



An Evaluation of Weak State Mechanism For Large-Scale Dynamic Networks

R.Vimal Raj

Computer science

Vel Tech Dr.RR & Dr.SR Technical University

R. Krishnamoorthy

school of Electrical

Vel Tech Dr.RR & Dr.SR Technical University

krishnamoorthy.mkr@gmail.com

ABSTRACT: Forwarding decisions in routing protocols rely on information about the destination nodes provided by routing table states. When paths to a destination change, corresponding states become invalid and need to be refreshed with control messages for resilient routing. In large and highly dynamic networks, this overhead can crowd out the capacity for data traffic. For such networks, we propose the concept of weak state, which is interpreted as a probabilistic hint, not as absolute truth. Weak state can remain valid without explicit messages by systematically reducing the confidence in its accuracy. Weak State Routing (WSR) is a novel routing protocol that uses weak state along with random directional walks for forwarding packets. When a packet reaches a node that contains a weak state about the destination with higher confidence than that held by the packet, the walk direction is biased. The packet reaches the destination via a sequence of directional walks, punctuated by biasing decisions. WSR also uses random directional walks for disseminating routing state and provides mechanisms for aggregating weak state. Our simulation results show that WSR offers a very high packet delivery ratio (≥ 98). Control traffic overhead scales as $O(N)$, and the state complexity is $\theta(N^{3/2})$, where N is the number of nodes. Packets follow longer paths compared to prior protocols (OLSR, GLS-GPSR), but the average path length is asymptotically efficient and scales as $O(\sqrt{N})$. Despite longer paths, WSR's end-to-end packet delivery delay is much smaller due to the dramatic reduction in protocol overhead.

Key words: Dynamic networks, unstructured routing, weak state, Weak state Routing, Probabilistic routing table.

I. Introduction

In this Paper, we consider the problem of designing robust and scalable routing protocols for large and dynamic networks like large-scale mobile ad hoc networks (MANETs) or metropolitan-scale vehicular networks, where every vehicle provides an open compute/storage/communication platform. Though such networks are not prevalent today, they show an immense potential for future deployment. We seek to anticipate and understand the fundamental problem of routing and the nature of routing tables in such future networks.

Routing protocols in communication networks rely on routing table entries ("states") to decide where to forward a packet. The routing table state typically maps an ID (e.g., destination address) or an aggregate (e.g., a destination network) to an entity such as a next-hop, a sequence of hops, a location in plane, etc. If a destination moves significantly within the network, the corresponding routing table states become invalid and need to be refreshed. As the network size increases and it becomes more dynamic, routing table entries. Several routers must be refreshed, leading to a huge increase in control traffic

For such large and dynamic networks, we propose to use probabilistic routing tables, where routing table entries are considered as probabilistic hints and not absolute truth. Such state information is called weak state. Weak state can be locally refreshed by reducing the associated confidence value, a measure of the probability that the state is accurate. Weakening the state is similar to aging the state, albeit in terms of semantics. The state is associated with an implicit "soft timeout," i.e., once the associated confidence value is below a threshold, the state is removed from the system.

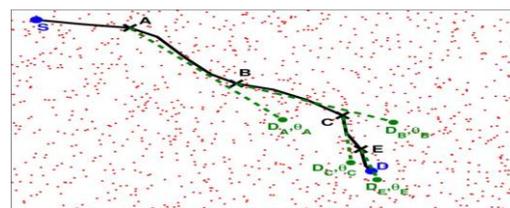


Fig. 1. An illustration of routing with WSR.

A data packet is forwarded from node S to D using random directional walks. The packet is successively biased in intermediate nodes A, B, C, and E in directions toward D_A , D_B , D_C , and D_E , respectively, which are the nodes believed to lead to destination. The strength of the bias at each intermediate

node is $\theta_A, \theta_B, \theta_C, \theta_E$, respectively. Weak state biasing the packet at an intermediate node yields stronger information than the previously biasing state, i.e., $\theta_A < \theta_B < \theta_C < \theta_E$.

The intermediate node biases the packet in the direction toward this location, and the new confidence value is carried by the packet. This directional walk continues until the packet reaches another node that contains a weak state providing information about the destination ID with a higher confidence value or greater accuracy of localization (i.e., stronger state) than what is carried in the packet. The packet's directional walk is now biased using this information. This process of the walks being biased with increasing confidence continues until the packet reaches the destination.

II. Related Work

Traditional state concept can be classified into two broad categories: hard and soft state approaches. Hard state is maintained at a remote node until it is explicitly removed using state-teardown messages by the node that installed the state. Since the state is removed explicitly, reliable communication is essential. Soft state, which was first coined in, times out unless it is refreshed within timeout duration. The node that installed the state periodically issues refresh messages. Once a message is received by the node maintaining the soft state, the timer corresponding to the state is rescheduled. If the timer expires, the state times out and is removed from the system. Soft state does not require explicit removal messages, unlike hard state. Hence, reliable signalling is not required. Analytical comparisons of hard state, soft state, and the hybrid approaches are presented.

In both hard state and soft state, the state information is regarded as absolute truth. We refer to such state information as having strong semantics or that it is an example of strong state. When the original state changes, the strong state value at the remote nodes should be explicitly refreshed in both approaches (hard or soft). Weak state, on the other hand, has "weak" or probabilistic semantics. The state can be refreshed locally by weakening or decaying the confidence value associated with the state over time. The confidence value is an estimate of the probability that the true state is valid. Once the confidence in the state is below a threshold value, the state is removed from the system. Weakening the state is similar to aging it and is equivalent to a soft timeout. Hence, weak state is a generalization of soft state. A comparison of hard, soft, and weak states is given in Fig. 2.

MANET routing that uses link states has two subclasses: proactive routing (for large but less dynamic networks) and reactive or on-demand routing (for dynamic but relatively smaller networks). Recent protocols such as FRESH and EASE utilize node encounter histories as "state." They use iterative searches to find nodes that encountered the destination more recently. FRESH forwards a packet to an intermediate node that encountered the destination more recently, whereas EASE sends it to the location where the destination is encountered by such an intermediate node.

These works are inspired by Tse Grossglauser model. If the mobility scope is small relative to the size of the network, packets may not be delivered to the destination. PROPHET positions itself between the two extremes. It maintains transitive probabilities for each destination, such as a probabilistic distance vector. The state information is used to create gradients toward the destination rather than an explicit mapping as in WSR.

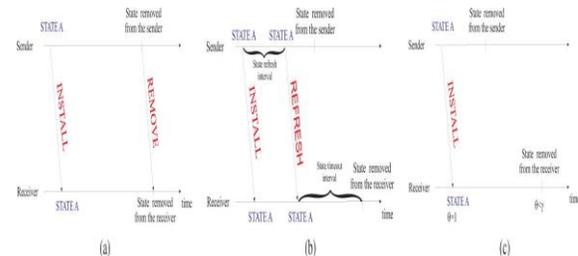


Fig.2. comparison summary of hard-state, soft-state, and weak-state approaches.

Hard state requires explicit control message to be removed. Soft state times out if it is not refreshed within the timeout interval. Weak state is associated with a confidence value θ , which is a decreasing function of time. When the confidence is below a threshold value γ , it is removed.

WSR functions as a distributed hashing method. Therefore, WSR resembles the distributed hash tables (DHTs) that provide lookup services at large-scale P2P networks. In a DHT, every node stores a range of keys, and any node can locate the node in which a particular key is stored using consistent hashing. A DHT relies on a structured overlay network. In it has been shown that maintaining such a structure is hard and may require substantial overhead in P2P systems. This is also true for mobile networks.

III. WEAK STATE ROUTING

This section presents the details of the WSR protocol. Specifically, we address the following:

- 1) Assumptions made by WSR;
- 2) Weak state and its semantic strength;
- 3) Proactive location announcements from destinations using random directional walks;
- 4) Packet forwarding strategy using successively biased random directional walks.

A. Assumptions

The assumptions WSR makes are similar to those made by traditional location based routing protocols: Nodes know their positions on a 2-D plane, either using a GPS device or through any other localization techniques. By using periodic single hop beacon messages, each node also knows its neighbours and their positions. The nodes have uniform unidirectional antennas. The source nodes in general do not know the location of the destination nodes. We consider the

scenario where the nodes move independently and the network density is high enough for connectivity at any time. The maximum node speed is known. Though this value can be large, we assume that the average displacement in unit time is small in comparison to the maximum distance between any two points in the area covered by the network.

B. Weak State Realization

In WSR, a weak state corresponds to a mapping from a persistent node ID or a collection of IDs (SetofIDs) to a geographical region (GeoRegion) in which the node (or the set of nodes) is believed to be currently located. The state information captures the uncertainty in the mapping. An explicit mapping from a SetofIDs to a GeoRegion can be used to “bias” the random directional walks of packets being forwarded. If the destination ID is an element of the SetofIDs, the packet can be biased toward the center of the associated Geo-Region (subject to other conditions described later in this section).

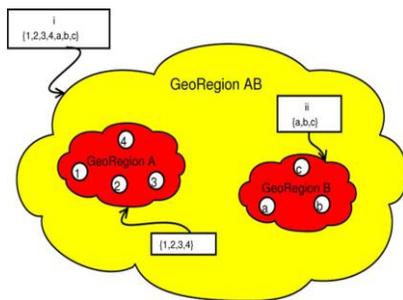


Fig. 3. Weak state concept: A set of nodes (SetofIDs) are mapped to an aggregated geographical region (GeoRegion). Mappings are more definite for closer nodes.

The union of two filters is a new filter with the same size and characterized by the same hash functions and obtained by the bitwise OR operation. In a regular Bloom filter, the membership query for an element yields yes only if all the bits in array positions are 1. Bloom filters are subject to false positives, and the false-positive rate increases with the number of elements added to the filter. To reduce the false positives, we also use a limit on the total number of bits set to 1 in Bloom filter B, which we call the cardinality and denote by B . Similar to the limit on the radius of the GeoRegion portion of the mapping, reaching the cardinality limit triggers the decay of SetofIDs portion the mapping. The decaying schedule of a mapping is summarized in Fig. 6. In addition, if the union of two mappings violate either criterion, we do not combine them.

C. Semantic Strength of Mappings

The forwarding decisions of the intermediate nodes are based on the quality of information that the mappings

offer. We now explain the mapping quality using two strength parameters: spatial strength and temporal strength.

1) Spatial Strength: The spatial strength of the mapping involves the uncertainty in the GeoRegion portion of the mapping. Consider two mappings M1 and M2 with GeoRegion portions A1 and A2, respectively. Given that for node $P_{\{m(t) \in A1\}} = P_{\{m(t) \in A2\}}$, we say that is spatially stronger if represents a smaller region, i.e., its radius is smaller than that of and it yields a more definite region.

2) Temporal Strength: The temporal strength of the mapping is associated with the probability of a node being placed in the GeoRegion part of the mapping. Again, consider two mappings

and with corresponding GeoRegions and .We say that is temporally stronger for node at time if node is placed in at time with a larger probability, i.e., Given that node is located within a region at time, i.e., $P_{\{m(t) \in A1\}} > P_{\{m(t) \in A2\}}$, the probability of the node being in the same area in a future time, is a nonincreasing function of. Therefore, a temporal strength one that provides more recent information about a node should be temporally stronger $P_{\{m(t) \in A1\}} = P_{\{m(t) \in A2\}}$.

D. Dissemination of Location Information

Our routing mechanism is based on forwarding data packets toward the region where the node believes the destination is located using the information given by weak states. Initially, nodes have no information about the location of the destination. Nodes know the location of their neighbours through periodic beacon messages. Once two nodes that were neighbours become nonneighbours, i.e., get out of each other's transmission range, they create mappings for each other using their last known locations. For nodes farther away, WSR uses periodic announcements from destinations in random directions (random directional walks) to disseminate location information. Note that a random directional walk is different from a standard.

Random walk. In random walks, the random walker can proceed to each neighbour with equal probability. In random directional walks, a node selects the direction of the announcement packet randomly and sends the announcement in that direction, and the walk proceeds in that chosen direction. The node first picks an angle uniformly between 0 and radians. The direction on which the location announcement is sent is determined by this angle. WSR calculates the position of a point that is far from the location of the node along this direction (a point outside the area Covered the network) and uses geographical routing to forward the announcement.

E. Forwarding Data Packets

Our data forwarding mechanism is a simple greedy geographical forwarding algorithm, albeit using random directional walks and consulting the weak state at intermediate nodes. Similar to announcement packets, a data packet is initially sent in a random direction (assuming the source does not have any weak state information about the

destination). However, unlike location announcements, a data packet is subsequently biased at an intermediate node if the node has a weak state about the location of the destination. We leave the problem of acknowledgements and reliability, i.e., recovery of lost packets, to the higher layers (transport).

IV. Asymptotical Performance Analysis

In this section, we present a simple mathematical analysis that characterizes the asymptotical performance of our scheme. We show that the number of mappings stored in the network and the average path length scale as $\theta(N^{3/2})$ and $O(\sqrt{N})$ respectively. We study the notion of the weakness in terms of consistency of protocol decisions in a separate paper [11].

A. State Complexity

The location announcements are sent along the random directions with a constant TTL value. Therefore, each announcement is received by nodes. The procedure given in Section IV-B determines the probability for decaying SetofIDs portions of the mappings so that nodes maintain information about a destination for a duration that scales as $\theta(\sqrt{N})$. Within this duration, nodes receive the location announcements from a particular node because the announcements are sent in random directions and the nodes move independently. This implies that nodes maintain information about that node and each node maintains information on $\theta(\sqrt{N})$ nodes.

Because of the constant WBF length and the limit on the maximum number of bits set to 1 in WBF, SetofIDs portion of each mapping contains nodes. Hence, the number of mappings a node stores scales the same way as the number of nodes it maintains information about, i.e., $\theta(\sqrt{N})$. Since the WBF length is constant, this is also the number of bits a node allocates for state storage. If we consider the entire network, the state complexity of protocol becomes $\theta(N^{3/2})$.

TABLE I PROTOCOL PARAMETERS

Parameter	Description
u	WBF width in bits
γ	Minimum temporal strength (# 1-bits in a WBF for a node below which the state is timed out)
k	Number of hash functions in the WBF
p	Decaying probability
T_A	Announcement TTL
T_D	Data packet TTL

B. Path Length

In this section, we show that a random directional walk is received by a node that has complete temporal strength about the destination after it is biased by at most a constant time and forwarded hops, with high probability. At this point, the region where the destination is located is known with certainty, and we show that the probability of packet delivery is very high within another hop. Given that nodes maintain information about the destination, the fraction

of the nodes with the information about this destination is $\theta(1)$, where θ is a constant. Let n denote the number of hops a random directional walk is forwarded until the packet first encounters a node containing information about the destination. We have Hence

$$P(n > n) = (1 - q)^n (1 - c/\sqrt{N})^n$$

Where n is a constant. Let P be the probability that it is biased at a node that has information about the destination after it is forwarded times.

$$1 - P = (1 - c/\sqrt{N})^{b \cdot \sqrt{N}} \approx e^{-c|b|}$$

In words, a packet that is forwarded times is biased with an approximately high probability. This probability is high if the product is large.

In WSR, the protocol first checks the temporal strength of the mappings to bias the packets. Remember that the temporal strength of a mapping is given by the number of 1's in the indices that correspond to destination ID. There are a total of temporal strength levels in the mappings (see Table I for n and c). Because of the way the decaying probability is set, the number of nodes that have a weak state with temporal strength is in for each such that $\theta(\sqrt{N})$.

V. Conclusion And Future Work

We present Weak State Routing (WSR) protocol, an unstructured forwarding paradigm based on the partial knowledge about the node locations. The nodes periodically announce their locations on random directions. The nodes use these announcements to create aggregated SetofIDs-to-GeoRegion mappings. A routing state consists of a weak Bloom filter (WBF) that contains a set of nodes and a geographical region where the nodes are believed to be located. WBF also yields the confidence that a node is an element of SetofIDs. When a node has a data packet, the packet is sent in a random direction with the belief that an intermediate node will give the packet a superior hint about the location of the destination node. The packet trajectory is then biased toward the center of the region indicated by this state value.

WSR provides a high data packet delivery ratio greater than 98%. The total control traffic overhead scales as $\theta(\sqrt{N})$, where θ is the number of nodes. The state complexity of the protocol is $\theta(N^{3/2})$. The average path length is $\theta(\sqrt{N})$ and asymptotically efficient in that routes are at most a constant factor longer than the shortest path. Our simulation results show that WSR significantly outperforms OLSR and GLS with GPSR in large-scale networks achieving high reach ability, low overhead and delay, but needing a larger number of hops to reach the destination.

REFERENCES

[1] U. G. Acer, S. Kalyanaraman, and A. A. Abouzeid, "Weak state routing for large scale dynamic networks," in Proc. ACM MobiCom, 2007, pp. 290–301.

- [2] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in Proc. IEEE INMIC, 2001, pp. 62–68.
- [3] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris, "A scalable location service for geographic ad hoc routing," in Proc. ACM MobiCom, 2000, pp. 120–130.
- [4] B. Karp and H. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in Proc. ACM MobiCom, 2000, pp. 243–254.
- [5] N. Bisnik and A. A. Abouzeid, "Capacity deficit in mobile wireless ad hoc networks due to geographic routing overheads," in Proc. IEEE INFOCOM, 2007, pp. 517–525.
- [6] D. Wang and A. A. Abouzeid, "Link state routing overhead in mobile ad hoc networks: A rate-distortion formulation," in Proc. IEEE INFOCOM, 2008, pp. 2011–2019.
- [7] B.-N. Cheng, M. Yuksel, and S. Kalyanaraman, "Orthogonal rendezvous routing protocol for wireless mesh networks," IEEE/ACM Trans. Netw., vol. 17, no. 2, pp. 542–555, Apr. 2009.
- [8] D. D. Clark, "The design philosophy of the DARPA internet protocols," in Proc. ACM SIGCOMM, 1988, pp. 106–114.