Efficient Routing Protocols for a Free Space Optical Sensor Network

Unoma Ndili Okorafor and Deepa Kundur
Department of Electrical Engineering
Texas A & M University, College Station, Texas 77840-0250
Email: unondili, deepa@ee.tamu.edu

Abstract— **For very low power, high bandwidth applications, free space optical sensor networks (FSOSN) have shown potential. They promise increasing node functionality, lower energy consumption, lower cost and smaller sizes. However, the new optical communication architecture yields new routing challenges. The objective of our paper is to introduce novel routing protocols for FSOSN that take into account the line-of-sight requirement for optical communications. Our network is modeled as a directed hierarchical random sector geometric graph, in which sensors route their data via multi-hop paths, to a powerful base station, through a cluster head. Following the dominant communication pattern in sensor networks, we propose a new efficient routing algorithm for local neighborhood discovery and a base station (up-link and down-link) discovery algorithm. We show that our routing protocols require $O\log(n)$ storage at each node, versus $O(n)$ seen in the literature, and present analytical and simulation results to evaluate the proposed protocols.**

I. Introduction

Recently, there has been increased interested in the development of sensor nodes that can communicate via free space optics (FSO) [1], [2], [3], [4]; FSO refers to the transmission of modulated visible or infrared (IR) beams through the atmosphere to obtain broadband communications over distances of several kilometers. The main limitation of FSO is the requirement that a direct line-of-sight path exist between a sender and a receiver. However FSO networks offer several unique advantages over RF networks. These include the fact that FSO avoids interference with existing RF communications infrastructure [5], is cheaply deployed since there is no government licensing of scarce spectrum required, is not susceptible to "jamming" attacks, and provides a convenient bridge between the sensor network and the nearest optical fiber [4]. In addition, "well-designed" FSO systems are eye-safe, consumes less power and yields smaller sized nodes because a simple baseband analog and digital circuitry is required, in contrast to RF communication [1]. More importantly, FSO networks enable high bandwidth bursty traffic which makes it possible to support multimedia sensor networks [4]. We term sensor networks that use FSO communication as free space optical sensor networks (FSOSN).

An added advantage of a FSOSN is that a device called corner-cube retroreflector (CCR) makes passive communication of nodes to and from the base station (BS) possible and energy efficient [1]. Here, the BS periodically sends interrogating beams of light to the entire network. Any node whose random orientation is such that it shares a direct line-of-sight path with the BS can establish bi-directional communication with the BS using its CCR. All up-link communication with the BS occurs in this manner. We will assume that with probability p_c, a node will be oriented such that it can communicate with the BS. In our routing algorithm, such nodes are compulsorily designated as Cluster Heads (CHs). The energy required for this communication to the BS by the CH is negligible, therefore does not adversely deplete the nodes energy resources. All other nodes in the network identify the CH closest to them, and route data to the BS via their CHs.

This communication model presents interesting advantages, as well as a new set of routing challenges. Our aim in this paper is to investigate novel routing algorithms for FSOSN.

0-7803-9466-6/05/$20.00 ©2005 IEEE MASS 2005 Workshop - RPMSN05

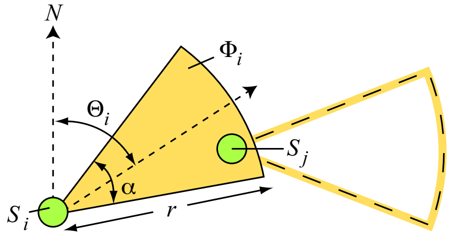

Fig. 1. Node S_j can only hear node S_i if it falls into S_i's communication section.

II. Network Setup

Consider a FSOSN in which n nodes labeled as $S_i : i = 1, 2, \cdots n$, are randomly deployed in a unit area of say 1-m $\times$ 1-m. All nodes are equipped with an optical trans-receiver consisting of photo-detectors and a semi-conductor laser (e.g. eye-safe 1550 nm wavelength laser), which have a given communication range $r(n)$. Each node S_i has a random position (x_i, y_i) and random directional orientation Θ_i, and can orient its transmitting laser to cover a contiguous scanning area $\frac{-\alpha}{2} + \Theta_i \leq \Phi_i \leq \frac{+\alpha}{2} + \Theta_i$. Following the model in [1] and as depicted in Figure 1, each node S_i can send data over a randomly oriented sector Φ_i of α degrees, for a fixed angle $0 < \alpha < 2\pi$. A typical value of α is $\frac{2\pi}{9}$. The receiving photo-detector is omni-directional and can thus receive data from any direction, so that the sensing region of the node is not limited to its communication sector. For a node S_j to receive data from node S_i, we must have that

$$d(S_i, S_j) \leq r(n) \quad \text{and} \quad (x_j, y_j) \in \Phi_i$$

where $d(S_i, S_j)$ is the Euclidean distance between S_i and S_j. In this setup, S_i may directly talk to S_j (denoted as $S_i \rightarrow S_j$); however, S_j can only talk to S_i via a multi-hop backchannel or reverse route, with other nodes in the network acting as routers. This creates a network topology that can be modeled as a directed random scaled sector graph [5]. We assume that all nodes know their approximate coordinates and avoid message collisions, after running the localization and synchronization algorithms introduced in [5]. We define a node S_i's forward neighborhood $FNeb(S_i)$ as the set of all nodes that S_i can talk to, so that $FNeb(S_i) = \{S_k\}, \forall k$ such that $(x_k, y_k) \in \Phi_i$ and $d(S_i, S_k) \leq r(n)$. The nodes in $FNeb(S_i)$

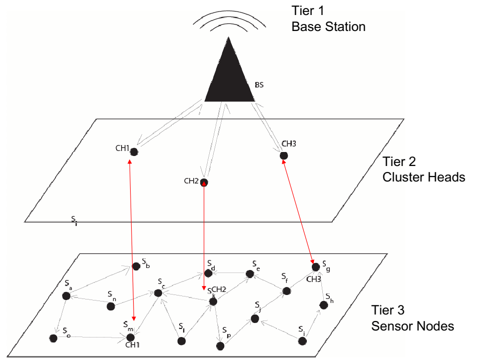

Fig. 2. Hierarchical network structure for the FSOSN based on node function specialization.

are called S_i's successors. Similarly, backward neighborhood $BNeb(S_i) := \{S_h\}, \forall h$ such that $(x_i, y_i) \in \Phi_h$ and $d(S_i, S_h) \leq r(n)$. Such nodes are called S_i's predecessors. Unlike in [5] where the angle of the laser for each node is fixed after the network initialization, we assume that nodes may broadcast packets at any time to their $FNeb$ by scanning over their Φ, or that nodes can send data to any one of its successors by appropriately orienting its laser towards that neighbor. In other words, we do not fix the angle of the laser for the life of the network. Due o the almost negligible energy dissipation of CCR technology, it enhances the survivability of the network, and yields a natural three-tier hierarchical communication structure for better scalability [6]. Figure 2 depicts this structure. The BS as the highest tier, has "unlimited" power resources, and securely routes data to a wired infrastructure. The CHs form the second tier while the regular nodes are at the third layer. S_i^* denotes that node S_i is a CH.

The communication model for the FSOSN requires the initial discovery of a nodes' local neighborhood, as well as a down-link channel, a one-way channel from the base station to the node, and an up-link channel from each node back to the base station. The down-link is necessary to ensure that the base station can broadcast requests through out the network structure, and sensor nodes may send readings to the BS via the up-link channel. The main contribution of this paper is to introduce two novel routing algorithms in FSOSN: The neighborhood discovery algorithm (NDA) is used for local neighborhood discovery and maintenance, while the base station discovery algorithm (BDA) handles up-link and down-link channels discovery.

III. Literature review

Current routing protocols based on Link State, Distance Vectors, Path Vectors or Source Routing differ from routing in FSOSNs in one or two significant ways. First, they assume that a fraction of links are bidirectional. This is not true in a FSO network in which all links are unidirectional. Second, many current protocols are designed for ad hoc networks in which the routing protocol is designed to support multi-hop communication between any pair of nodes. As pointed out in [7], the goal of a sensor network is to route sensor readings to the base station. Therefore, the dominant traffic patterns are different from those found in an ad hoc network. In a sensor network, we are dealing mostly with nodes-to-base station, base station-to-nodes, and local neighborhood communication.

Recent studies have considered the effect of unidirectional links [8], and report that as many as 5% to 10% of links in wireless ad hoc networks are uni-directional [9] due to various factors. Routing protocols such as DSDV and AODV which use a reverse path technique implicitly ignore such unidirectional links, and are therefore not relevant in this scenario. Other protocols such as DSR [10], ZRP [11] or SRL [12] have been designed or modified to accommodate unidirectionality, by detecting unidirectional links, and then providing a bi-directional abstraction for such links [13], [14], [15], [16]. The simplest and most efficient solution proposed for dealing with unidirectionality is Tunneling [17], in which bi-directionality is emulated for a uni-directional link by using bi-directional links on a reverse backchannel to establish the tunnel. Tunneling also prevents implosion of acknowledgement packets and looping by simply repressing link layer acknowledgments for tunneled packets received on a unidirectional link. Tunneling however works well in a mostly bi-directional network with few unidirectional links [8].

In the FSOSN, nodes use a directional transmitters with omni-directional receivers, hence all the links in the network are uni-directional. Due to the differences cited above, current approaches for dealing with uni-directionality are not applicable. Also, according to Ernst and Dabbous [8], modifying existing routing protocols to deal with FSOSN is not desirable. A better idea involves designing from scratch, a routing protocol for the unique applications in a FSOSN.

A similar bottom-up from-scratch approach for routing in purely unidirectional ad hoc networks has been considered in [8], [18] and [19]. The aim in an ad hoc network is to discover circuits for all pairs of nodes. A circuit is defined as a sequence of unidirectional links leading away from one node and back to the same node. The protocols strive to perform circuit discovery by assuming that the network is strongly connected and there is at least one circuit between every pair of nodes. In [8], Ernst and Dabbous discuss circuit discovery, validation, integration and deletion of links. Huang *et al.* [19] present algorithms for a single circuit discovery to each destination, based on distance-vector-based Routing Information Protocol (RIP). Each node in the network has a FROM and TO table each of $O(n)$. Lou and Wu [18] extend this RIP idea by storing a circuit to a given destination through each outgoing link. These protocols differ from our approach because they all assume the communication model of an ad hoc network.

We propose a NDA that is similar to [18], [19] in the sense that we also attempt to discover one most efficient circuit from a node through each of its successors. However, our aim is to discover our local neighborhood. Therefore the destination of each circuit is the originating node itself. That is, if node S_i has M neighbors, we expect to discover M circuits which represent the best M different routes from S_i back to itself. These circuits also represent the best routes for each of the nodes along that circuit, through its successor on that circuit.

The BDA enables a node discover its up- and down-link paths to the BS. A similar up-link and down-link protocol [5], [20] proposed two algorithms: simple-bro (for down-link broadcasting) and simple-link (for up-link communication). The simple-bro is first performed to enable nodes determine what level they are from the base station, where CHs are at level 0, communicating neighbors of CHs are at level 1, and so on. This protocol terminates after a given number of rounds, such that with high probability all nodes in the network have determined their level. After this, the simple-link protocol is performed using the broadcast channel discovered by simple-bro. The important difference between our approach and [20] is that in our case, the orientation of the laser is not fixed once a neighbor is discovered. For our algorithms, we urge the reader to keep in view the differences between routing algorithms for ad hoc networks and those for the FSOSN scenario.

- The definition of connectivity in FSOSN differs from that of ad hoc networks in which each node must be able to send and receive to every other node in the network. For FSOSN, connectivity is the ability of every node to send and receive data from the BS.
- The BS acts as a relay for data so that any two nodes can communicate via the base station. Due to this, we can accommodate disconnected clusters as long as the clusters are connected within themselves and to the BS.
- We aim to generate in each node a routing table containing the most efficient circuits for its $FNeb$ (NDA) as well as to and from the BS (BDA). Routing tables stored at each node is $O(\log n)$ versus $O(n)$ in the literature [19]. The routing table at the BS is $O(n^2)$.

IV. Neighborhood Discovery Algorithm

The NDA is specifically adapted for routing in sensor networks with uni-directional links. The philosophy in the design of NDA considers the difference in communication pattern between ad hoc networks (in which routing is typically flat, and between any two nodes) and optical sensor networks with a (naturally-occurring) hierarchy in which most traffic is from sensors-to-base station and/or base station-to-sensors, using a local neighborhood. Apart from nodes sending reading to the BS, local neighbors may wish to exchange keys for secure link communication or perform local data aggregation. The NDA helps these types of local communication, as well as enables BDA.

NDA enables a node to discover its $FNeb$, and a circuit back to itself via all its successors. Because NDA is performed locally, the information storage for each node is $O(\log n)$. This is because as shown in [21], [5], to guarantee network connectivity, each node should have $O(\log n)$ neighbors. The pseudo code for NDA is detailed in Algorithm 1. Initially, the neighborhood routing tables (NRT) of all nodes are empty. After the NDA, each node is able to extract an NRT circuit entry for each of its successor. The format of an entry in the NRT for node S_i is $\{S_j, S_h, h_{jh}\}$ where $S_j \in FNeb(S_i); S_h \in BNeb(S_i)$; and h_{jh} is the number of hops for this circuit.

Algorithm 1: NDA(k, n)

```
while r_k < r_z
for i = 1 : n
  for all S_x ∈ BNeb(S_i)
  if S_i receives HELLO from S_x
  S_i checks for its ID in HELLO(S_x)
  S_i ∈ HELLO(S_x) implies RP found!
  break
    else S_i checks for loop in HELLO(S_x)
  If loop exists in HELLO(S_x)
  break
  if ( S_i is in BM )
  extracts new information from HELLO(S_x)
  HELLO(S_i) = HELLO(S_x) − HELLO(S_i)
  S_i → FNeb( S_i ) : HELLO(S_i)
  S_i → successor( S_i ) :
  RP found via successor
k = k + 1
```

The NDA uses flooding to advertise links to successors. NDA is run in z rounds, where each round r_k for $k = 1 \cdots z$, lasts a given fixed time interval. In any given round, a node may be in a broadcast mode (BM) with probability p_{bm}. Every node that is not in BM just listens. Note that a node may simultaneously broadcast and receive messages in the same round since the optical transmit and receive hardware are decoupled. The random time schedule optimizes NDA and minimizes network congestion and bandwidth usage.

In a round, nodes in BM send HELLO messages. The format of a HELLO message from S_i is

$$S_i : \{|S_h|_{BM}(_1|S_g|_{BM}(_2|S_f|_{BM}(_3\cdots(_{d\ldots}))))\}$$

where $|S_h|_{BM}$ is the set of nodes in $FNeb(S_i)$ such that S_j is in BM. $|S_g|_{BM}$ is the set of nodes in BM in $FNeb(S_h)$, and so on. This HELLO message represents a tree of depth d, rooted at S_i, and each path from a leaf to the node represents that leaf nodes circuit to the root node. Figure 3(a) shows this tree representation.

Note that in the first round, all HELLO messages contain only the ID of the sending node. In a round,

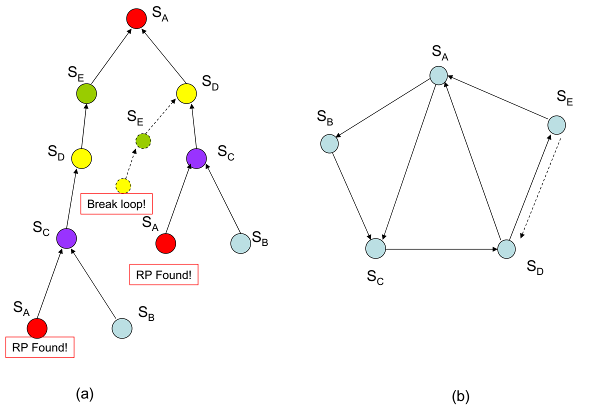

Fig. 3. (a) Circuits found by NDA for S_A for network configuration. (b) Example of a simple network.

TABLE I

S_A'S HELLO MESSAGES IN THE VARIOUS ROUNDS FOR THE SAMPLE NETWORK OF FIGURE 3

Round #	S_A's Hello Message
1	S_A:
2	$S_A : (S_D, S_E)$
3	$S_A : (S_D(S_C), S_E(S_D))$
4	$S_A : (S_D(S_C(S_B, S{*}_A)), S_E(S_D(S_C)))$
5	$S_A : (S_D(S_C(S_B(S{*}_A), S{*}_A)), \cdots$
	$...S_E(S_D(S_C(S_B(S{*}_A), S{*}_A))))$

receiving nodes append all $P_{BM}.\log n$ IDs from the previous round to their own HELLO message, where P_{BM} is the probability that a node is in BM. As the index of the current round increases, the size of the HELLO message increases so that in round r_k the message size is $(P_{BM}.\log n + 1)^k$.

It has been shown that in a FSOSN, a non-boundary node will almost surely find a circuit within a finite number of hops [22]. We denote the expected number of hops for a circuit in the network as h_c. The number of rounds for the NDA to converge is bounded by $h_c/P_{BM} + \Delta$, where Δ is a constant to take care of boundary nodes. We will call this value r_z, and terminate NDA in this round. Reverse routes that have not been found by r_z are discarded as too long. Experiments have shown h_c to be about 4 hops[22]. The maximum size of a HELLO message is $(1 + h_c)\log_2 n$ for n nodes in the network.

In the NDA, at each round, each node checks to see if there is a previous entry for a node. If this is the case, it compares the number of hops for both paths. If the number of hops of a circuit from a successor in a HELLO message is less than an existing entry, we

TABLE II

S_A'S HELLO MESSAGES WITH ONLY NEW INFORMATION FROM PREVIOUS ROUND, TO REDUCE SIZE OF MESSAGE

Round #	S_A's Hello Message
1	S_A:
2	$S_A : (S_D, S_E)$
3	$S_A : (S_D(S_C), S_E(S_D))$
4	$S_A : (S_C(S_B, S{*}_A), S_D(S_C))$
5	$S_A : (S_B(S{*}_A))$

TABLE III

NEIGHBORHOOD ROUTING TABLES FOR ALL NODES IN THE NETWORK OF FIGURE 3

Node	$FNeb\&BNeb$	Circuits
S_A	$BNeb = (S_D, S_E)$ $FNeb = (S_B, S_C)$	$\{S_B, S_D, 4\}$ $\{S_C, S_D, 3\}$
S_B	$BNeb = (S_D, S_E)$ $FNeb = (S_B, S_C)$	$\{S_C, S_A, 4\}$
S_C	$BNeb = (S_D, S_E)$ $FNeb = (S_B, S_C)$	$\{S_D, S_B, 4\}$
S_D	$BNeb = (S_D, S_E)$ $FNeb = (S_B, S_C)$	$\{S_E, S_C, 4\}$ $\{S_A, S_C, 3\}$
S_E	$BNeb = (S_D)$ $FNeb = (S_A)$	$\{S_A, S_D, 4\}$

replace the circuit with the new path. Similarly, each individual circuit is inspected for repeated node IDs, to avoid loops. Once a node finds a its ID in a received HELLO message, it declares that a reverse path (RP) has been found and stops NDA for this circuit. Finally, it forwards this route to all the nodes on that circuit via the appropriate successor, to avoid further processing at those nodes.

We use an example to illustrate that the NDA converges to expected NRT. Consider the network in figure 3. For ease of analysis, we assume $P_{BM} = 1$, so all nodes broadcast in each round. The HELLO message for node S_A for each round is given in Table I. By the fifth round, S_A would have discovered the reverse routes $S_A \rightarrow S_B \rightarrow S_C \rightarrow S_D \rightarrow S_E$ and $S_A \rightarrow S_C \rightarrow S_D \rightarrow S_E$. One technique to reduce the size of messages is for nodes to only broadcast new information received in a previous round. In this case, the HELLO messages for S_A is given in Table II. For this simple network, after 5 rounds of NDA, the routing tables for all the nodes in the network is given in Table III.

Note that, even though S_A finds the circuit from successor S_B as $S_A \rightarrow S_B \rightarrow S_C \rightarrow S_D \rightarrow S_E \rightarrow S_A$ of 5 hops, it soon replaces this path with $S_A \rightarrow S_B \rightarrow S_C \rightarrow S_D \rightarrow S_A$ of 4 hops in NRT, since the second circuit has fewer hops. Also, consider a case in which the link DE is bidirectional as in figure 4 (depicted by

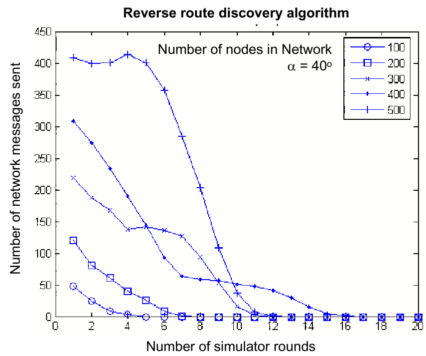

Fig. 4. Number of messages sent versus number of rounds for $p_{BM} = 0.7$.

the dotted arrows). The loop $S_D \rightarrow S_E \rightarrow S_D$ occurs in the circuits that use this link. However, this link is deleted from the `HELLO` messages once it is detected by node S_D. As in [17], we also prevent "ack implosion" by dis-enabling nodes from sending acknowledgement packets for routing/control packets.

Figure 4 shows one of our simulation scenario for the total number of messages sent in the network versus round number for $P_{BM} = 0.7$, for various values of n. We note that fewer messages are sent as the rounds increase. The number of messages sent tapers off to zero as most circuits are discovered in the first few rounds. For example, for a network of 500 nodes, by the 12^{th} round, the NDA has converged.

V. Base-Station Discovery Algorithm

While NDA deals with local neighborhood discovery using flat routing, BDA considers the efficient establishment and maintenance of hierarchical up-link and down-link routes to the BS. The main design consideration in BDA is secure route establishment to and from the base station. This is because it is known that security is difficult to achieve as an after thought in a protocol [7].

The BDA is a reactive routing protocol using localized packet multi-casting. It is similar to the NDA, except that it is initiated and terminated by the base station. In BDA, authenticated cluster route packets (CRP) originate and terminate at the BS. A CRP may leave the network via a different CH from the one from which it entered. Therefore, BDA implicitly takes advantage of the bi-directionality of links between CHs and the BS. For example, the network in Figure 5 shows a CRP which enters the network via node S_i^* and returns to the BS through S_d^* via the route $BS \rightarrow S_i^* \rightarrow S_a \rightarrow S_b \rightarrow S_c \rightarrow S_d^* \rightarrow BS$.

A node forwards a CRP to its $FNeb$ (now known from NDA), once it receives it. The CRP has a hops-traversed (HT) field in its header that counts the number of hops it has traversed. Each node upon receiving the CRP, increments HT by one, appends its ID to the CRP packet, and re-broadcast it to its own $FNeb$. The HT field ensures data freshness and prevents replay attacks. Once this CRP reaches any CH, if HT > 2, it terminates this route and forwards the CRP to the BS. If HT $= 2$, this means that two cluster heads are adjacent and no useful route has been discovered. The CRP is said to be expired if the HD field is greater than a given constant δ, and is consequently discarded. A node will likely process several CRPs from different CH's and neighbors.

Algorithm 1: BDA(CRP, HT)

$BS \rightarrow CH's$: (CRP Packet)
while $HT < \delta$
if $HT! = 0$: ignore request and discard packet
else $\{$append ID(CH) to CRP header
$CH \rightarrow FNeb(CH)$: (CRP Packet)

if $S_i \in \Phi_{(CH)}$ is a CH **and** $HT < 2$
$S_i$ignores request and discards packet
else if $S_i \in \Phi_{(CH)}$ is a CH **and** $2 < HT \leq \delta$
$\{$append ID(S_i) to CRP header
$S_i \rightarrow BS$: (CRP Packet)
else if $S_i \in \Phi_{(CH)}$, not a CH **and** $2 < HT \leq \delta$
$\{$append ID(CH) to CRP header
$S_i \rightarrow FNeb(S_i)$: (CRP Packet)

$HT = HT + 1;$
end

When a CRP returns to the BS, the BS extracts routing information from this packet and makes entries into the base stations' $(n \times n)$ routing table (BSRT). It then forwards the routing entry to the nodes on this route through their entry cluster head. For example, the CRP in figure 5 generates the entry for the BSRT shown in table IV. This routing information is passed on to all nodes in this route via S_i^*, so that S_i, S_a, S_b, S_c and S_d now know their up-link and down-link paths.

After the BDA, the BS is able to construct a complete BSRT reflecting the topology of the network. The BS uses this routing table to send individual, broadcast or cluster requests to nodes in the network. The BSRT is also useful in constructing and informing affected nodes of alternative paths to a destination, for route maintenance in the case of link failure. Also, for scalability the BSRT is useful in the authentic introduction and hand shaking for new nodes to the network. Note that memory

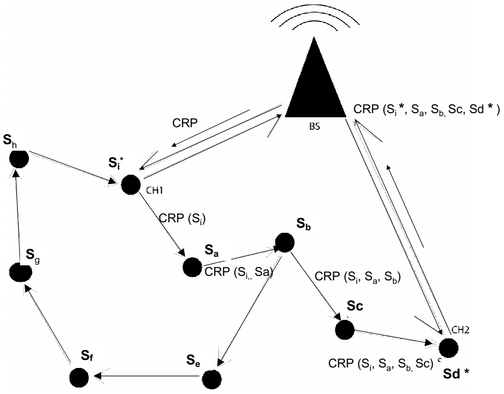

Fig. 5. Example of a BDA cluster routing configuration.

TABLE IV
ENTRY TO THE BSRT FOR THE CRP OF FIGURE 5

F/T	S_a	S_b	S_c	S_d^*	S_e	S_f	S_g	S_h	S_i^*
S_a		1							
S_b			1						
S_c				1					
S_d^*									
S_e									
S_f									
S_g									
S_h									
S_i^*	1								

for the BSRT is not considered, since BSRT is sparse and the BS is assumed to have unconstrained resources.

VI. CONNECTIVITY ANALYSIS IN FSOSN

It has been shown that for $r(n) \geq \sqrt{c(n)\log(n)/n}$ and for a sufficiently large constant $c(n)$, the probability that an ad hoc network is connected approaches 1, as n grows [23]. This result assumes a circular omnidirectional communication area. We proffer a general result for random sector graphs, that accounts for α, where $0 < \alpha \leq 2\pi$.

Theorem 6.1: For $r(n,\alpha) \geq \sqrt{\frac{k(n,\alpha)\log(n)}{\alpha n}}$ and for a sufficiently large $k(n,\alpha)$, the probability that a random geometric graph is connected approaches 1, as n grows.

Proof: To guarantee asymptotic connectivity as n tends to ∞, the area of the communication sector $\frac{\alpha r(n,\alpha)^2}{2}$ should be proportional to the expected number of neighbors $\frac{c(n,\alpha)\log(n)}{n}$ [5], [21], [24]. The result follows for $k(n,\alpha) = 2\pi c(n,\alpha)$, and the case for $\alpha = 2\pi$ yields the known result for random disc graphs. ■

Our simulations reveal that $c(n,\alpha)$ is an important tuning parameter for optimal network connectivity, in which each node is connected to the optimal number of neighbors, in our case $\log(n)$ [21]. This value guarantees connectedness, while minimizing network bandwidth, by not overloading each node with too many neighbors. We experimentally derived optimal values of $c(n,\alpha)$ for various n and α, some of which are listed in Table VI.

TABLE V
TABLE SHOWING OPTIMAL C(N) FOR VARIOUS VALUES OF N AND α.

n	$\log(n)$	optimal c(n) $\alpha = 20^o$	$\alpha = 40^o$	$\alpha = 90^o$
50	3.9120	.8665	.6502	.4818
100	4.6052	0.7809	.4932	.4380
500	6.2146	0.4369	.4121	.3742
1000	6.9078	0.3956	.3694	.3498
2000	7.6009	0.3697	.3448	.3393
4000	8.2940	0.3540	.3436	.3333

It is known that a sparse network of BSs (in our case CHs) significantly improves connectivity [25]. Taking advantage of this, we define connectivity for FSOSN as the ability of every node to have at least one up-link and down-link path to the BS. In addition, the FSOSN is h-connected if within h hops any node can communicate with at least one CH in the network. This means that within at most $2h+1$ hops, a node can route data to any other node in the network by enlisting the help of the BS. This leads to our next theorem.

Theorem 6.2: If p_c is the probability that a node is a CH, the probability that the number of hops from any node to a CH is less than h approaches 1, as h grows.

Proof: Let H be the random variable counting the least number of hops from a node in the network to a cluster head. From probability theory, we know that $H \sim$ geometric(p), such that $P(H \leq h) = 1 - (1 - \frac{np_c}{n-h})^h$. We obtain the pdf as $P(H = h) = p(1 - \frac{np_c}{n-h})^{h-1}$ for $1 \leq h$; and the expected value of H is $\sum_{h=1}^{\infty} h.P(H = h)$. Using Markov inequality, we bound $P(H \geq h) = (1 - \frac{np_c}{n-h})^h \leq 2\exp^{\frac{-2h^2}{\log(n)}}$. It is trivial to show that as h grows, $P(H \geq h) \Rightarrow 1$. ■

Figure 6 graphs h for various p_c versus $h \cdot P(H = h)$. For example, when $p_c = 0.2$ expected number of hops from a node to a CH is 4.

VII. CONCLUSIONS AND FUTURE WORK

In this paper we have proposed novel neighborhood discovery and base station discovery routing algorithms for FSOSNs. In designing our algorithms, we considered the basic differences in communication pattern between ad hoc and sensor networks. We show that the information storage of routing tables at the nodes is $O\log(n)$. We presented analytical and simulation results to evaluate our algorithms. Preliminary discussion of our work is presented online at *http://opsenet.tamu.edu/*.

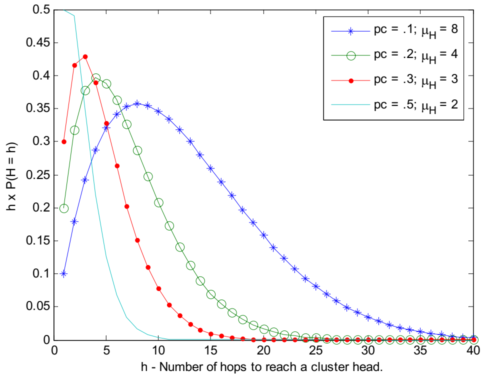

Fig. 6. Expected number of hops to reach a CH for various values of p_c.

References

[1] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for "smart dust"," in *Proc. ACM/IEEE International Conference on Mobile Computing and Networking*, Seattle, Washington, August 1999, pp. 271–278.

[2] B. A. Warneke, M. D. Scott, B. S. Leibowitz, L. Zhou, C. L. Bellew, J. A. Chediak, J. M. Kahn, B. E. Boser, and K. S. J. Pister, "An autonomous 16mm^3 solar-powered node for distributed wireless sensor networks," in *Proc. IEEE Sensors*, Orlando, Florida, January 2002, pp. 1510–1515.

[3] W. Mao and J. M. Kahn, "Free-space heterochronous imaging reception of multiple optical signals," *IEEE Transactions on Communications*, vol. 52, no. 2, pp. 269–279, February 2004.

[4] J. Llorca, A. Desai, U. Vishkin, C. Davis, and S. Milner, "Reconfigurable optical wireless sensor networks," in *Proc. SPIE vol. 5237, Optics in Atmospheric Propagation and Adaptive Systems VI*, J. D. Gonglewski and K. Stein, Eds., Barcelona, Spain, February 2004, pp. 136–146.

[5] J. Díaz, J. Petit, and M. Serna, "A random graph model for optical networks of sensors," *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, pp. 186–196, July-September 2003.

[6] M. Bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor networks," in *WiSe '03: Proceedings of the 2003 ACM workshop on Wireless security*, New York, NY, USA, 2003, pp. 79–87, ACM Press.

[7] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. IEEE International Workshop on Sensor Network Protocols and Applications*, May 2003, pp. 113–127.

[8] V. Ramasubramanian and D. Mosse, "A circuit-based approach for routing in unidirectional links networks.," in *INRIA Research Report 3292*, 1997.

[9] V. Ramasubramanian and D. Mosse, "Statistical analysis of connectivity in unidirectional ad hoc networks," in *International Workshop on Ad Hoc Networking (IWAHN).*, Vancouver, Canada,, 2002.

[10] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, Imielinski and Korth, Eds., vol. 353. Kluwer Academic Publishers, 1996.

[11] M. R. Pearlman Z. J. Haas and P. Samar, "The zone routing protocol (zrp) for ad hoc networks," in *Internet Draft - Mobile Ad Hoc NETworking (MANET) Working Group of the Internet Engineering Task Force (IETF)*, 2001.

[12] V. Ramasubramanian, R. Chandra, and D. Mosse, "Providing a bidirectional abstraction for unidirectional ad hoc networks," in *Proceedings of IEEE Infocom*, New York, NY, USA, 2002, pp. 1258–1267.

[13] L. Bao and J. J. Garcia-Luna-Aceves, "Link-state routing in networks with unidirectional links," in *In Proceedings of International Conference on Computer Communications and Networks (IC3N),*, Boston, Massachusetts, 1999, pp. 358–363.

[14] W. Dabbous, E. Duros, and T. Ernst, "Dynamic routing in networks with unidirectional links," in *WOSBIS'97*, Budapest, Hungary, October 1997, pp. 35–47.

[15] M. Marina and S. Das, "Routing performance in the presence of unidirectional links in multihop wireless networks," in *Proc. ACM MobiHoc.*, 2002, pp. 12–23.

[16] R. Prakash, "A routing algorithm for wireless ad hoc networks with unidirectional links," *Wireless Networks*, vol. 7, no. 6, pp. 617–625, 2001.

[17] S. Nesargi and R. Prakash, "A tunneling approach to routing with unidirectional links in mobile ad-hoc networks," in *In Proceedings Ninth International Conference on Computer Communications and Networks.*, 2000, pp. 522–7.

[18] W. Lou and J. Wu, "A multi-path routing protocol for unidirectional networks," in *Proc. of 2001 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'2001)*, 2001, pp. 2021–2027.

[19] H Huang, G.H. Chen, F.C.M. Lau, and L. Xie, "A distance-vector routing protocol for networks with unidirectional links," in *Computer Communications, Vol. 23, No. 4*, 2000.

[20] J. Díaz, J. Petit, and M. Serna, "Random scaled sector graphs," Tech. Rep. LSI-02-47-R, Department de Llenguatges i Sistemes Informàtics, Universitat Politècnica de Catalunya, Jordi Girona Salgado 1–3, Barcelona, 2002.

[21] F. Xue and P. R. Kumar, "The number of neighbors needed for connectivity of wireless networks," *Wireless Networks*, vol. 10, no. 2, pp. 169–181, 2004.

[22] J. Díaz, V. Sanwalani, M. Serna, and P. Spirakis, "The chromatic and clique numbers of random scaled sector graphs," Tech. Rep., Research report, 2004.

[23] M. D. Penrose, "On k-connectivity for a geometric random graph," *Random Struct. Algorithms*, vol. 15, no. 2, pp. 145–164, 1999.

[24] X. Liu and R. Srikant, "An information-theoretic view of connectivity in wireless sensor networks," in *The first IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, 2004.

[25] O. Dousse, P. Thiran, and M. Hasler, "Connectivity in ad-hoc and hybrid networks," in *IEEE INFOCOM*, 2002.