Skewed Map Forwarding for Location-Based Multipath Routing in Ad Hoc Networks

Chang Liu* and Winston K.G. Seah†*

*School of Computing, National University of Singapore, Singapore 117543
†Network Technology Department, Institute for Infocomm Research, Singapore 119613
Email: liuchang@nus.edu.sg, winston@i2r.a-star.edu.sg

Abstract— **In this paper, we present a generic extension of location-based ad hoc routing protocols named Skewed Map Forwarding (SMF). SMF incorporates multipath routing into any location-based routing protocol, while preserving the stateless property of location-based protocols. It alters/distorts the view of the network topology from the routing protocol by mapping the physical coordinates of nodes to logical coordinates and letting the routing protocol work on these logical coordinates. The resultant routes discovered by the routing protocol would appear as being skewed from the original route, thus creating multiple routes depending on how much we alter the view of the topology. We evaluate the performance of SMF as an extension of GPSR using the GloMoSim simulator.**

I. Introduction

In this paper we aim to combine the advantages of location-based routing protocols and multipath routing protocols in ad hoc networks. We introduce the characteristics of these two families of protocols and why it is a challenge to combine their strengths before we proceed to describe our approach to the problem.

A. Location-based Routing

A class of distributed ad hoc routing protocols called *location-based routing* emerged in the past few years. It exploits the fact that in mobile ad hoc networks, connectivity is usually associated with proximity. Location-based routing assumes that 1) each node knows its own *geographical address*, either from some localization hardware or from a distributed ad hoc localization protocol, and 2) the sender knows the *geographical address* of the receiver. This can be satisfied by a location service protocol, such as Grid Location Service (GLS) [1] or Geographic Hash Table (GHT) [2].

Current high performance location-based routing protocols such as Greedy Perimeter Stateless Routing (GPSR) [3] and Greedy Other Adaptive Face Routing (GOAFR/GOAFR+) [4][5] demonstrate that location-based routing can be nearly stateless. Topology information needs to be propagated for only a single hop. Therefore, the only control messages (overheads) are the periodic HELLO messages. A routing decision made at each node is derived solely from the destination address, local topology and any additional information stored in the packet. The primary method of location-based routing is *greedy forwarding*. In greedy forwarding, a packet is forwarded to the neighbor physically nearest to the destination. Other techniques, such as *face routing*, can be used to recover from zones where the greedy heuristic fails.

The stateless property gives location-based routing protocols some unique advantages. Like reactive protocols, location-based protocols do not maintain topology information when there is no traffic, and like proactive protocols, they incur minimal setup time when a connection needs to be established. Stateless location-based routing protocols are arguably the most scalable reactive ad hoc protocols currently known.

However, the stateless property precludes any precise control over the routing path, because such a control almost necessarily implies propagation of routing information. As we shall see, effective multipath routing is impossible without considerable control over the exact path taken.

B. Multipath Routing

Multipath routing protocols aim to build more than one path during one route discovery phase, preferably with little additional work on top of that needed to establish a single path. The main advantages of multipath routing protocols are fault tolerance and load balancing [6].

In multipath routing protocols, when one path breaks, communication can continue via the remaining paths, while a new path is established to replace the broken one. This is the fault tolerance property. It can avoid disrupting time sensitive services. Since location-based routing protocols do not have a route setup phase, a location-based multipath routing protocol would necessarily focus on the other property – load balancing.

Load balancing refers to the distribution of traffic among available network resources, like different possible routes. Load balancing can be a complex cross-layer design problem involving resource allocation over different layers of the protocol stack. However, in this paper we focus solely on providing high-quality multiple paths in layer 3. To reduce contention between the multiple paths, multipath protocols usually require the paths to be either *link-disjoint* or *node-disjoint*. Link-disjoint paths must not share a common link, whereas node-disjoint paths must not share a common node.

Most current ad hoc multipath routing protocols are extensions of Ad hoc On-demand Distance Vector (AODV) protocol [10] or Dynamic Source Routing (DSR) protocol [11], the two most prominent ad hoc routing protocols today. Both AODV and DSR are reactive in the manner that they discover new routes using a network-wide flood of route requests. Not surprisingly, multipath protocols emphasize on redesigning the route discovery phase. The different protocols compete on designing route request (RREQ) and route reply (RREP) propagation rules that find as many paths as possible with the desired disjointness and hop count requirements.

C. Problem Statement

From the preceding discussion, we can see a clear mismatch between location-based routing and current multipath routing protocols. In location-based routing protocols, the sender only needs minimal information to send out a packet, therefore no network-wide flood or setup delay is necessary. In contrast, discovering effective multiple paths requires a more involved flooding process and when existing routes are broken, a new route discovery cycle may be necessary. It is therefore a challenge to design a location-based multipath protocol that 1) is stateless, and 2) finds multiple paths satisfying strict disjointness conditions.

In this work, we propose to insert an additional layer between the location-based routing protocol and the link layer protocol, as shown in Figure 1. The *Skewed Map Forwarding* (SMF) protocol is responsible for altering the view of the network as seen by the layer above, so that we can assert some influence on the location-based routing protocol without modifying them. This novel approach makes our multipath protocol a generic extension that is applicable to all location-based routing protocols.

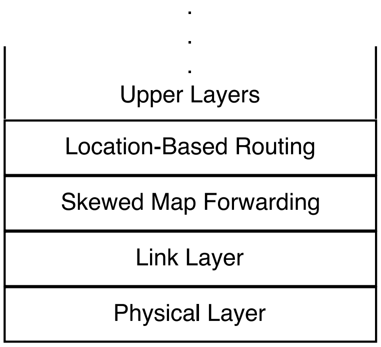

Fig. 1. Layers of a location-based ad hoc protocol stack

II. Skewed Map Forwarding

A. The Protocol

The principle technique SMF uses to *influence* the path taken by the packets is to map the nodes' physical addresses to logical coordinates, and to run the location-based routing protocol in logical coordinates. The mechanism is demonstrated in Figures 2 to 4.

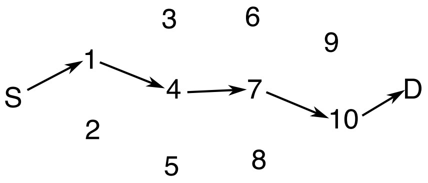

Fig. 2. An example ad hoc network

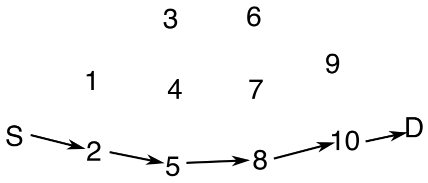

Fig. 3. Intermediate nodes have been moved upwards relative to S and D.

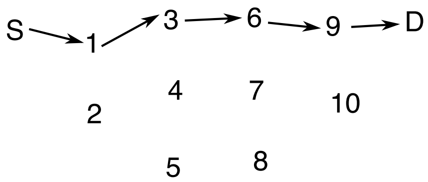

Fig. 4. Intermediate nodes have been moved downwards relative to S and D.

Figure 2 shows an arbitrary ad hoc network and the chain of arrows depicts a likely route discovered by greedy forwarding. If SMF maps physical addresses to logical addresses in such a way that the positions of both the source and the destination are unaffected but all the intermediate nodes are moved upwards (by different amounts), then to the location-based routing protocol in the upper layer, the network appears as in Figure 3. Assuming greedy forwarding, the route discovered is likely to be the one in the figure, $S \to 2 \to 5 \to 8 \to 10 \to D$. Similarly, if SMF's mapping function moves all intermediate nodes downwards, then the network would look like Figure 4. The likely route to be chosen is then $S \to 1 \to 3 \to 6 \to 9 \to D$.

In reality, the mapping function of SMF is parameterized, it can either be the one shown in Figure 3 or the one in Figure 4, depending on the value of the parameter, which we refer to as α. The α value to be used by SMF to route a particular packet is recorded in the header of the packet. Therefore, every packet can have a different α value.

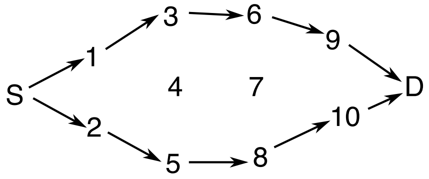

Fig. 5. Packets are forwarded along two different paths

It is important to remember that the different networks shown in Figures 3 and 4 are simply an illusion created by SMF. There is only one physical network, shown in Figure 2. If we send a stream of packets with alternating α values, then the packets will follow the two different paths to their destination and the network traffic is shown in Figure 5. We have incorporated multipath routing into a location-based ad hoc network, and the resulting protocol remains stateless.

B. The Mapping Function

The mapping function from physical address to logical address lies at the heart of the SMF protocol. The importance of the mapping function is that it redefines the *preferred path* of the location-based routing protocol. In a plain location-based routing protocol, the straight line connecting the source and the destination is the preferred path[1]. If SMF is in use, then the straight line connecting the source and the destination *in logical coordinates* is the preferred path. The shape of the preferred path in physical coordinates therefore depends solely on the mapping function.

Regardless of the exact form of the preferred path, we may assume a reasonable choice has the following properties:

1) It passes through points $(-1, 0)$ and $(1, 0)$, the normalized source and destination addresses.
2) The preferred paths when $\alpha = \alpha_0$ and $\alpha = -\alpha_0$ are symmetrical about the x-axis.
3) When $\alpha = 0$, the preferred path is the x-axis.
4) As the absolute value of α increases, the preferred path deviates further from the x-axis.

A very simple type of mapping function with the properties above is defined as follows:

$$(x', y') = f_\alpha(x, y) = (x, y - \alpha \cdot p(x))$$

Here, the coordinates of the source and of the destination have been normalized to $(-1, 0)$ and $(1, 0)$ respectively. It is easy to verify that the function $\alpha \cdot p(x)$ defines the new preferred path in physical coordinates given the value of α. The function $p(x)$ defines the preferred path when $\alpha = 1$. The preferred paths at other α values are obtained by vertical scaling.

The function $p(x)$ can take on many formats, such as Bezier curves or simple polynomial functions. In this paper, we use

$$p(x) = 1 - x^6$$

III. Parameter Tuning

Whereas intermediate nodes participating in SMF only needs to route according to the α-values recorded in the header of the packets, it is the responsibility of the end nodes to decide the exact α values to use for optimal multipath performance.

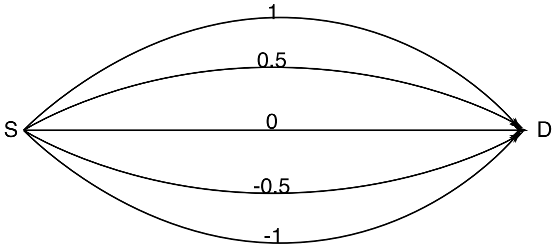

Fig. 6. Effect of α value on the preferred path

Larger $|\alpha|$ values cause the paths taken to deviate further from the shortest path. This leads to a larger hop count and may degrade the network throughput. Conversely, if the $|\alpha|$ values are too small, the different

[1] At least when only greedy forwarding is considered.

paths may be too close, which results in contention among nodes transmitting packets simultaneously. Typically, conventional multipath routing protocols enforce the following criteria during the path discovery phase:

1) The hop-count of every alternative path discovered must satisfy some requirement. For example, in Split Multipath Routing (SMR) [9], intermediate nodes only propagate RREQs whose hop count is not larger than that of the first received RREQ.
2) The alternative paths discovered must satisfy some disjointness requirement, such as node-disjointness or link-disjointness.

The above criteria help the protocols discover efficient multiple paths. However, they are tied to the route discovery phase. In SMF, the absence of such a phase necessitates continuous adjustment to the α values used. In this section we discuss how the appropriate α values are found.

A. Establishing the Value of α

We study the case when two paths are used for each data stream $S \rightarrow D$. The same scheme can be adapted to more than two paths with minor modifications. For simplicity, we shall use α_0 and $-\alpha_0$ ($\alpha_0 > 0$) as the α values of the two paths. The optimal α_0 is then the smallest α_0 for which there is no contention between the two paths.

We first try to estimate the range of "reasonable" α_0 values in SMF. Let s be the average distance between neighboring nodes, P_α be the preferred path given the α value, and let $p(x) = 1 - x^6$ as previously defined. We observe that even if S and D are $20s$ apart, P_α and $P_{\alpha+0.05}$ are separated by at most $s/2$. Therefore, in medium-sized networks with at most a few hundred nodes, changes of α smaller than 0.05 can be considered insignificant. On the other hand, when $\alpha = 2$, the length of the preferred path is almost three times the direct distance between S and D. Having a higher performance than the plain location-based routing protocol when $\alpha > 2$ is highly unlikely. Therefore, the "reasonable" range of α_0 is fairly limited, roughly between 0 and 2.

At the beginning of each data stream $S \rightarrow D$, we can set α_0 to a moderate value. 0.5 is used in our implementation. Then, after each packet is sent, S decreases α_0 by a small amount, for example, 0.002. If a packet arrives at D with the *contention* bit unset, no action is required at D. Otherwise, D informs S to increase α_0 by sending the value $(a + 0.1)$ in an *α-update*, where a is the α_0 value of the packet that has just arrived with the contention bit set. Upon receiving an α-update, S changes its α_0 value accordingly. The α-updates can be piggybacked to other packets from D to S, for example, TCP ACKs or the data stream $D \rightarrow S$ if the communication is two-way, such as in a voice call. In the worst case, separate α-update packets need to be sent from D to S.

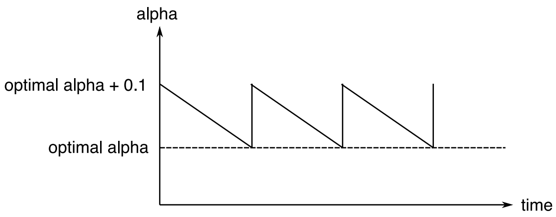

Fig. 7. Change of α value over time in a static network

Over a period of time, in a static network, the α_0 value varies as shown in Figure 7. One α-update packet is needed for roughly every $0.1/0.002 = 50$ data packets, so in the worst case, SMF adds about 2% to the network load in terms of the number of packets sent. The average α_0 of all data packets is $(\textit{optimal}\ \alpha_0 + 0.05)$.

In a dynamic network, the optimal α_0 value changes over time. Suppose the optimal α_0 suddenly increases from a to $a+1$. S sends the next data packet with $\alpha_0 = a$, which arrives at D with the contention bit set. D replies with an α-update containing the value $(a+0.1)$. The next data packet leaving S has an α_0 of $(a+0.1)$, and it arrives at D with the contention bit set. The process repeats and the outgoing α_0 increases by 0.1 every round-trip time (RTT). The new optimal α value is reached in $1/0.1 = 10$ RTTs.

Now let us suppose the optimal α_0 suddenly decreases from a to $a - 1$. S decreases α_0 by 0.002 for each data packet sent and never receives any α-update. The new optimal α_0 is reached after $1/0.002 = 500$ data packets have been sent. In either situation, SMF finds the new optimal α_0 in a reasonable amount of time, even after a drastic change in the network topology that shifts the optimal α_0 by 1.

B. Contention Detection

The intermediate nodes are responsible for setting the *contention* bit of a packet if the desired disjointness condition is violated. For example, to maintain node-disjoint paths, each intermediate node caches the $(src, dest, \alpha)$ tuple of recently forwarded packets. If an incoming packet matches the source and destination of a previous packet, but the signs of α are opposite, then a contention has been detected. Link-disjoint paths can be maintained similarly.

Although node-disjoint paths and link-disjoint paths are the most commonly used, neither is contention-free at the MAC layer, assuming IEEE 802.11 is used. Our simulation shows that even node-disjoint paths, the stricter of the two, fail to deliver near-optimal performance in SMF. For this reason, in this work we introduce an even stricter requirement, *range-disjoint paths*. Range-disjoint paths are paths that can be used simultaneously at the physical and link layers, except in the transmission ranges of the source and of the destination.[2]

We detect violations of range-disjointness in a similar way to how we detect violations of node-disjointness. However, every node now listens in promiscuous mode and caches the $(src, dest, \alpha)$ tuple of every recently forwarded and overheard packet. Two packets with the same source and destination but opposite signs of α indicate contention, unless the intermediate node is within the transmission range of the source or of the destination. It is easy to show that this method is consistent with the range-disjoint condition defined on IEEE 802.11 MAC layer.

IV. Performance Evaluation

A. Simulation Environment

In this work, we evaluate the empirical performance of SMF by simulation using the GloMoSim simulator (version 2.02). We compare the performance of the bare GPSR protocol against GPSR with the SMF extension.

A static network is simulated in this work due to certain abnormalities of the GPSR protocol encountered in mobile networks, which are documented briefly at the end of this section. Our simulation terrain consists of 100 nodes with three pairs of communicating nodes and a total of six Constant Bit-Rate (CBR) data streams. Each simulation is repeated five times with different random seeds and each run lasts five minutes of simulation time. The delay between two packets are adjusted and the delivery ratio is plotted against the delay between packets.

B. Simulation Result

The summary of our simulation results are presented in Figures 8 and 9. In Figure 8, we manually set the value of α in order to observe the effect of different α on the delivery ratio. We use the same α value for all the data streams. When α is set to zero, the protocol is equivalent to GPSR. As we increase the α value up to 0.8, we observe a boost in the delivery ratio. Further increase in the α value has a negative impact on the performance as the paths deviate further and further from the shortest path. Note that the optimal α value is highly dependent on the simulation scenario and it is therefore difficult to generalize our findings here.

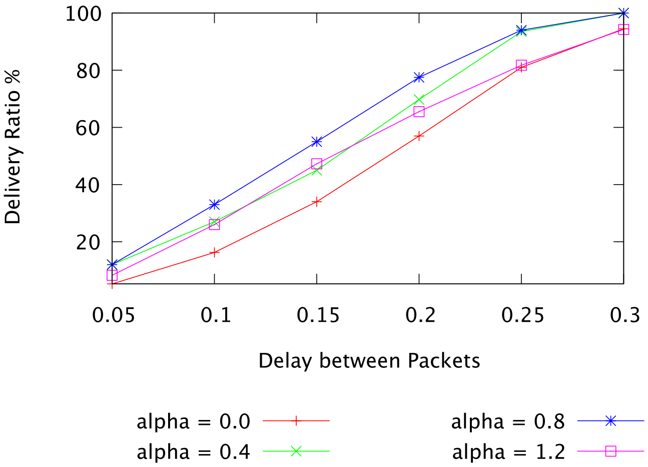

Fig. 8. Performance of SMF with fixed α values

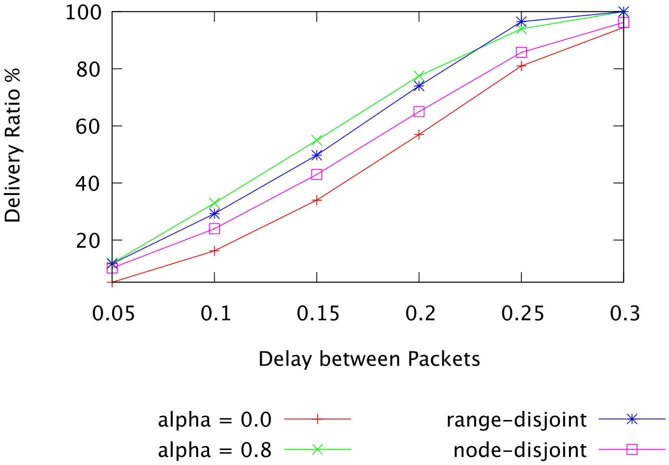

Fig. 9. Performance of SMF with automatic α values

In Figure 9 we turn on the automatic tuning of α value and compare the performance with that of bare GPSR and GPSR/SMF with a fixed α value. The α's of each data stream are now independent from each other. We observe that both range-disjoint paths and node-disjoint paths offer a better performance than bare GPSR ($\alpha = 0$), and the performance of range-disjoint paths is comparable to that of $\alpha = 0.8$, the best performance we obtained from trying different fixed values of α. This demonstrates that our tuning algorithm is able to deliver

[2] It is impossible for two nodes to communicate with the source or with the destination simultaneously, therefore we make this exception so that range-disjoint paths are possible.

near-optimal performance without any hints about the application scenario.

C. Abnormalities of GPSR

One of the theoretical strengths of stateless location-based routing protocols is the efficiency in networks with rapidly changing topology. However, while simulating GPSR, we encountered a few abnormalities in dynamic networks which result in temporary routing loops. The problem interferes with the contention detection mechanism and we are forced to use a static network instead. These abnormalities are briefly documented here.

Although the GPSR protocol is shown to be free of routing loops, certain assumptions of the protocol are not realistic in practice. The most well-known one is likely the *unit-disk* assumption, which asserts that the transmission range is the same for all nodes and in all directions. The reality is shown to be very different [7]. Nevertheless, the simulation environment that we use observes this assumption.[3]

The family of abnormalities that we encountered while simulating the bare GPSR protocol relates to the mobility of nodes. GPSR assumes that the network is static during the transmission of a packet, because the duration of the latter is short compared to the frequency of topology changes. While this assumption is reasonable in most cases, there are at least two scenarios where the probability of incorrect routing is non-negligible. The two scenarios are documented below.

a) Boundary Traversal: When perimeter routing starts, GPSR records the first hop traversed in the packet header. If the graph is disconnected, the packet will traverse the boundary of the entire connected subgraph of the network and eventually traverse the recorded link again. GPSR detects the second traversal and correctly discards the packet.

However, if the network is reasonably large, the time between the two visits of the link can be relatively long. If the link is broken or if it is no longer on the boundary of the connected subgraph, GPSR will not be able properly discard the packet, leaving the packet in the network until its Time To Live (TTL) expires.

b) Inconsistent Planarization: Face routing requires the connectivity graph to be planar. Since connectivity graphs are often not planar, GPSR needs to planarize the graph in face routing mode. On the other hand, in GPSR location updates are delivered without guarantee, typically by IEEE 802.11 broadcast. Therefore, different nodes often know slightly different locations of other nodes due to lost location updates. The inconsistency in itself is not particularly harmful, but it could interact with GPSR's planarization algorithm in an undesirable way.

An instance of the problem is depicted in Figure 10. Node A knows a slightly different location of Node B from Nodes B and C. With the right relative positions, this small difference could cause the edge AC to be pruned during planarization from A's point of view (shown on the left) but not from B's and C's point of view (shown on the right). Under the right-hand rule of face routing, when an incoming packet reaches A, A forwards it to B (A should have forwarded the packet to C had the edge AC not be pruned), which in turn forwards it to C and then back to A, creating a routing loop $A \to B \to C \to A \to \cdots$. Once a packet has entered the routing loop, a correctly received location update will not free it from the loop. Again, the packet is only dropped after its Time To Live expires.

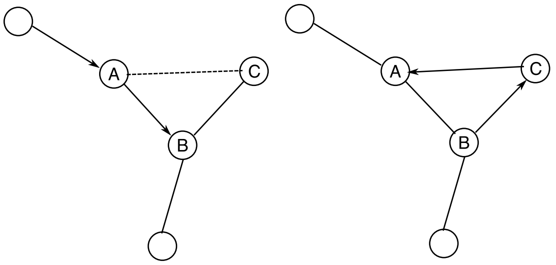

Fig. 10. Inconsistent Planarization

The abnormalities documented above cause prolonged existence of certain packets in the network. This interferes with our contention detection mechanism, causing unnecessary fluctuationsn of the α value. As such, we are forced to use a static network in our evaluation. Given the stateless nature of the protocols concerned, static networks should also give us a reasonable assessment.

V. Security-related Application

SMF provides a mechanism to influence the path chosen by location-based routing protocols in a non-intrusive manner. While this paper focuses on its application as a multipath extension, SMF can be applicable in other situations where such capability is beneficial. In this section, we demonstrate briefly how SMF could help in securing location-based routing protocols.

[3] More specifically, the assumption is valid in GloMoSim in *physical coordinates*, but not necessarily valid in *logical coordinates*. For this reason, SMF does physical to logical mapping only for GPSR greedy-mode packets. GPSR face routing still runs in physical coordinates.

When the sender knows or suspects that malicious nodes are present on a route, it can steer its traffic away from these nodes by using a different α value. In particular, if the source fails to receive a legitimate acknowledgment from the destination within a certain time period, it can use SMF to resend the packet along a different route. The sender can try different α values until one is found that avoids the malicious node. This is shown in Figure 11, where node 7 is malicious. Note that the sender need not, and most likely does not, know exactly which node is malicious to use this technique.

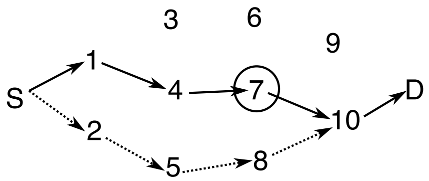

Fig. 11. Routing around malicious node 7

The stateless nature of location-based routing protocols, together with SMF, provide substantial security benefits. Assuming an end-to-end security mechanism is in place to provide confidentiality and integrity, the main responsibility of a secure routing protocol is then availability. Consequently, the main attack against ad hoc routing protocols is the Denial-of-Service (DoS) attack. The authors of Ariadne [12] noted that "attacks on an ad hoc network routing protocols generally fall into one of two categories: *routing disruption* attacks and *resource consumption* attacks. In a routing disruption attack, the attacker attempts to cause legitimate data packets to be routed in dysfunctional ways. In a resource consumption attack, the attacker injects packets into the network in an attempt to consume node resources such as memory (storage) or computation power."

In a stateless location-based ad hoc network, the effect of any routing disruption attack is limited to the malicious node's transmission range due to the absence of routing messages. Non-neighboring nodes can usually avoid the affected region by using suitable α values, provided that alternative routes exist. Therefore, location-based ad hoc networks utilizing the SMF extension can be largely immune to routing disruption attack from non-neighboring nodes.

Regarding resource consumption attacks, [12] further noted that "we require the ratio between the total work performed by nodes in the network and the work performed by the attacker is on the order of the number of nodes in the network." There are no broadcast messages in stateless location-based ad hoc networks, and each data packet is transmitted at most TTL times. We therefore conclude that resource consumption attack is infeasible in such networks.

We have demonstrated that stateless location-based ad hoc network with SMF extension can be largely immune to both types of DoS attacks launched from non-neighboring nodes. As the IEEE 802.11 MAC layer itself is vulnerable to DoS attacks from neighboring nodes, no secure routing protocol can do better in defending against DoS attacks by protecting against malicious neighbors. Although we cannot claim the best possible security, we believe that SMF coupled with proper end-to-end security such as IPSec can provide enough security for most civilian use-cases.

VI. Future Work

The current SMF parameter tuning mechanism does not explicitly monitor the impact of increasing α on the hop-count. Ideally we want to set an upper limit on the hop-count relative to that of the shortest path. The α value is not allowed to further increase when this limit is reached, therefore it is guaranteed only "good" paths are ever used.

The contention detection mechanism can be extended to consider the contention between unrelated data streams, making the protocol avoid congested areas in the network. In other words, we can optimize the α values globally. Devising a completely distributed algorithm for such optimization that converges fast in changing topology can be a significant challenge.

It is yet unclear how well SMF performs in sparse networks and in networks with obstacles. In these situations, SMF may not be as effective as conventional multipath protocols in discovering certain routes, such as the ones that traverse between obstacles. Further simulations and/or mathematical analysis are needed.

VII. Conclusion

The Skewed Map Forwarding (SMF) protocol is a generic extension to location-based ad hoc routing protocols that enforces disjointness requirements and preserves the stateless property of location-based protocols. It gives us flexible control over the path chosen by the location-based routing protocol without modifying the routing protocol itself. We also devise a method to automatically tune the parameter, α, used by SMF and demonstrate through simulation that the tuning algorithm is able to find near-optimal values of α.

REFERENCES

[1] Jinyang Li, John Jannotti, Douglas S. J. De Couto, David R. Karger, and Robert Morris, *A Scalable Location Service for Geographic Ad Hoc Routing*, Proc. 6th Annual International Conference on Mobile Computing and Networking, August 2000.

[2] Sylvia Ratnasamy, Brad Karp, Scott Shenker, Deborah Estrin, Ramesh Govindan, Li Yin, and Fang Yu, *Data-centric storage in sensornets with GHT, a geographic hash table*, Mobile Networks and Applications, Volume 8 Issue 4, August 2003

[3] Brad Karp and H. T. Kung, *GPSR: Greedy Perimeter Stateless Routing for Wireless Networks*, Proc. ACM MOBICOM, 2000.

[4] Fabian Kuhn, Roger Wattenhofer, and Aaron Zollinger, *Worst-Case Optimal and Average-Case Efficient Geometric Ad-Hoc Routing*, Proc. 4th ACM International Symposium on Mobile Ad hoc Networking & Computing, 2003.

[5] Fabian Kuhn et al., *Geometric Ad-Hoc Routing: Of Theory and Practice*, Proc. 22nd ACM Symposium on Principles of Distributed Computing, 2003.

[6] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal, *Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges*, M.C. Calzarossa and E. Gelenbe (Eds.): MASCOTS 2003, LNCS 2965, pp. 209-234, 2004. Springer-Verlag Berlin Heidelberg 2004.

[7] David Kotz, Calvin Newport and Chip Elliott, *The mistaken axioms of wireless-network research*, Dartmouth College Computer Science Technical Report TR2003-467, July 2003

[8] Fabian Kuhn, Roger Wattenhofer and Aaron Zollinger, *Asymptotically Optimal Geometric Mobile Ad-Hoc Routing*, Proc. 6th international workshop on discrete algorithms and methods for mobile computing and communications, September 2002.

[9] Sung-Ju Lee and Mario Gerla, *Split Multipath Routing with Maximally Disjoint Paths in Ad hoc Networks*, Proc. IEEE ICC, 2001.

[10] C. Perkins, E. Royer, and S. Das. *Ad hoc on demand distance vector (aodv) routing*, IETF Draft, January 2002.

[11] D.B. Johnson and D.A. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, in Mobile Computing, T. Imielinski and H. Korth, eds., Kluwer Academic Publishers, 1996, pp. 153-181.

[12] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, *Ariadne, A Secure On-Demand Routing Protocol for Ad Hoc Networks*, pages 21-38, Wireless Networks. Springer Science.