A New Routing Technique of Weak State Identification in Large Scale Dynamic Networks

K.V.V.Haritha [#1], S.Sowjanya [#2]

[1#] B.Tech Scholar

Department of CSE ,

Kaushik College Of Engineering,Gambheeram
Visakhapatnam,AP,India.

[2#] B.Tech Scholar

Department of CSE ,
Gayatri Vidya Parishad,College of Engineering for Women
Kommadi, Visakhapatnam,AP,India.

Abstract

Routing in communication networks involves the indirection from a persistent name (or ID) to a locator. The primary goal of a routing protocol is to gather information, which gives directions on performing these indirections and how to reach a node with a specific ID. In a large-scale, highly dynamic network, the ID-to-locator mappings are both large in number, and change often. Traditional routing protocols require high overhead to keep these indirections up-to-date. In this paper, we propose Weak State Routing (WSR), a routing mechanism for large-scale highly dynamic networks. WSR's novelty is that it uses random directional walks biased occasionally by weak indirection state information in intermediate nodes. The indirection state information is *weak*, i.e. interpreted not as absolute truth, but as *probabilistic hints*. Nodes only have partial information about the region a destination node is likely to be. This method allows us to *aggregate* information about a number of remote locations in a geographic region. In other words, the state information maps a *set-of-IDs* to a *geographical region*. The intermediate nodes receiving the random walk use a method similar to longest-prefix-match in order to prioritize their mappings to decide how to bias and forward the random walk. WSR can also be viewed as an unstructured distributed hashing technique. WSR displays good rare-object recall with scalability properties similar to structured DHTs, albeit with more tolerance to dynamism and without constraining the degree distribution of the underlying network. Through simulations, we show that WSR offers a high packet delivery ratio, more than 98%. The control packet overhead incurred in the network scales as $O(N)$ for N-node networks.

Keywords: Dynamic Networks, Routing Algorithms, Unstructured Distributed Hashing, Weak States, Weak state Routing

1. Introduction

Routing in communication networks involves the *indirection* from a *persistent name (or ID)* to a *locator*. The primary goal of a routing protocol is to gather information, which gives directions on performing these indirections and how to reach a node with a specific ID. In a dynamic network where the network topology and the neighborhoods of nodes continuously change, the information the nodes use to make routing decisions should also change and remain up-to-date for resilient routing.

One approach in routing is to use the geographical location information where forwarding is achieved by leveraging Cartesian properties like distance and direction as in Greedy Perimeter Stateless Routing (GPSR) protocol [1]. In dynamic networks, such a mechanism may be favored over link state protocols because the entropy of the link state is usually higher than the node location entropy. Still, ID-to-location indirection is a problem and nodes require an efficient location service which tracks down location changes in the network through receiving location updates from all the nodes. Updating location information in remote location servers causes overhead and deteriorates the capacity of the network [2].

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.

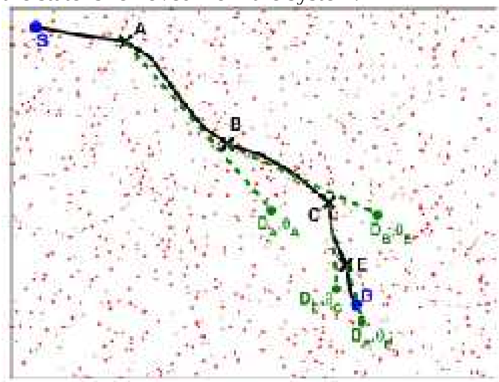


Fig. 1. An illustration of routing with WSR

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 the nodes believe to lead to destination. The strength of the bias at each intermediate node is θ_A, θ_B ,θ_C , θ_E , respectively. Weak state biasing the packet at an intermediate node yields stronger in format ion 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 informat ion 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 informat ion. This process of the walks being biased with increasing confidence continues until the packet reaches the destination.

2. Background Theory

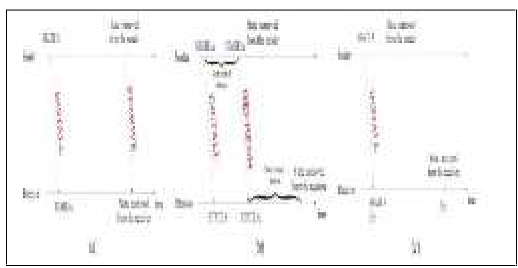
Routing protocols are classified into four major types: reactive, proactive, position-based, and hybrids of these approaches.Reactive protocols like Dynamic Source Routing (DSR) [3] flood the network to perform route discovery when a path between a source node and a destination node is needed. Data is not transmitted until a route is found. Typically, the changes in the routes are handled by route maintenance schemes, in which the node experiencing route failure flood the network to find a new route. Flooding route discovery and maintenance packets may not be a problem in small scale networks. However, the cost of flooding the network is significant in large scale networks. By contrast, proactive protocols like Destination Sequence Distance Vector (DSDV) [4] periodically broadcast route information across the entire network. When a node needs to send a packet to a destination node, it knows the path to this node without the route discovery phase. Similar to reactive protocols, network floods of control packets cause high overhead. In dynamic networks, the nodes need to broadcast state information frequently in order to keep up with the changes in the network topology.

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 communicat ion 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 signaling 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 informat ion 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 informat ion is used to create gradients toward the destination rather than an explicit mapping as in WSR.



[illegible]

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.

3. Weak State Routing

In this section, we detail the assumptions, weak state concept, specifications of WSR. Specifically, we address the following:

1) Assumptions made by WSR.

2) Explanation of state concept and weakening the states.

3) Proactive element of WSR: location announcements.

4) Packet forwarding strategy using successively biased random directional walks.

3.1. 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.

3.2. Weak State Realization

In WSR, a weak state corresponds to a mapping from a persistent node ID or a collection of IDs (Set of IDs) to a geographical region (GeoRegion) in which the node (or the set of nodes) is believed to be currently located. The state informat ion 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).Once either the limit on the maximum radius of the GeoRegion portion of the mapping or the limit on the cardinality of the SetofIDs portion of the mapping is reached, the nodes decay the SetofIDs portion of the indirections they maintain. We refer to this weakened SetofIDs portion of the indirection as a "weak Bloom filter" (WBF). A WBF is similar to exponentially decaying Bloom filter (EDBF) proposed for P2P networks in [5]. In that method, the Bloom filter data structure is used to represent a set of resources that can be reached through a particular node either directly or over multiple hops after that node. The filters are decayed at every hop they propagate by setting a random subset of bits to 0. In other words, the filter becomes a probabilistic or fuzzy set, and a query yields a *signal* (or probability) of membership, rather than a binary yes/no or 0/1 answer. A random walk in a P2P network would sense a local gradient in the "signal" between a node and its neighbors and use that information for biasing its progress.

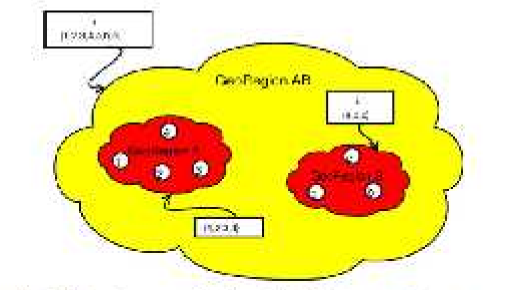


Fig. 3. Weak state concept: A set of nodes (SetofIDs) are mapped to an aggregated geographical region (GeoRegion). Mappings are more definite for closer nodes.

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 bit s set to 1 in Bloom filter B , which we call the cardinality of 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. In addition, if the union of two mappings violate either criterion, we do not combine them.

3.3 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)ϵ A1}= P{m(t)ϵ 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)ϵ A1} > P{m(t)ϵ A2} , the probability of the node being in the same area in a future time , is a non increasing function of. Therefore, a temporal strength one that provides more recent information about a node should be temporally stronger P{m(t)ϵ A1}= P{m(t)ϵ A2}.

3.4. 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 informat ion about the location of the destination. Nodes know the location of their neighbours through periodic beacon messages. Once two nodes that were neighbours become nonneighbors, 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 informat ion. 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.

3.5. 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).

4. 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 [6].

4.1. 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 4.2 determines the probability for decaying SetofIDs portions of the mappings so that nodes maintain information about a destination for a duration that scales as 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[7]. This implies that nodes maintain information about that node and each node maintains information on 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., 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
m	WBF width in bits
c	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

4.2. 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 , where is a constant. Let 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

$$P(n1 \cdot n) = (1-q1)^{n}(1-c1/\sqrt{N})$$

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

$$1-P1 = (1-c1/\sqrt{N})^{b1\sqrt{N}} \approx e^{-c1b1}$$

In other 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[8]. 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 $\theta\ (\sqrt{N})$.

5. Conclusion

In this paper, we present the Weak State Routing (WSR) protocol, an unstructured forwarding paradigm based on the partial knowledge about the node locations. WSR offers high data packet delivery ratio in large and highly dynamic ad-hoc networks without incurring extensive overhead as flooding based routing mechanism do. The intermediate nodes forward data packets in the absence of location service. The nodes periodically announce their locations on random directions. The nodes receiving these announcements create ID-to-location mappings and combine it with the information about the nodes that are proximate to the announcing node. WSR provides high data packet delivery (at least 98%), with overhead increasing linearly with the number of nodes N and the total number of mappings scaling as $\Theta(N^{3/2})$. We also showed that increasing node speed up to 20 m/s does not significantly affect the performance. WSR enjoys these benefits at the cost of increased path length. Especially for very large scale networks (with nodes more than 700), our simulation results show that WSR significantly outperforms DSR and GLS with GPSR retaining high reachability, low overhead and delay but with higher number hops to reach the destination. Even though GLS stores less number of entries in its location database, the number of states WSR stores has good scalability properties.

6. References

[1] KARP, B., AND KUNG, H. Gpsr: Greedy perimeter stateless routing for wireless networks. Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM (2000), 243 – 254.

[2] BISNIK, N., AND ABOUZEID, A. A. Capacity deficit in mobile wireless ad hoc networks due to geographic routing overheads. In 26th IEEE International Conference on Computer Communications (INFOCOM'07). (2007),pp. 517–525.

[3] JOHNSON, D. B., AND MALTZ, D. A. Dynamic source routing in ad hoc wireless networks. In Mobile Computing, T. Imielinski and H. Korth, Eds., vol. 353. Kluwer Academic Publishers, 1996.

[4] PERKINS, C. E., AND BHAGWAT, P. highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. Computer Communications Review 24, 4 (1994), 234 –.

[5] KUMAR, A., XU, J., AND ZEGURA, E. W. Efficient and scalable query routing for unstructured peer-to-peer networks. Proceedings of IEEE INFOCOM 2 (2005), 1162 – 1173.

[6] GROSSGLAUSER, M., AND VETTERLI, M. Locating mobile nodes with ease: Learning efficient routes from encounter histories alone. IEEE/ACM Transactions on Networking 14, 3 (2006), 457 – 469.

[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 DARPAinternet protocols," in Proc. ACM SIGCOMM, 1988, pp. 106–114.

7. About the Authors

K V V Haritha is currently pursuing her B.Tech in CSE at Kaushik College of Engineering, Gambheeram, Visakhapatnam. Her area of interests includes Networks and Security.

S.Sowjanya is currently pursuing her B.tech in CSE at Gayatri Vidya Parishad, College of Engineering for Women, Visakhapatnam. Her area of interests includes Networks and Security