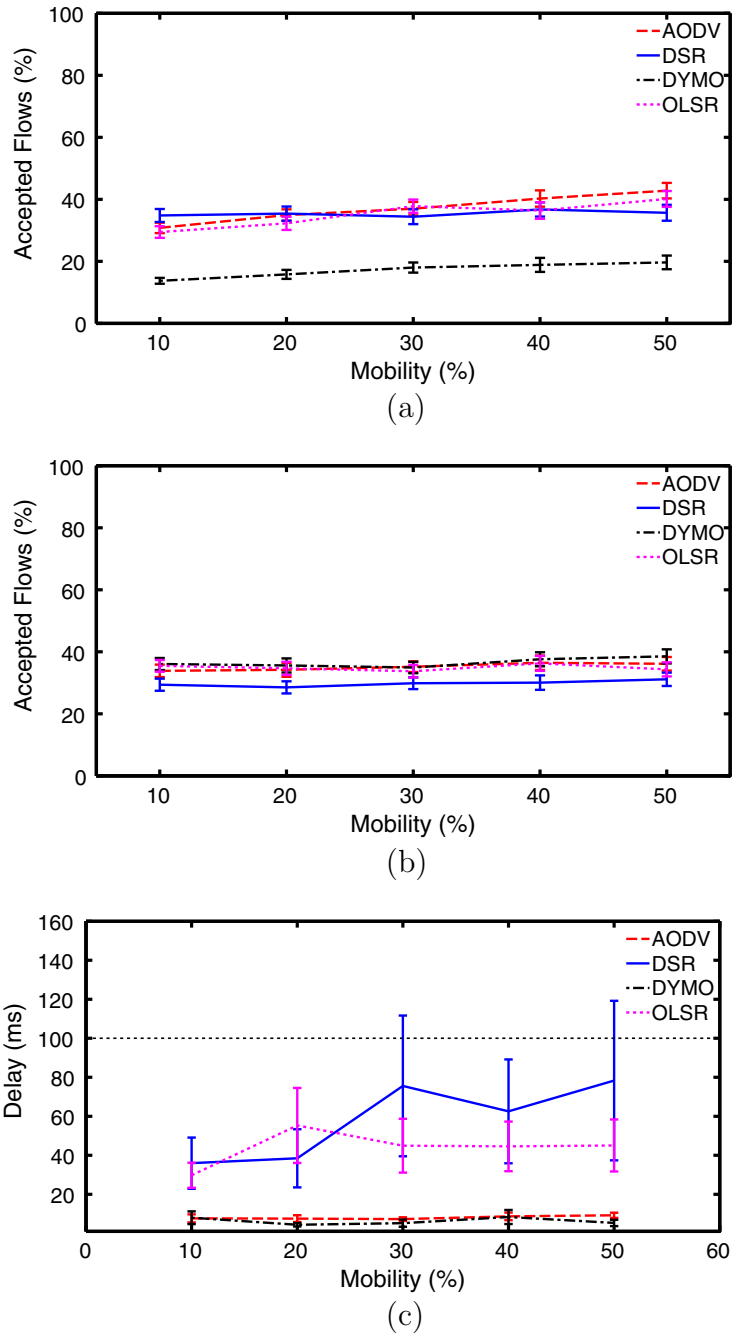
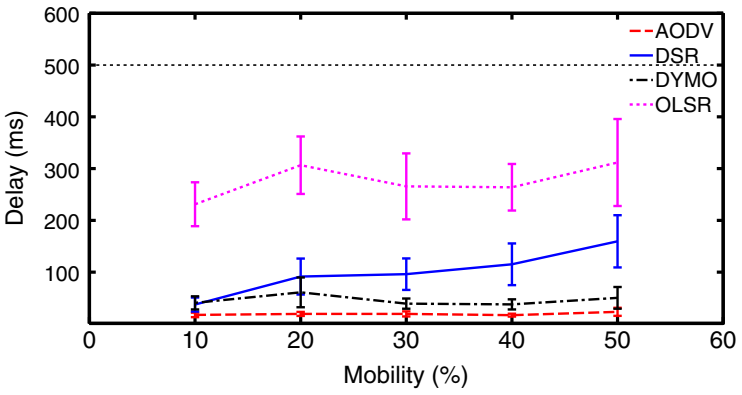
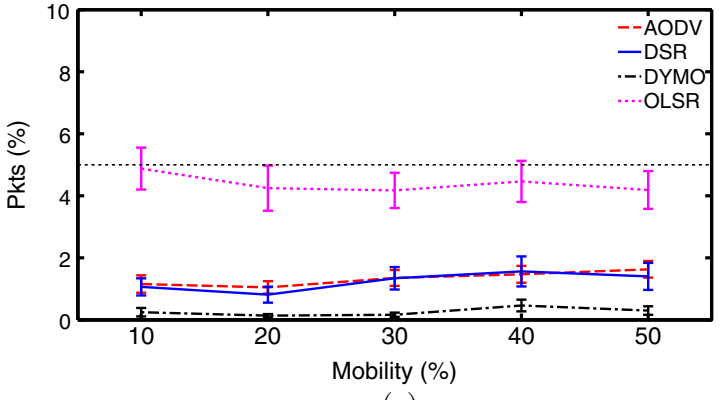


Fig. 8. Statistics of EBAC in a scenario with mobile nodes and a rate of 1 fpm. Figures (a) (voice) and (b) (data) show the percentage of flows accepted; (c) (voice) and (d) (data) depict the average delay of each traffic class; (e) (voice) and (f) (data) correspond to packet losses.

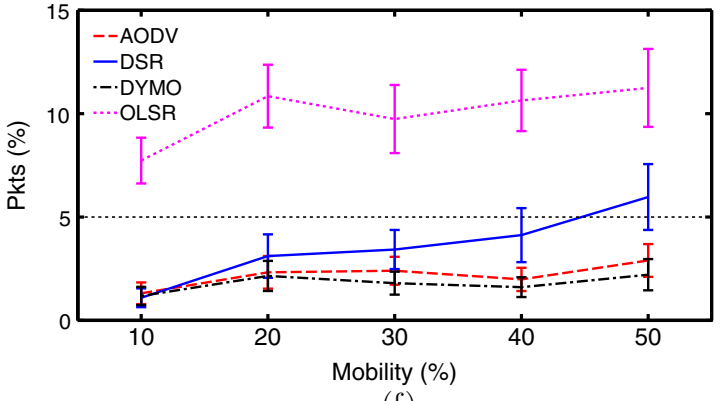
average delay and percentage of lost packets. The percentage of accepted flows, depicted in Fig. 5(a) and (b), is a direct consequence of the probing traffic measurements discussed above. Despite the loss of probing packets, the joint use of the AODV protocol with EBAC led to the highest percentage of accepted flows as a consequence of the low delay produced. In contrast, when the DYMO and DSR protocols are used, the percentage of voice flows accepted is very low. Specifically with the DSR protocol, EBAC can only guarantee delay bound for a rate of incoming flows of 1 fpm. The packet salvaging option of the DSR protocol can be a disadvantage when the network traffic increases and the next hop link is frequently disconnected. When the MAC layer acknowledgment is not received after forwarding a packet, the node tries to salvage the packet. However, if the packet is successfully salvaged, but it has



(d)



(e)



(f)

Fig. 8 (*continued*)

already been delivered to the next-hop node, multiple copies of the same packet may arrive at the destination node. Since EBAC needs to receive the probing packets in the correct order, thus packet salvaging can be a problem rather than a solution.

There is a tendency for an increase of delays for all routing protocols as the rate of incoming flows increase. Only the AODV and DYMO protocols are able to keep the delay within the acceptable bounds (shown as the dotted line in graphs Fig. 5(c) and (d)).

Packet losses are shown in Fig. 5(e) and (f), with dotted line corresponding to 5% packet loss, included as a reference value. The DYMO protocol is the one that produces the lowest packet loss, especially for voice traffic. The AODV protocol also leads to little packet loss, although for voice traffic and for loads greater than 4 fpm, packet

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

loss is very close to the reference value. The joint use of EBAC with the OLSR protocol accepts almost the same percentage of flows as does the AODV protocol, although packet losses either exceed or are very close to the reference value. The DSR protocol produces packet losses even greater than 10% for data traffic under loads greater than 1 fpm.

The number of accepted flows in a wireless scenario, such as the one studied here, depends on the spatial distribution of the flows requesting admission. When traffic flows are close to each other, the acceptance probability is low since nearby flows can interfere with each other. This fact is illustrated in Fig. 6, which depicts the acceptance probability of two different sets of incoming traffic flows while using the AODV protocol. Each set was generated by randomly selecting the source and destination nodes of each traffic flow. Even though the nodes in both cases are located in the same position, the acceptance probability differs, especially for voice traffic and for a rate of incoming flows less than 5 fpm.

5.3. Performance with node mobility

In this section, the EBAC scheme is tested using the same scenario described above but under conditions of node mobility, which is modeled by setting a certain percentage of mobile nodes while the rest remain static. The percentage of mobile nodes will be called the *mobility factor*. Nodes move according to a pedestrian mobility pattern that follows the random waypoint model. The node speed ranges from 0.5 m/s to 1 m/s and the pause time is equal to 180 s.

The operation limits of the EBAC for each routing protocol are determined by assuming the following condition: the maximum value allowed for $P(X > 5\%)$ is 0.1 for both traffic classes, where the random variable X corresponds to the percentage of packet losses. Based on this condition, Table 2 summarizes the limits for the operation of EBAC with each routing protocol.

The joint operation of EBAC and OLSR produced large packet losses. As stated in [11], the OLSR protocol is designed for large and dense networks and this 50-node scenario could not provide the necessary conditions for it to recover from link failures and recalculate routes.

On the other hand, the DYMO protocol is the routing protocol that supports the greater mobility level. Fig. 7 shows the empirical complementary distribution of packet loss for each traffic class when the EBAC scheme operates jointly with each one of the four routing protocols. The figures were obtained at the operation limits of EBAC with DYMO, i.e. 1 fpm and a mobility factor equal to 50%. Especially with voice traffic, the use of EBAC jointly with the DYMO protocol produced the lowest probability that packet losses exceed 5% and it is far better than that of DSR and AODV protocols. Nevertheless, the large delays involved with the use of the DYMO protocol, mean that the EBAC operating jointly with DYMO accepts only half of the voice flows admitted by the other routing protocols, as shown in Fig. 8(a) and (b).

The EBAC scheme keeps the average delay of both traffic classes within the acceptable bounds, as can be seen in Fig. 8(c) and (d). In fact, in terms of average delay and packet losses, the joint performance of the EBAC with AODV and DYMO protocols seems independent of node mobility. However, when the OLSR and DSR protocols were used, both packet loss and the length of delay showed large variance. When operating jointly with the DSR protocol, node mobility increased the average packet delay of both traffic types but almost as many flows were accepted as were when operating with the AODV protocol. However, due to node mobility, alternative routes discovered by the DSR protocol could also be broken when the active route fails.

According to the results obtained here, the best protocol for joint use with the EBAC scheme is the AODV protocol, since it is able to guarantee average packet delay, to accept the largest number of incoming flows and to support up to 40% of mobile nodes for a flow arrival rate of 1 fpm.

6. Conclusions

Envelope-Based Admission Control (EBAC) is a stateless admission control scheme designed for IEEE 802.11 wireless ad hoc networks which is decoupled from the routing protocol. The EBAC measures the envelopes of incoming traffic, as well as the service provided by the network to decide whether to admit an incoming flow. In this paper, EBAC was tested with four routing protocols: AODV, DSR, OLSR and DYMO. Probing packet statistics were analyzed to understand the way that each routing protocol affects the service due to its specific way of handling outbound packets in case of link failures. Based on that analysis, EBAC performance was evaluated both with and without node mobility. It was found that EBAC with OLSR has the poorest performance, probably because the OLSR protocol is a protocol designed for "large and dense networks", and the 50-node scenario did not provide conditions to meet its requirement. With the DSR protocol, EBAC supported up to 1 fpm with a mobility factor of 10%. In contrast, however, the AODV and DYMO protocols allowed the EBAC to support mobility factors up to 40 and 50% respectively, under the incoming flow rate of 1 fpm. Nevertheless, the DYMO protocol accepted only half as many as voice flows did by the other routing protocols, due to long packet delays. Considering the average end-to-end delay, packet losses and the percentage of accepted flows, the use of the AODV protocol in conjunction with EBAC achieved the best performance.

References

[1] L. Hanzo, R. Tafazolli, Admission control schemes for 802.11-based multi-hop mobile ad hoc networks: a survey, IEEE Commun. Surv. Tutorials 11 (4) (2009) 78–108.
[2] M. Salamanca, N. Pena, N. da Fonseca, A distributed envelope-based admission control for multihop IEEE 802.11 ad hoc networks, in: Proceedings of IEEE Latin-America Conference on Communications, 2012, pp. 1–6.
[3] C. Cetinkaya, V. Kanodia, E.W. Knightly, Scalable services via egress admission control, IEEE Trans. Multimedia 3 (1) (2001) 69–81.
[4] M. Salamanca, N. Pena, N. da Fonseca, Evaluation of an envelope-based access control scheme in multihop IEEE 802.11 ad hoc networks, in: Proceedings of IEEE Latin-American Conference on Communications, 2011.

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008

[5] J. Schlembach, A. Skoe, P. Yuan, E. Knightly, Design and implementation of scalable admission control, in: M.A. Marsan, A. Bianco (Eds.), Quality of Service in Multiservice IP Networks, Lecture Notes in Computer Science, vol. 1989, 2001, pp. 1–15.
[6] E. Castillo, Extreme Value Theory in Engineering, Statistical Modeling and Decision Science, Academic Press, 1988.
[7] C. Perkins, E. Royer, Ad-hoc on-demand distance vector routing, in: Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, WMCSA, 1999, pp. 90–100.
[8] D. Johnson, Y. Hu, D. Maltz, The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for Iv4, RFC 4728, February 2007. <http://www.ietf.org/rfc/rfc4728.txt>.
[9] C. Perkins, S. Ratliff, J. Dowdell, Dynamic MANET On-demand (AODVv2) Routing, Draft IETF MANET DYMO 26, February 2013. <http://tools.ietf.org/pdf/draft-ietf-manet-dymo-26.pdf>.
[10] T. Clausen, C. Dearlove, J. Dean, C. Adjih, Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format, RFC 5444 (Proposed Standard), February 2009. <http://www.ietf.org/rfc/rfc5444.txt>.
[11] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), RFC 3626, October 2003. <http://www.ietf.org/rfc/rfc3626.txt>.
[12] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot, Optimized Link State Routing protocol for Ad Hoc networks, in: IEEE International Multi Topic Conference – INMIC, 2001, pp. 62–68.
[13] Qualnet simulator. <http://web.scalable-networks.com/content/qualnet> (last accessed 06.02.14).
[14] R. Estepa, J. Vozmediano, A. Estepa, Background noise influence on VoIP traffic profile, in: V. Roca, F. Rousseau (Eds.), Lecture Notes in Computer Science, vol. 3311, Springer, Berlin/Heidelberg, 2004, pp. 13–24.
[15] M. Salamanca, N. Pena, N. da Fonseca, A distributed envelope-based admission control for multihop IEEE 802.11 ad hoc networks, IEEE Lat. Am. Trans. 11 (3) (2013) 933–940.
[16] C. Perkins, E. Belding-Royer, S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, July 2003. <http://www.ietf.org/rfc/rfc3561.txt>.
[17] F. Baker, Requirements for IP Version 4 Routers, RFC 1812, June 1995. <http://tools.ietf.org/html/rfc1812>.

Maria del Pilar Salamanca received her M.Sc. degree in Electrical Engineering from Universidad de los Andes, Bogotá, Colombia in 2007. Currently, she is member of the Electronics and Telecommunication Systems Group (GEST) at Universidad de los Andes, where she is Ph.D. candidate in Electrical Engineering. She was awarded with a scholarship from the Latin America and Caribbean Collaborative ICT Research (LACCIR) to perform a research stay at Universidade Estadual de Campinas, Campinas, Brazil. Her research interests are bandwidth estimation and QoS in ad hoc networks.

Nestor Misael Peña is Electrical Engineer, Mathematician and M.Sc. in Electrical Engineer from Universidad de Los Andes, Bogotá, Colombia. He received his D.E.A and Ph.D. degree in Telecommunications and Signal Treatment from the University of Rennes 1 in 1994 and 1997, respectively. Currently, he is the Head of the Department of Electrical and Electronics Engineering at Universidad de los Andes. His research interests are modeling and evaluation of communication protocols in ad hoc and sensor networks, development of numerical methods in electromagnetism at very high frequencies, and electromagnetic compatibility.

Nelson Luis Saldanha da Fonseca received his Ph.D. degree from the University of Southern California in 1994. Nelson is a Full Professor at the Institute of Computing, State University of Campinas. He received the 2001 Elsevier Computer Network Editor of the Year and the IEEE Communications Society (ComSoc) Joseph LoCicero Award for Exemplary Services in Publications. Nelson Fonseca is former EiC of the IEEE Communications Surveys and Tutorials. Currently, he serves as Associate Editor for Elsevier Computer Networks, Senior Editor for the IEEE Communications Magazine and for the IEEE Communications Surveys and Tutorials and Editor for the Journal of Internet Services and Applications, Peer-to-Peer Networking and Applications and Journal of the Brazilian Computer Society.

Please cite this article in press as: M.P. Salamanca et al., Impact of the routing protocol choice on the Envelope-Based Admission Control scheme for ad hoc networks, Ad Hoc Netw. (2015), http://dx.doi.org/10.1016/j.adhoc.2015.03.008