Security and Energy Considerations for Routing in Hierarchical Optical Sensor Networks

Unoma Ndili Okorafor, Kyle Marshall and Deepa Kundur
Department of Electrical & Computer Engineering
Texas A & M University, College Station, Texas 77843-3124
Email: {unondili, deepa}@ece.tamu.edu

Abstract— **In this paper we evaluate the energy and security consideration for a security-aware routing protocol proposed for uni-directional, hierarchical optical sensor network. We bootstrap the unconstrained resources of the base station to design GORA, a greedy optimized routing algorithm, in which the base station is responsible for network route optimization and updates. This paper extends our recent work on OPSENET, a novel and efficient protocol that facilitates secure routing in directional optical sensor networks. We evaluate security and energy metrics for our scheme proposed scheme. Analysis and simulation results are used to show the performance of our algorithm, compared with other hierarchical bi-directional clustering routing schemes.**

I. Introduction

Uni-directional optical wireless sensor networks (OSNs) that communicate using free space optics (FSO) with a directed sector of communication are of recent gaining more visibility due the the advantages that FSO yields over traditional omni-directional RF based techniques [1]–[4]. Notably, directional communication greatly improves communication efficiency and transmission energy of nodes, and yields security benefits in the routing and physical layers, thereby resulting in a highly desirable improvement to the lifetime and reliability of the sensor network. Additionally, OSNs realize ultra-high bandwidths which can benefit real-time multimedia and visual sensor network applications [5].

Directional communication has distinct characteristics and effects on security and routing in the network layer that warrant novel analysis and solutions. Efficient route setup in a purely uni-directional OSN requires that optimal (back channel) reverse routes for each forward link in the network be discovered. The random deployment of nodes (node positions and orientations are not known a priori), makes secure network discovery in OSNs challenging. In this paper, we consider the security and energy benefits of directional hierarchical clustering, which is inherent in our network model of the OSNs. We compare the performance of the OSN to conventional clustered sensor networks, in terms of security and energy.

A. Related Work

Traditionally, routing decisions in sensor networks are made by nodes themselves, based on some cost function such as minimum energy, order of received routing beacon [10], received signal strength, geographic distance [6] etc. This approach implicitly assumes the bi-directionality of network links in which reverse paths are used to build a minimum spanning routing tree, rooted at the base station. For example, in tinyOS routing [7] the base station floods beacons which yield reverse paths back to the base station. A node that hears the beacon marks the base station as its parent, and recursively rebroadcast the beacon. Nodes who do not have a parent node, and receive the beacon mark the sender as its parent. Data is routed to the base station when each node forwards its data to its parent. Many other routing schemes in sensor networks such as Directed Diffusion [8], Dynamic Source Routing [9], Minimum Cost Forwarding [10], and Geographic routing [6] also employ a similar reverse path approach. In an OSN, all network links are uni-directional, and reverse path routing cannot be leveraged.

Because of lack of bi-directionality, a node cannot discover other nodes in the network who can 'hear' or receive packets from it using simple passive or active listening. Without bi-directionality, link layer acknowledgements is also non-trivial. One approach to route discovery in this scenario involves using circuit paths [11], in which a node floods routing beacons which travel through circuits rooted at the node, gathering route data as it traverses the circuit. Once a given node's beacon returns, the node can tell from the sequence of node IDs, who can hear him. This technique of abstracting bi-directionality using the underlying unidirectional circuits is known as *tunneling* [12]. In [13], Ernst and Dabbous discuss circuit discovery, validation, integration and deletion of links. Huang et al. [11] present algorithms for a single circuit discovery to each destination, based on distance vector Routing Information Protocol, in which each node stores a *FROM* and *TO* table. Lou and Wu [14] extend this idea by storing a circuit to a given destination through each outgoing link.

B. Summary of Our Contribution

In this paper, we present a secure and efficient network discovery and routing scheme, under a hierarchical directional OSN model, in which some nodes in the network act as *cluster head* nodes. Cluster heads have a low-energy bi-directional link with the base station using *passive* optical communication. They are ordinary nodes which by virtue of their orientation (based on how they fall after random deployment), have bi-directional line-of-sight with the base station, and therefore act as gateways to the network. All other nodes in the network seek to discover and route data to the cluster heads (uplink).

1-4244-0507-6/06/$20.00 ©2006 IEEE

The base station also seeks to discover and route data to all nodes via cluster heads (downlink). Routing between nodes in the network employs *active* optical communication (lasers or LEDs), while cluster heads and the base station use passive communication [3].

We propose a novel secure routing philosophy which heavily leverages hierarchy and the all-powerful base station, by further pushing complexity and processing to the base station. In essence, we trade-off the inherent and unavoidable overhead of uni-directional routing with less processing at the nodes, to yield energy savings in the network. Furthermore, we exploit the directionality of links and the trusted base station to achieve tight security for route setup. The novelty of our work lies in exploiting network hierarchy and the base station's unconstrained resources to achieve efficient and secure network discovery and routing.

Our scheme entails centralized network discovery and optimized routing decisions handled by the base station as follows: The base station floods secure routing beacons into the network via the various gateways (i.e. cluster heads), which are uniformly distributed through the network. The beacons act as agents that traverse the network, gathering routing data as they propagate. Beacons are terminated when they reach a cluster head, which then forwards them back to the base station. The base station can authenticate returned beacons as well as per hop node information on the path (or base station circuit), using shared keys with the nodes, pre-deployed keying and one way key chains. Data gathered from the returned beacons is used to construct the optimized network topology, and hence, efficient uplink and down-link paths for each node.

In our recent work [15], [16], heuristics and algorithms for secure and efficient network discovery in the OSN were developed. Specifically, we developed OPSENET, a novel secure cluster-based routing protocol for base station circuit (BS-circuit) discovery. In this paper, we extend our work to consider security and energy issues for an efficient Greedy Optimization Routing Algorithm (GORA), anchored at the base station. GORA is fast, efficient and greedy, yielding sub-optimal (locally optimal) routing paths which we affirm is sufficient for our routing purposes, versus the complexity of globally optimal schemes. Our algorithm is similar to Dijkstra's [17] and other shortest path routing algorithms, with additional optimization constraints, namely; the routing tree originates and terminates at a given subset of nodes (the cluster heads), and traverse every network link once only.

The rest of our paper is organized as follows: In Section 2, we present preliminaries and network setup. Section 3 presents a review of the OPSENET routing protocol [15], while Section 4 details GORA. We present security and energy analysis in Section 5, and concluding remarks in Section 6.

II. Preliminaries, Network Setup and Assumptions

A. OSN Network Setup Preliminaries

Consider an OSN in which all nodes are equipped with an optical trans-receiver consisting of photo-detectors and a semiconductor laser with a given maximum communication range

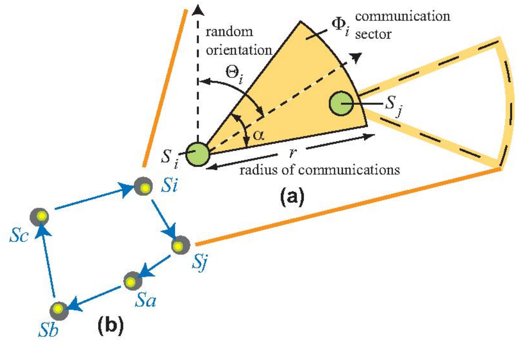

Fig. 1. Node S_j can only hear node S_i if it falls into S_i's communication section. However S_j talks to S_i via the back channel $S_j \rightarrow S_a \rightarrow S_b \rightarrow S_c \rightarrow S_i$.

r_{max} chosen to verify network connectivity constraints [1], [16]. Let $\{S_n\}$ be the set of n nodes placed in a given area according to a uniform distribution $\sim U[0,1]^2$, and indexed as $S_i : i = 1, 2, \cdots n$. Let $I(.)$ be an information assignment function on $\{S_n\}$, where I is a positive real valued mapping from $\{S_n\}$ to the 3-tuple as:

$$I(S_n) : \{S_n\} \rightarrow (\mathbf{x}, \mathbf{y}, \Theta)$$

$\mathbf{x} = (x_1, x_2, \cdots x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots y_n)$ represent the $x-y$ position coordinates of $\{S_n\}$, such that $x_i, y_i \sim U(0,1]$. The orientation vector $\Theta = (\Theta_1, \Theta_2, \cdots \Theta_n)$ is obtained as $\Theta_i \sim U(0, 2\pi]$ $\forall i$. $I(S_n)$ is known as the Information on $\{S_n\}$.

Each node S_i can orient its transmitting laser within a contiguous angular scanning region $\frac{-\alpha}{2} + \Theta_i \leq \Phi_i \leq \frac{+\alpha}{2} + \Theta_i$. Following the model in [1], [2] and as depicted in figure 1(a), this means that each node S_i can send data over a randomly oriented communication sector Φ_i of α degrees, for a fixed angle $\alpha \in [0, 2\pi]$. The case with $\alpha = 2\pi$ represents bi-directional communication. The receiving photo-detector is omni-directional and thus receives data from any direction. This means that node S_i may directly talk to S_j ($S_i \rightarrow S_j$) if $(x_j, y_j) \in \Phi_i$; however, S_j can only talk to S_i via a multi-hop back-channel or reverse route, with other nodes in the network acting as routers along the path (unless $(x_i, y_i) \in \Phi_j$). In figure 1(b) this reverse route is: $S_j \rightarrow S_a \rightarrow S_b \rightarrow S_c \rightarrow S_i$.

B. OSN Hierarchical Network with Cluster Heads

In addition to optical trans-receivers, all nodes are also equipped with corner cube retroreflectors (CCR) [4]. A CCR is a simple optical device that reflects incident light back to source, and when used to modulate an interrogating beam from the base station yields huge energy savings compared to an active laser. This mode of communication is passive and bi-directional between a node and the base station, and is especially attractive because all the optical energy for communication is supplied by the base station, with negligible energy used for the modulating circuitry of the CCR on the node. CCRs are good for OSN nodes due to their small size, ease of operation and negligible power consumption.

After random deployment, a fraction of nodes $\{CH\}$ called cluster heads, are oriented such that they have a communication line-of-sight path with the base station, and can thus employ their CCRs to exploit the advantages of passive bi-directional communication with the base station [2]. Let P_{CH} be the probability that a node is a cluster head. Assume there are $m \cong nP_{CH}$ cluster heads in the network, we designate any node S_i^* which is a cluster head, as CH_j, for $j = 1, \cdots m$. The set of cluster heads $\{CH\}$ depends on node orientation (which is uniformly random), and the base station's location, so that cluster heads are uniformly distributed in the network.

Cluster heads forward/receive data to/from the base station without adversely depleting their energy resources. This leads naturally to a hierarchical structure in which nodes route data to the upwards 'closest' cluster head for onward forwarding to the base station (uplink), or receive data or broadcasts from the base station (down-link) via another downwards closest cluster head. This hierarchical architecture is tied to currently existing FSO and CCR technology, and has been studied, under Berkeley's Smart Dust Program [2].

C. Graph Theoretic Preliminaries

The OSN yields an underlying directed graph structure $G_n = (S_n, \mathcal{E}, \Theta, r_{max})$ which has been identified by Diaz et al [1] as a *random directed sector graph*. The directed graph consists of a vertex node set S_n and edge set $\mathcal{E}$, where every edge is an ordered pair of distinct nodes. $\mathcal{E}$ is represented as the $n \times n$ *adjacency matrix* of G_n with one row and one column for every node in the network, where:

$$\mathcal{E}(i,j)_{1 \leq i,j \leq n} \quad = \quad \left\{ \begin{array}{l} 1 \text{ if } \ (x_j, y_j) \in \Phi_i. \\ 0 \quad \text{otherwise} \end{array} \right.$$

indicates that there is (or not), an edge $S_i \rightarrow S_j$. $\mathcal{E}(i,i) = 0$ disallows self loops, and directionality implies $\mathcal{E}(i,j) \neq \mathcal{E}(j,i)$ necessarily, $\forall i, j$. Cardinality $|\mathcal{E}| = \sum_{\forall i} \sum_{\forall j} \mathcal{E}(i,j)$ is the total number of edges in G_n.

Let S_i's forward neighborhood denoted $FNeb(S_i)$ be the set of nodes $\{S_k\}$ that S_i can talk to, i.e. $S_i \rightarrow \{S_k\}$. Formally, $FNeb(S_i) = \{S_k\}, \forall k : \mathcal{E}(i,k) = 1$. Nodes in $FNeb(S_i)$ are called S_i's *successors*, and the cardinality, $|FNeb(S_i)|$ also denoted as S_i^+, is equivalent to $S_i's$ out degree. Similarly, S_i's *predecessors* are nodes in its backward neighborhood defined as $BNeb(S_i) = \{S_h\}, \forall h : S_h \rightarrow S_i$. $|BNeb(S_i)|$ denoted S_i^- is equivalent to $S_i's$ in degree. The sum along the i^{th} row of $\mathcal{E}$ is the out-degree of node S_i while S_i^- is the sum along the i^{th} column of $\mathcal{E}$. A **path** from node S_1 to S_k in G_n is a sequence of nodes $[S_1 \cdots S_k]$ such that (S_i, S_{i+1}) (denoted $S_i \rightarrow S_{i+1}$) is an edge for $i \in [1 \cdots k-1]$. A **circuit** is a closed path, which means that it starts and ends at the same vertex. We define a **BS-circuit** as a circuit which starts and ends at the base station. Note that a BS-circuit must pass through either one or two (different) cluster heads.

D. Network Assumptions and Threat Model

We make the following assumptions on our network entities:

1) All network nodes are homogeneous, possessing the same capabilities and resources. Each node is equipped with beam steering circuitry, and knows its geographical location [1]. At initialization every node is good.
2) The base station is part of the trusted infrastructure that may not be compromised, and is resource rich.
3) At the least, an attacker may launch an outsider attack by deploying alien nodes in the network. This includes eavesdropping on network communication, injecting false data, and replaying previously overheard packets.
4) Nodes are not tamper resistant, so an attacker may subvert a random subset of nodes. A subverted node reveals its code, keys and security primitives to the attacker, making it possible for an attacker to control the node in an arbitrary way.
5) A judicious attacker may act in smart ways designed to maximally disrupt network activities. For example, an attacker may cause more damage by targeting cluster heads or highly connected nodes who are in the path of several BS-circuits.

III. Review of OPSENET Routing Protocol

OPSENET is a security aware optimized BS-circuit (uplink/down-link) discovery algorithm that assures nodes of the origin and integrity of routing signals. A summary of the five stages of OPSENET are:

- **Initialization and key setup:** *Base Station pre-generates and stores a one-way key chain [18], where F is a publicly known forward one way function, K_n^1 is an initial random bit string and K_1^1 is the commitment to the key chain. S_i is pre-deployed with: an individual key K_i shared with the base station, a counter C_i initialized to a random value (known to the base station), and the commitment K_1^1. Base station scans network to discover authentic cluster heads and floods routing beacons called cluster discovery packets (CDPs) to network via $\{CH\}$.*
- **Flooding Routing Beacons (CDPs):** *When a node S_i receives a CDP it has not previously processed, it increments the CDPs Hops Traversed (HT) field by one, appends its information $I(S_i)$ in the CDP packet's payload, and rebroadcast the updated CDP to its successors $FNeib(S_i)$, else it drops CDP.*
- **Terminating Routing Beacons:** *CDP routes are terminated when the CDP expires (i.e., length of path > predefined constant δ, or it reaches an (exit) cluster head who completes the BS-circuit by forwarding the CDP back to the base station.*
- **Base Station Network Topology Construction:** *Given $I(S_n)$ extracted from all returned CDPs, the base station constructs approximate graph topology and performs route optimizations.*
- **Multicasting Routing Information Packets (RIPs):** *The base station constructs and multicasts secure RIPs which contain individually secured information on the locally optimal next-hop uplink and downlink path for each node. Returned RIPs through uplink paths act as acknowledgement packets to help detect and prevent black hole and denial of service attacks.*

A. Node processing of the CDP

The CDP, illustrated in figure 2 consists of a 160-bit header and a variable payload. A new CDP $[HT = 0|K_2^1|E(K_1^1(nonce))][.]$ has an empty payload. Upon receiving a CDP from a cluster head, node S_i processes the CDP as shown in the Table below.

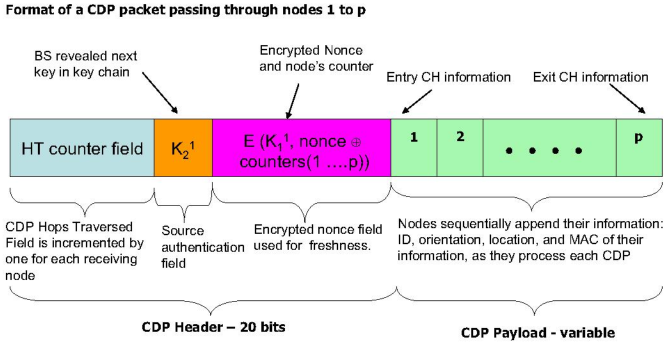
Format of a CDP packet passing through nodes 1 to p
BS revealed next key in key chain
Encrypted Nonce and node's counter
Entry CH information
Exit CH information
HT counter field
K$_2$^{1}
E (K$_1$^{1}, nonce ⊕ counters(1 ....p))
1
2
• • • •
p
CDP Hops Traversed Field is incremented by one for each receiving node
Source authentication field
Encrypted nonce field used for freshness.
Nodes sequentially append their information: ID, orientation, location, and MAC of their information, as they process each CDP
CDP Header – 20 bits
CDP Payload - variable

Fig. 2. Illustrating the format of a CDP; The first Hops Traversed (HT) field counts the number of hops made by the CDP, used to expire a packet and prevent excessively long paths. The second field is for broadcast authentication. Encrypted nonce field is for data freshness, and provides per hop node authentication with each node's counter XOR'ed to the nonce. The payload successively stores the MAC of information of nodes that process the CDP, to prevent routing loops, sinkhole or identity replication attacks.

```
1. Verify: $F(K_1^2) = K_1^1, HT < \delta; S_i$ has not processed CDP.
If 1. verifies
    Decrypt: $D(K_1^1, M.Nonce)$
    Update: New $M.Nonce$ = Old $M.Nonce \oplus C_i$
    Encrypt: $E(K_1^1, M.Nonce)$
    Increment: $HT = HT + 1$;
    Sign: $[S_i.authenticate] = MAC(K_i, M.Nonce|I(S_i))$
    Append: $I(S_i)$ and $[S_i.authenticate]$ to CDP packet.
    Rebroadcast: CDP → $FNeb(S_i)$ (CDP → BS if $S_i^* \in \{CH\}$)
```

Each node verifies the CDP originated from the base station using K_2^1, and increments HT by one. Nodes decrypt, update the nonce by 'XORing' their counters to the nonce, and re-encrypt, resulting in a modified nonce M.nonce. XOR function is chosen as it does not expand the bit size of the field. We assume 64-bit keys, nonce and counters, and a 32-bit HT field. To avoid routing loops, each node first examines a received CDP's payload to ensure that it's information is not in the payload (i.e., it has not previously processed this CDP from the same route of predecessors). Excessively long routing paths are avoided by terminating CDPs whose $HT > \delta$, a pre-defined constant. If both conditions above are false, the node appends an individually signed message authentication code (MAC) of its ID, *Information* $I(S_i)$ and M.nonce to the CDP's payload, and re-broadcasts. If the node is a cluster head, routing is terminated and the CDP returned to the base station. p is the number of appended sections in the CDP's payload.

B. Base Station Processing

The base station, with its unconstrained memory, energy and processing power, has the task of constructing the network topology, optimizing and communicating routing decisions to nodes. Each returned CDP reveals a BS-circuit, from which $\mathcal{E}$ is populated. Base station processes received CDPs as follows:

```
1. Verify HT = p; number of appended sections in CDP payload
2. if (1): $\forall p$ sections $\in$ CDP payload, identify & verify
   MAC of the nodes $S_1 \cdots S_p$.
3. if (2): Verify encrypted nonce by: $D(K_1^1, M.Nonce)$
   $Nonce \equiv M.Nonce \oplus C_1 \oplus C_2 \oplus \cdots \oplus C_p$
4. if (3): Extract $I(S_1) \cdots I(S_p)$ into base station routing table
Else:
Discarded CDP & initiate intrusion detection for the BS-circuit.
```

IV. GORA: Greedy Optimized Routing Algorithm

The aim of optimized routing in the OSN is to find the globally optimal uplink and downlink path for each node to/from the base station (from the maze of possible paths), with respect to some cost function. Unfortunately, global network route optimization is known to be NP-complete [20], therefore, we propose a simple distributed greedy approximation heuristic called GORA (Greedy Optimization Routing Algorithm) which quickly determines a locally optimized routing graph for G_n. GORA is anchored at the base station. We employ a minimum cost network flow model [20], with an integrated security and energy cost function. Each edge $\mathcal{E}_{ij}$ is associated with a cost C_{ij} given as $C_{ij}^U = \frac{D_{ij}}{\Gamma_j}$ for uplink, and $C_{ij}^D = \frac{D_{ji}}{\Gamma_i}$ for downlink, where $D_{ij} \propto d(i,j)^2$ is the transmission energy/bit expended on link $S_i \rightarrow S_j$ (known for FSO communication [3]), and $\Gamma_i = S_i^+$ or $\Gamma_j = S_i^-$ represents the trust factor (security confidence) of S_i for uplink or downlink respectively. C_{ij} trades off energy efficient routes versus security gains, and formalizes the idea that a highly connected node poses a higher security risk, since if compromised, several dependent BS-circuits are undermined.

GORA optimizes uplink and downlink routing paths for each node [16] by obeying the rules: (1) *Uplink*: $S_i^+ \ \forall \ S_i \in G_n = 1$ exactly. (2) *Downlink*: $S_i^- \ \forall \ S_i \in G_n = 1$ exactly. (3) Each link is traversed once only for any routing event. The pseudo-code for GORA uplink paths is detailed below[1].

```
Input ← $\mathcal{E}, D, C$, Child
Initialize Child[i] = NULL, for every node i
    Set C[i] = 0, for $i \notin$ {CH}; C[i] = $\infty$, for $i \in$ {CH}
    State0 $\equiv \{CH\}$
while(StateX != NULL SET)
  for int i=0 to StateX.count
    FNEB(StateX[i] = j for which $\mathcal{E}(i,j) = 1$;
    for (int $j = 0; j$ <FNEB(StateX[i].count; $j$++)
     StateX+1.add ( FNEB (StateX[i]) [j])
   if (C[StateX[i]] + D[StateX[i], FNEB(StateX[i])[j]]
        < C[FNEB(StateX[i])[j]]);
     C[FNEB(StateX[i])[j]] = C[StateX[i]]
        + D[StateX[i], FNEB(StateX[i])[j]];
     Child[FNEB(StateX[i])[j]] = StateX[i];
     end if;
```

Starting with each cluster head, for incoming uplinks, GORA compares the cumulative cost for each node to reach the set $\{CH\}$, and assigns the uplink with the minimum

[1] down-link procedure is similar, except the transpose of $\mathcal{E}$ and input vector Parent (instead of Child) is used.

cost to each node. The optimal next hop link for every node is stored in the vector $Child[n]$. After GORA executes, the base station constructs and multicasts individually secure route information packets (RIP) to all nodes containing the ID and information of their next uplink and downlink hop, via the appropriate entry cluster heads.

A. *Power and Topology Control at the Nodes*

Given ID and location of the optimal uplink and downlink next hop for S_i, denoted $[Child[i], (x_{Child[i]}, y_{Child[i]})]$, and $[Parent[i], (x_{Parent[i]}, y_{Parent[i]})]$ respectively, S_i initiates power and topology control by fixing its laser to the appropriate orientation (depending on broadcasting or gathering) and adjusting its transmitter power level relative to $Child[i]$ or $Parent[i]$. For example, with uplink gathering, S_i orients its laser to $\widehat{\Theta_i} = \arctan(x_{Child[i]} - x_i/y_{Child[i]} - y_i)$, and adjusts its transmitter power such that $r_i = \max[d(S_i, Child[i]), d(S_i, Parent[i])]$.

V. Analysis and Simulations

A. *Complexity Analysis for Network Discovery*

Theorem 1: *Network discovery routing for hierarchical OSN is $O(mn\lceil\log n\rceil - m^2\lceil\log n\rceil)$ in message complexity, and $O(\delta)$ in time complexity.*

Proof: Each of the m cluster heads receives a CDP packet to broadcast down link. The $n - m$ nodes (including entry but excluding exit cluster heads) have an out-degree of $O(\lceil\log n\rceil)$ [1]. Consider m spanning trees, each rooted at every cluster head. Every tree contains $O((n-m)\lceil\log n\rceil)$ edges, so that number of broadcast messages required to discover the network topology is $O(mn\lceil\log n\rceil - m^2\lceil\log n\rceil) \approx O(mn\lceil\log n\rceil)$ for $m << n$. Since all CDPs are terminated after δ hops, time complexity is limited by this constant.

B. *Security Considerations*

We enumerate the security properties of our scheme as:

- A judicious attacker may not elect himself cluster head for the purpose of denial of service or other malicious attacks, as cluster heads are not self-elected. The only way this may occur is if the malicious node is capability-enhanced in a way that he obtains a line-of-sight path to the base station irrespective of its orientation or the base stations' location. We do not consider this attack here, since we assume all nodes are homogeneous.
- Directionality may be leveraged to counter attacks based on traffic pattern analysis. Unlike conventional clustering based on geographical Euclidean radius from a cluster head, OSN clustering does not reveal the position or direction of a cluster head, unless each link is followed to a cluster head.
- Our cost function which integrates an energy and trust factor consideration mitigates attacks that target highly connected nodes in the hope of placing the attacker in several paths.
- Individual keys k_i are used in each nodes MAC to provide per hop (node) authentication to the base station. Individual MAC on a nodes' data also prevents a malicious node from arbitrarily inserting false IDs in the CDP to lengthen routes, as he cannot manufacture an authentic individual key.
- Due to cumulatively changing the counter (employing XOR function), routing messages may not be arbitrarily altered. Because nodes decrypt, add their counter and re-encrypt the nonce, if a malicious node deletes a previous entry into the CDP, computation on the final nonce will not verify at the BS.
- Alien nodes may not participate in route establishment since only authentic nodes know K_1^1 used to decrypt the nonce, and their individual keys used for MAC.
- Since only the base station knows future keys e.g., K_2^1 prior to network discovery, and a unique nonce used to authenticate routing signals, it is difficult for another entity to spoof, fabricate or initiate routing signals. Even though K_2^1 is revealed in the CDP in the clear, it does not lead to sinkhole attacks due one way paths for link directionality. Wormhole attacks to confuse base stations topology construction and GORA are concievable, however position information inserted into the CDP by each node helps mitigate this threat. In addition, wormhole attacks require enhanced-capability malicious nodes, which we do not address in this paper.
- A subverted node is restricted only to denial of service (blackhole) attacks, which is the best that can be hoped for.

C. *Energy Considerations*

We consider energy required for uplink data gathering, as it is similar for downlink broadcasting. Assume fixed packet size p-bits and E_p is transmission energy/p-bits/unit distance (receiver energy for FSO is negligible). Consider two sensor monitoring possibilities:

(1) *Continuous Monitoring*: All nodes constantly sense and route their data to the base station, e.g., habitat monitoring. Number of packets sent by node S_i is $D_i + 1$ where D_i is the number of descendants of S_i. Total network routing energy is given by $E_N = \sum_{\forall i \in G^c} E_p.(D_i + 1).D_{i,Child[i]}$.

(2) *Leaf-Node Monitoring*: Data is sampled only by the leaf nodes who forward data to the base station (similar to reverse flooding). In this case: $E_N = \sum_{\forall i \in G^c} E_p. * D_{i,Child[i]}$.

Simulations: All simulations are done on `OPSENET` software designed for testing OSN routing algorithms [19]. Our simulation use $n = 500$ nodes, $r_{max}(n) = \sqrt{\frac{1.2 \log n}{n}}$ and $\alpha = 2\pi/9$ (unless stated otherwise), in a square region of unit area. In our simulations, we compare the OSN hierarchical directional clustering with conventional bi-directional 1-hop clustering (all nodes are one hop from the clusterhead), and multi-hop clustering (nodes employ multihop routing within clusters using same r). We have assumed the same network setup (i.e., same G_n and given set of clusterhead nodes $\{CH\}$) for all simulations scenarios. Figure 3 shows energy versus node density graphs for (b)leaf-node, and (c) continuous monitoring. We see that in all cases, increasing node density does not significantly impact the energy dissipated in the network, since routing distances (and energy) $\propto 1/n$. Also, as would be expected, multi-hop clustering outperforms 1-hop clustering, and both clustering techniques in a bi-directional network outperforms directional hierarchical clustering. Figure 4(a) and (b) comparing energy versus P_{CH} show that increasing the

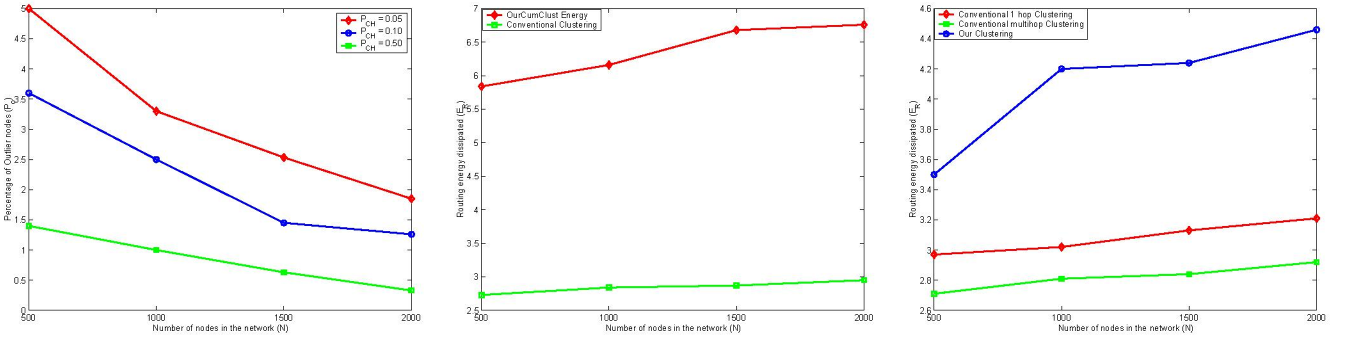

Fig. 3. (a) Plotting the percentage of outlier nodes versus the number of nodes in the network reveals that connectivity improves with network density and P_{CH}. (b-c) Comparing routing energy versus node density for (a) leaf-node and (b) continuous monitoring versus conventional bi-directional clustering. Both graphs show that node density does not impact total network routing energy, and conventional bi-directional clustering out-performs uni-directional clustering.

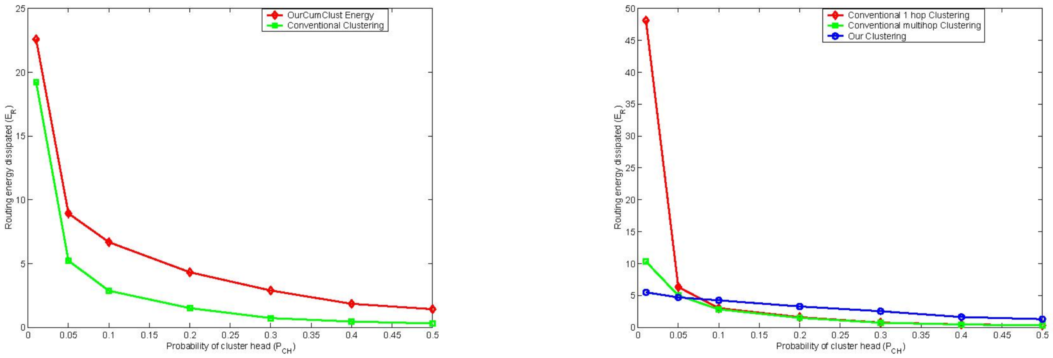

Fig. 4. Routing energy versus probability of cluster heads in the network for (a)leaf-node monitoring and (b) continuous monitoring.

number of cluster heads in the network significantly improves network routing energy in all scenarios.

VI. Conclusions

In this paper, we presented energy and security considerations for network discovery and optimized routing protocol for OSNs. Our analysis and simulations show the performance of proposed algorithms in terms of energy and security.

References

[1] J. Diaz, J. Petit, and M. Serna, A random graph model for optical networks of sensors, In *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, pp. 186196, July- September 2003.

[2] J. M. Kahn, R. H. Katz, and K. S. J. Pister. Next century challenges: Mobile networking for smart dust. In *Proc. ACM/IEEE Int. Conf. on Mobile Computing and Networking*, Washington, Aug 1999, pp. 271278.

[3] J. Hill, R. Szewczyk, A. Woo, S. Holler, D. Culler and K. Pister. System architecture directions for networked sensors. *Proceedings of the ninth international conference on Architectural support for programming languages and operating systems*, pages 93–104, 2000.

[4] S. Teramoto and T. Ohtsuki. Optical wireless sensor network system using corner cube retroreflectors. *EURASIP Journal of Applied Signal Processing* 1, 39-44. (Mar. 2005).

[5] W. Luh and D. Kundur, Distributed Privacy for Visual Sensor Networks via Markov Shares, *Proc. 2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, Maryland, April 2006.

[6] Brad Karp and H. T. Kung, GPSR: greedy perimeter stateless routing for wireless networks, MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking, Boston, Massachusetts, United States, pp 243–254, 2000.

[7] C. Alvarez, J. Diaz, J. Petit, J. Rolim and M. Serna. Efficient and reliable high level communication in randomly deployed wireless sensor networks *MOBIWAC-2004*.

[8] C. Intanagonwiwat, R. Govindan and D. Estrin. Directed diffusion: A scalable and robust communication paradigm for sensor networks. *Proc. of the Sixth Annual Int. Conf. on Mobile Compt and Networking*, 2000.

[9] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. In Imielinski and Korth, editors, *Mobile Computing*, volume 353. Kluwer Academic Publishers, 1996.

[10] F. Ye, A. Chen, S. Lu, and L. Zhang. A scalable solution to minimum cost forwarding in large sensornetworks. *Proc of Tenth International Conf on Computer Comm. and Networks*, pp 304–309, 2001.

[11] H. Huang, G.H. Chen, F.C.M. Lau and L. Xie, A Distance-Vector Routing Protocol for Networks with Unidirectional Links, *Computer Communications*, Vol. 23, No. 4, 2000

[12] S. Nesargi and R. Prakash, A tunneling approach to routing with unidirectional links in mobile ad-hoc networks, *In Proc. Ninth International Conf. on Computer Comm. and Networks.*, pp 522-7, NJ, USA, 2000.

[13] W. Dabbous, E. Duros, and T. Ernst, Dynamic routing in networks with unidirectional links, *WOSBIS97, Budapest, Hungary* Oct 1997.

[14] 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* (PDPTA2001), pp. 2021 2027.

[15] U. Ndili Okorafor and D. Kundur. OPSENET: A Security Enabled Routing Scheme for a System of Optical Sensor Networks *Proc. International Conference on Broadband Communications, Networks, and Systems (BROADNETS)*, San Jose, California, Oct 2006.

[16] U. Okorafor and D. Kundur, Efficient Routing Protocols for a Free Space Optical Sensor Network, In *Proc. IEEE Int. Conference on Mobile Ad Hoc and Sensor Systems*, Washington, D.C., November 2005.

[17] Dijkstra's algorithm, *http://en.wikipedia.org/wiki/Dijkstra's algorithm*

[18] H. Chan and A. Perrig Security and Privacy in Sensor Networks . In *IEEE Computer Magazine*, October 2003.

[19] OPSENET: Optical Sensor Network Simulator, *http://opsenet.tamu.edu*.

[20] R. K. Ahuja, T. L. Magnanti, J. B. Orlin Network Flows: Theory, Algorithms, and Applications Prentice Hall 1993