A Secure Integrated Routing and Localization Scheme for Broadband Mission Critical Networks

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

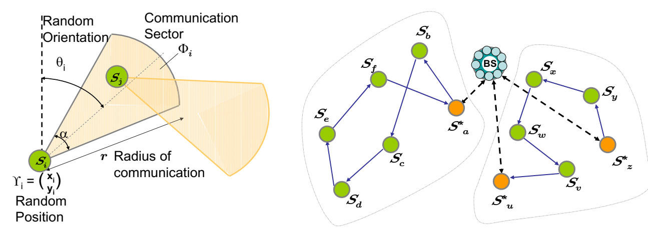
***Abstract*— In randomly-deployed wireless mission critical networks, the crucial steps of ad hoc route setup and node localization are vulnerable to various security breaches and attacks. In this paper, we introduce SIRLoS, a lightweight secure integrated routing and localization scheme which addresses this problem by exploiting the security benefits of link directionality in directed networks that have found popularity for multimedia networking. SIRLoS is a circuit-based algorithm that leverages the resources of the base station and the hierarchical structure of the network to reconstruct the graph of the network, and detect any security violations in the neighborhood discovery and routing schemes. We demonstrate the performance of our algorithm, and provide security and attack analysis.**

I. Introduction

Research in the emerging area of mission critical networks (MCNs) aims to develop mechanisms to promote specialized networks that are robust, ultra-dependable, and secure in the face of adverse conditions. In some contexts, they are comprised of small-sized wireless battery-operated nodes that are randomly and rapidly deployed, and their resource limitations pose significant security challenges [2]. In particular, without adequate security design, they are vulnerable to attacks including passive eavesdropping, denial-of-service and data corruption [1]; these can easily lead to catastrophe for life-critical applications such as health-care monitoring and disaster exploration.

There has recently been a push toward the development of *directional optical mission critical networks* (DOMCNs) that can provide the Gbps speeds for broadband multimedia-capable communications. Such capabilities are imperative to provide multimodal surveillance for effective decision-making. By focusing transmission energy in one direction, longer communication ranges, reduced multi-path interference, and greater spatial reuse over conventional radio frequency (RF) communications is possible. As witnessed by the popularity of the UC Berkeley Smart Dust mote [2], [3], the use of free space optical (FSO) communications has distinct advantages for MCN applications.

Several MCN applications such as disaster exploration rely on the ability of nodes to securely gain knowledge of their location and to establish secure ad hoc routing mechanisms to identify, track and communicate critical data such as the presence of survivors. Due to the directionality of links in DOMCNs, neighborhood discovery and routing mechanisms for traditional omnidirectional RF networks [4] do not apply.



(a) The DOMCN node (b) The BS-circuit

Fig. 1. The Directional Mission Critical Network. Directionality of data transmission at the physical layer results in unidirectional links at the network-level giving rise to a circuit-based routing paradigm.

Furthermore, the resource constraints of the nodes impedes the use of global positioning systems (GPS) and costly security primitives based on asymmetric cryptography. It is therefore imperative that the feasibility of an integrated and low-cost routing and localization scheme for DOMCNs be explored.

In this paper, we introduce SIRLoS, a novel lightweight *secure integrated routing and localization scheme* for DOMCNs. SIRLoS does not employ range estimation methods, time synchronization or expensive localization hardware. Instead SIRLoS exploits a hierarchical cluster-based organization of the network to offer: (1) lightweight security services based on symmetric cryptography; (2) a novel circuit-based neighborhood discovery and routing approach; (3) a simple location estimation algorithm based on topology control. SIRLoS guarantees that routing and location information are protected against eavesdropping and unauthorized manipulation, while providing broadcast authentication, data confidentiality, integrity and freshness. We demonstrate the security benefits of link directionality in SIRLoS and provide performance evaluations as well as attack and security analysis to demonstrate the potential of SIRLoS in MCN applications.

II. The Directional Mission Critical Network

We consider the secure integrated routing and localization problem under the DOMCN scenario with a set $\mathcal{S}_n = \{s_i : i = 1, 2, \cdots n\}$ of n DOMCN nodes randomly (and densely) deployed in a simple planar *two-dimensional* region $\mathcal{A}$ according to a uniform distribution. Each node s_i, has an equal and independent likelihood of falling at any coordinate location $\Upsilon_i = \binom{x_i}{y_i} \in \mathcal{A}$, and facing a random orientation

978-1-4244-2219-7/08/$25.00 (c)2008 IEEE

$\Theta_i \sim$ Uniform$[0, 2\pi)$ with respect to a reference axes drawn vertically in Figure 1 (a). We denote $I(s_i) = (\Upsilon_i, \Theta_i)$ as s_i's *information vector*.

In an ideal model, every node is equipped with a directional broad beamed FSO transmitter of *communication radius* r km and *beamwidth* α radians, pointing in the node's orientation. As depicted in Figure 1 (a), through scanning a laser beam, s_i transmits data within a contiguous, randomly oriented *communication sector* $\frac{-\alpha}{2} + \Theta_i \leq \Phi_i \leq \frac{+\alpha}{2} + \Theta_i$ of radius r, and angle $\alpha \in [0, 2\pi)$, with Φ_i uniquely defined by $(I(s_i), r, \alpha)$. Following convention [3], the node's receiver is omnidirectional, so s_i may directly transmit to s_j (denoted $s_i \rightarrow s_j$) if and only if $\Upsilon_j \in \Phi_i$. However, s_j can only transmit to s_i via a *directed multi-hop reverse route* (denoted $s_i \rightsquigarrow s_j$), with other nodes acting as routers (unless of course $\Upsilon_i \in \Phi_j$, resulting in the bidirectional link $s_i \rightleftarrows s_j$). Naturally, in discovering a multi-hop reverse path, the notion of a *circuit* [6] (a closed multi-hop loop originating and terminating at the same node), results, and serves as the fundamental mechanism for bidirectional communications in DOMCNs [7]. The hierarchical network structure popular for ad hoc FSO networks [2] involves a base station BS and an appropriate clustering of nodes as we will later elaborate. We define a *BS-circuit* illustrated in Figure 1 (b) as a circuit that necessarily includes the BS. An *uplink* and *downlink* for each node in a BS-circuit consists of the directed path from the BS to that node, and from that node to the BS, respectively. For example, in Figure 1 (b) s_d's downlink path is $BS \rightarrow s_a^* \rightarrow s_b \rightarrow s_c \rightarrow s_d$ and uplink path is $s_d \rightarrow s_e \rightarrow s_f \rightarrow s_a^* \rightarrow BS$. Future research considers effects of a fading channel model.

The directed n-node graph $G_n(\mathcal{S}_n, \mathcal{E})$ representing the DOMCN consists of the vertex node set $\mathcal{S}_n$ and edge set $\mathcal{E}$ (represented as the $n \times n$ *adjacency matrix*, with every edge representing an ordered pair of distinct nodes, where $\mathcal{E}(i,j)_{1 \leq i,j \leq n} = 1$ if $\Upsilon_j \in \Phi_i$ or 0 otherwise, indicates that the edge $s_i \rightarrow s_j$, does or does not exist, respectively. We define $\mathcal{E}(i,i) = 0$ to prevent self loops. $G_n(\mathcal{S}_n, \mathcal{E})$, defined by parameters (n, r, α) has recently been modeled as a random scaled sector graph (RSSG) [3], with properties that are predominantly distinct from the random geometric graph (RGG) model [6] conventionally employed for RF networks (with $\alpha = 2\pi$). The directional paradigm requires that two distinct sets of neighbors be defined for each node s_i: the set $\mathcal{S}_i =: \{s_k\}, \forall k : \mathcal{E}(i,k) = 1$ consisting of s_i's *successors*, and the set $\mathcal{P}_i =: \{s_h\}, \forall h : \mathcal{E}(h,i) = 1$ consisting of s_i's *predecessors*. In omnidirectional networks, such distinction between successors and predecessors does not exist.

As is common, we assume a cluster-based DOMCN [3] in which a fraction of nodes play the functional role of *cluster heads* (CHs); gateway nodes that employ simple, low-power and cost effective hardware such as passive *corner cube retroreflectors* to establish a bidirectional communication link with the BS without significantly depleting their energy resources [2]. CHs send/receive data directly to/from the BS on behalf of other nodes in their associated clusters; a cluster consists of all nodes within a BS-circuit that contains at least one CH. Thus, a node can be part of multiple clusters. We denote the set of CH nodes by $\mathcal{CH}$, and mark a node $s_k \in \mathcal{CH}$ with an asterisk to give s_k^*. Obviously, by this definition, a virtual bidirectional grid connects all CHs via the BS so that $\mathcal{E}(i,j) = \mathcal{E}(j,i) = 1, \quad \forall s_i, s_j \in \mathcal{CH}$.

A. Threat Model

The DOMCN threat model on routing consists of two general classes of attacks; (1) *outsider attacks*, in which the opponent possesses no special access to the network; examples include passive eavesdropping, injecting false routing packets, and replay attacks, and (2) *insider attacks* in which a motivated opponent compromises (via physical or remote exploitation) a subset of authentic nodes, gaining access to secret cryptographic materials, and then launching any number of disruptive attacks by masquerading as an authentic network entity. Insider attacks are restricted to the limited capabilities of the original nodes, however, their access to trusted infrastructure and network resources makes them potentially debilitating and more difficult to identify and stem than outsider attacks.

B. Assumptions

The BS is a resource-rich, powerful, location-aware and trusted entity that cannot be compromised. In a disaster exploration situation, the BS may, for example, be set up prior to first responder action or may be placed on a stationary medical aid vehicle. Nodes are homogeneous, with a fixed r and α selected to satisfy connectivity constraints [8]. Node s_i is pre-deployed with a unique *individual key* K_i and *password* PW_i it shares only with the BS, and with a *network-wide key* K_N shared with every node, all of which are 64-bit random values. Nodes are aware of a preset positive integer δ representing the *maximum hop count*. With probability p_{CH} each node $s_i \in \mathcal{CH}$, and security primitives employing pre-deployed symmetric keys are assumed. Nodes are not tamper resistant and with probability p_a may be subverted by an attacker. Each node s_i is uniquely identified by its name, and is aware of its orientation Θ_i by employing an inexpensive compass. We denote $A|B$ as the concatenation of message A with message B, while $\mathbb{E}_K[M]$ and $MAC_K\{M\}$ denote the *encryption* and *message authentication code* (MAC) of message M with key K, respectively [9], both of which use a symmetric 64-bit key with the RC5 scheme and the HMAC-MD5 algorithm (with a 128-bit authenticator value), respectively [10]. We employ the XOR function $\oplus$ in our algorithms to avoid byte expansion.

III. SIRLoP: Secure Integrated Routing and Localization Protocol

A. Off-line Key Setup

The first stage of SIRLoS is off-line key generation and setup performed prior to network deployment. A μ-TESLA mechanism [10] is leveraged for BS broadcast authentication. Briefly described, the BS pre-computes and stores a length-E one-way *key chain* $\{K_e\}$ for $e = 0 \cdots E$, by successively applying a known one-way hash function $\mathcal{F}$ to a randomly generated initial key K_E, so that $K_e = \mathcal{F}(K_{e+1})$ where $e =$

978-1-4244-2219-7/08/$25.00 (c)2008 IEEE

$0, 1, \cdots E-1$ indexes a particular broadcast era, and E is large enough to span the network's lifetime. The last key of the chain K_0, known as the *commitment*, is preloaded into each node. Due to the nature of $\mathcal{F}$, future keys cannot be computed from previous keys. However, it is trivial to verify that a key K_e once revealed was derived from a previous key, by simply applying $\mathcal{F}$ to K_e $(e-1)$ times, denoted $\mathcal{F}^{e-1}(K_e)$, and verifying that the result equals K_0. After deployment, keys in $\{K_e\}$ are revealed to nodes by the BS in the reverse order from which they were generated, yielding an efficient, simple and lightweight mechanism for BS authentication.

B. Secure Neighborhood Discovery

After deployment, each CH, say $s_x^* \in \mathcal{CH}$, indicates its readiness to begin neighborhood discovery by sending a READY signal to the BS who responds by generating a unique nonce η_t^x at the current time t for s_x, and initiating the *challenge-and-respond protocol* (CRP) [10] to authenticate s_x^* employing K_x and PW_x. The CRP also provides a simple *range and angular* estimation mechanism for determining Υ_x. If s_x^* passes the challenge, the BS sends it a *circuit discovery beacon* (CDB) containing its position Υ_x, marked with η_t^x and encrypted with K_N for onward flooding. The exchange is:

$$
\begin{aligned}
&BS \rightarrow s_x^* : \mathbb{E}_{K_x}[\eta_t^x] \\
&s_x^* \rightarrow BS : \mathbb{E}_{K_x}[PW_x \oplus \eta_t^x] \\
&BS \rightarrow s_x^* : [\mathbb{E}_{K_N}[\,\underbrace{|\ HT = 0 \mid e = 1 \mid K_1 \mid \eta_t^x \mid \Upsilon_x \mid \ldots\ |}_{CDB}\,]
\end{aligned}
$$

where HT is a variable that counts the number of hops traveled by the CDB and is thus incremented at every intermediate node. The CDB consists of a 140-bit header and a variable payload into which each node s_i encountering the CDB inserts a 160-bit entry consisting of its 32-bit information vector (8-bit name, 16-bit position and 8-bit orientation values) and a 128-bit MAC signature computed as $MAC_{K_i}\{I(s_i)|PW_i\}$. The header consists of a 4-bit field for HT, an 8-bit field to hold e, and two 64-bit fields for revealing K_e and the rolling nonce values, respectively.

Each node s_i (including CHs) maintains a *predecessor routing table* PRT(s_i) into which it makes entries of the information vector of each of its predecessor along with the corresponding downlink and an associated *cost value*, computed based on HT. Upon receipt of a CDB from s_h, s_i decrypts the packet and performs the following security checks: (1) validation of the source of the packet by checking that $\mathcal{F}^{e-1}(K_e) = K_0$; (2) verification that $I(s_i)$ is not in the CDB's current payload, to avoid routing loops.

If $s_i \notin \mathcal{CH}$, it estimates its location Υ_i^{est} based on the location of its predecessors included in the payload of CDB's it receives, by employing the location estimation algorithm described in the following section. If $s_i \in \mathcal{CH}$, it simply obtains its accurate coordinates from the CDP received from the BS as previously noted above. It then performs a subsequent *range-and-orientation constraint* (ROC) test to verify that $d(\Upsilon_h, \Upsilon_i^{est}) \leq r$ and $|\Theta_i - \Psi_{hi}| \leq \frac{\alpha}{2}$, where $d(a, b)$ is the Euclidean distance between points a and b, and $\Psi_{hi} = \arccos \frac{d(y_h^e, y_i)}{d(\Upsilon_h, \Upsilon_i^e)}$ ensures that $\Upsilon_i \in \Phi_h$. The ROC test provides a geometric constraint on the network graph which is exploited as a security check, and provides protection against routing attacks such as wormholes.

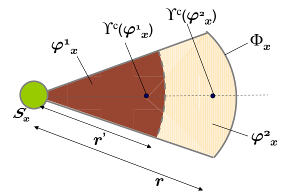


Fig. 2. The centroid of the two regions φ_x^1 and φ_x^2 that comprise the communication sector Φ_x of node s_x. The sector-based communication provides more localized estimation of the node position and the additional HELLO-phase provides even finer granularity.

Before forwarding the CDB, s_i verifies that $HT \leq \delta$ (i.e., the CDB has not expired), increments HT by one, updates the current nonce η_{t+HT}^* in the packet as $\eta_{t+HT+1}^* = PW_x \oplus \eta_{t+HT}^*$, appends its data $[I(s_i) \mid MAC_{K_x}\{I(s_x)|PW_x\}]$ to the CDB's payload, re-encrypts the new CDB with K_N, and then re-broadcasts the updated CDB to its successors. The route discovery task of a CDB with $1 < HT \leq \delta$ is terminated when it encounters a CH, who closes the BS-circuit by returning the packet to the BS. A CDB is discarded if $HT > \delta$ or if it fails any of the security checks. As a final step, within τ seconds after sending out the CDB, s_i broadcasts a low-bit hello packet (HELLO$_i$) within a communication sector $\frac{-\alpha}{2} + \Theta_i \leq \varphi_i^1 \leq \frac{+\alpha}{2} + \Theta_i$ of radius $r' < r$, discussed in the next section.

C. Location Estimation

The reception of the CDB provides a node s_i with knowledge that it lies within a sector ϕ_i of a predecessor. To provide finer granularity, the following procedure is employed. After τ seconds of receiving a CDB from s_i, s_j may determine that its location Υ_j lies either within the sector $\varphi_i^1 \in \Phi_i$ if it received HELLO$_i$, or otherwise within the circular segment $\varphi_i^2 \in \Phi_i$ as depicted in Figure 2, and then estimates its location Υ_j^{est} as the centroid of the corresponding region. The centroid is the least square error solution given s_j can fall with equal probability at any point in Φ_i.

Case 1: Node s_j concludes that $\Upsilon_j \in \varphi_i^1$ and determines Υ_j^{est} as the centroid $\Upsilon^c(\varphi_i^1)$ of φ_i^2, well known as:

$$\Upsilon_j^{est} = \begin{pmatrix} x_i \\ y_i \end{pmatrix} + \left| \frac{2r' \sin(\alpha)}{3\alpha} \right| \begin{pmatrix} \sin(\theta_i) \\ \cos(\theta_i) \end{pmatrix} \tag{1}$$

where $|.|$ denotes absolute value, and $r' = \frac{r}{\sqrt{2}}$ is determined to be the optimal radius of φ_1 such that $A(\varphi_1) = A(\varphi_2)$, implying it is equally likely that s_j falls within either part.

Case 2: Node s_j concludes that $\Upsilon_j \in \varphi_i^2$ and determines Υ_j^{est} as the centroid $\Upsilon^c(\varphi_i^2)$ of φ_i^2, determined as:

$$\Upsilon_j^{est} = \begin{pmatrix} x_i \\ y_i \end{pmatrix} + \left| \frac{2r \sin(\alpha)}{3\alpha} \right| \left(\frac{2\sqrt{2} - 1}{\sqrt{2}} \right) \begin{pmatrix} \sin(\theta_i) \\ \cos(\theta_i) \end{pmatrix}, \tag{2}$$

easily derived via the fundamental definition of *centroid*.

978-1-4244-2219-7/08/$25.00 (c)2008 IEEE

If s_y hears $m > 1$ predecessors, it estimates its location as the average of the centroids of the m regions within which it falls, given as $\Upsilon_j^{est} = \frac{1}{m}\sum_{q=1}^{m}\Upsilon^c(\varphi_i^q)$. In this case, Υ_j^{est} is not the centroid of the overlapping region of the m sectors, but simply an average point computation of a location within the overlap region that does not require complex search and grid score table schemes to obtain the boundary of the overlap region as employed in [11]. Note that our scheme differs from triangulation method [3] (each node waits to receive beacons from three known-location predecessors to determine its location), and nodes do not need to perform range estimation or angle-of-arrival measurements, keeping both computational and communication overhead low.

D. Base Station Network Topology Reconstruction:

The BS reconstructs $G_n(\mathcal{S}_n, \mathcal{E}')$ from BS-circuits and individual node information available in returned CDBs. First, it validates each CDB received (as discussed below), and then constructs an adjacency matrix $\mathcal{E}'$ by assuming that a subsequent node in a CDB's payload entry is a successor of the previous node. That is, if s_j's entry follows that of s_i, the BS assumes $s_i \rightarrow s_j$ and hence $\mathcal{E}'_{ij} = 1$. The BS also records (or compares with existing records) the information vector of each node represented in each received and validated CDB.

To validate a CDB, the BS performs the following security checks: (1) verifies that HT equals the number of appended sections in the payload; (2) verifies the claimed identity and per hop entry of each node s_i with an input in the payload, by ensuring that its computed $MAC_{K_i}\{I(s_i)\,|PW_i\}$ is equivalent to the signature entry of the node; (3) performs the ROC test for each link represented in the payload; (4) verifies that the final cumulative path nonce η^*_{t+h} included in the CDB for each h-length path, say $s*_1 \rightarrow s_2 \rightarrow \cdots \rightarrow s_h$, equals $\eta_t^1 \oplus PW_1 \oplus PW_2 \oplus \cdots \oplus PW_h$. If any of the security checks fail, or the BS observes any discrepancy in the entries of any CDB, that CDB is discarded, and intrusion detection mechanisms initiated on the affected and suspected routes.

E. Updating Nodes Routing Tables

From $\mathcal{E}'$, the BS constructs both the predecessor routing table PRT(s_i) and the successor routing table SRT(s_i) for each node s_i, and performs route optimizations. Similar to PRT(s_i), each of s_i's authentic successor's information vector, associated uplink and path cost is entered into SRT(s_i). The BS unicasts the encrypted routing tables $\mathbb{E}_{K_i}[\text{RT}(s_i)] = \mathbb{E}_{K_i}[\text{PRT}(s_i)|\text{SRT}(s_i)]$ to s_i, who upon receipt, compares the PRT from the BS with its self-registered PRT. Any discrepancy observed in entries triggers suspicion and deletion of the corresponding circuit from PRT(s_i) and a report to the BS. Nodes that receive valid routing tables conclude the neighborhood discovery phase by sending an acknowledgement (ACK) to the BS. The BS queries nodes from which it has not received an ACK within a stipulated time frame.

F. Dynamic Route Setup

Dynamic route establishment for the DOMCN entails a node, say s_i, seeking a secure and efficient route to any node s_j as needed, by leveraging the BS [10]: s_i sends an encrypted route request RREQ(s_j) for s_j to the BS, who responds by sending s_i the minimum cost path for $s_i \rightsquigarrow s_j$, and sending s_j the minimum cost RETURN link for $s_j \rightsquigarrow s_i$, encrypted with K_i and K_j respectively. The BS also includes a unique pairwise key K^e_{ij} to enable s_i and s_j establish a secure communication for a session. Due to space limitations, we have not discussed mechanisms for SIRLoS' route maintenance in this paper.

IV. Security Analysis

The BS verification and uplink-downlink path diversity in SIRLoS provides greater network monitoring, increasing the difficulty for a malicious node to control both the forward and reverse flow of the beacon (i.e., with high probability the CDB reaches the BS before returning to a node). This yields security benefits for DOMCNs and provides alerts of intrusion. We analyze attacks aimed at path diversity in section VI.

A. Per Hop Authentication and Alteration of Routing Beacons

Per hop authentication requires the BS to verify the correct participation of each node claimed in the CDB's payload. Employing the cumulative updating of a unique nonce originally generated by the BS, with node's passwords, a malicious insider node χ_A say, cannot arbitrarily alter routing information in a CDB without being detected. This distinguishing node-dependence feature strengthens the cryptographic property of SIRLoS, similar to the dependence structures used in encryption algorithms. Consider the two possible cases in which χ_A hopes to disrupt routing by forging a non-existent route: (1) he deletes the entry of one or more of it's *prior predecessors* (*ancestors*) from the CDB, and alters the HT value accordingly; (2) he inserts false node information in the CDB. In both cases however, without prior knowledge of the original nonce or the attacked/impersonated nodes' password and individual key, it is impossible to modify the accumulated nonce value in order to either extract entries to annihilate nodes, or input false entries into the CDB. Furthermore, tampering with the CDB in this way results in the non-verifiability of the final nonce received at the BS, and subsequent discarding of the packet. We have however identified two possible problem cases.

a) Problem Case I: In the two attacks enumerated above, χ_A may succeed in fooling its *following successors* (*descendants*) into making erroneous entries into their PRTs since the CDB is not verified until it is returned to the BS, prior to which nodes already update their PRTs. However, this falsehood is detected when the BS sends routing tables to each node, who then compares the PRT received from the BS with the one it recorded during neighborhood discovery. As previously stated, inconsistent entries are deleted and reported.

b) Problem Case II: A vulnerability exists where a bidirectional link $s_a \leftrightarrows s_b$ say, occurs. For example, the first node, say s_a, who receives the CDB is able to decipher s_b's password by storing the cumulative say $\eta^*_{t+\tau}$ when he first sees it at time step τ. After he receives the updated nonce

978-1-4244-2219-7/08/$25.00 (c)2008 IEEE

$\eta^*_{t+\tau+1}$ back from s_b via the bidirectional link, he deciphers PW_b as $\eta^*_{t+\tau} \oplus \eta^*_{t+\tau+1}$. To address this vulnerability, given the probability $(1 - \Pr[0 \leftrightarrows])$ that s_a has at least one bidirectional link (i.e., 1 minus probability it has no bidirectional link), and Z_a is the random variable (r.v.) counting the number of its successors, we consider the probability $p_{\chi_A}(> 0 \leftrightarrows)$ that χ_A compromises s_a which has at least one bidirectional link as:

$$
\begin{aligned}
p_{\chi_A}(> 0 \leftrightarrows) &= p_a \sum_{z=0}^{n-1} (1 - \Pr[0 \leftrightarrows] | Z_a = z]) \times \Pr[Z_a = z] \\
&= p_a \sum_{z=0}^{n-1} \left(1 - (1 - \frac{\alpha}{2\pi})^z\right) \frac{e^{\frac{-n\alpha r^2}{2}} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \\
&= p_a \left(1 - e^{\frac{-n\alpha r^2}{2}} \sum_{z=0}^{n-1} \frac{\left(\frac{n\alpha r^2}{2}(1 - \frac{\alpha}{2\pi})\right)^z}{z!}\right)
\end{aligned}
$$

$$
= p_a \left(1 - e^{\frac{-n\alpha r^2}{2}} e^{\frac{n\alpha r^2}{2}(1 - \frac{\alpha}{2\pi})}\right) = p_a \left(1 - e^{\frac{-n\alpha^2 r^2}{4\pi}}\right) \quad (3)
$$

for $n \to \infty$, where it is known from spatial point processes (see Chapter 8 of [12]) that Z_a, follows a Poisson distribution of parameter $n\frac{\alpha r^2}{2}$, with $\frac{\alpha r^2}{2}$ as Φ_a's area. Observe that for $\alpha \to 0$, $p_{\chi_A}(> 0 \leftrightarrows) \to 0$, however as $\alpha \to 2\pi$, $p_{\chi_A}(> 0 \leftrightarrows) \to p_a(1 - e^{-nr^2})$, which represents the RGG model [6], for which directionality cannot no longer be exploited. Furthermore, even if χ_A successfully deciphers PW_b, without knowledge of K_b, it can only succeed in dropping s_b's entry from the CDB, which may be acceptable as $s_a \leftrightarrows s_b$ represents an unwanted loop. Our future efforts study this "bidirectionality vulnerability" for general α values.

B. *Broadcast Authentication and Alien Node Participation*

Broadcast authentication ensures that only the BS is able to initiate routing. The CRP and encryption with K_N for confidentiality, both serve to prevent outsiders from sniffing the K_e and subsequently initiating, spoofing or fabricating CDBs. While $\{K_e\}$ provides initial broadcast authentication, (i.e., as no other entity but BS can reveal a correct K_e to CHs), we observe that, a key, once revealed in the CDB appears exposed to insider attackers. However, this information does not benefit the attacker as nodes do not route data back in the reverse direction from which they first received a CDB, but forward it along a directed path until it inadvertently reaches a CH. Additionally, the unique nonce marking all CDBs are eventually validated by the BS.

V. Performance Evaluation

We employ MATLAB simulations and analysis to study performance metrics of SIRLoS. With α, p_{CH} and r preset, $n = 300$ nodes are randomly positioned and oriented in a planar square region of unit area 1 km^2 according to a uniform distribution. As predecessor relationships are derived by reversing successor links, it suffices to populate $\mathcal{E}$ by determining successor relationships only, using the ROC test between each node and every other node. Each simulation scenario is repeated 1000, and results averaged over all trials to yield an acceptable statistical confidence of obtained results.

a) Localization Error: With p_{CH} set to 0.1, and r varying from 0 through 0.2 km, we run SIRLoS and compute the localization error LE $= \sum_{i=1}^{n} \sqrt{(x_i - x_i^c)^2 + (y_i - y_i^c)^2}/n$ as the mean squared error between the correct and estimated position vectors (initialized to zero) of $\mathcal{S}_n$. Figure 3 (a) illustrates plots of LE versus r for SIRLoS denoted "S" which performs better, compared with the centroid only [11] method (positions are estimated as the average centroid of the sectors of predecessors) denoted "C", as r increases and α decreases. Observe that as $r \to 0$, LE $\to (1 - p_{CH})$ (in this case 0.9), since the network is almost surely disconnected at small r values and CHs are the only nodes that determine their positions (accurately) from the BS. Another interesting observation is the 'phase transition' property [6], (LE transitions rapidly from a maximum to minimum value) which gets more dramatic as $\alpha \to 2\pi$. As expected, LE improves for larger α and r, as a greater number of predecessors are available for location estimation. In a second experiment, we vary p_{CH} from 0.1 through 0.5 and measure LE for various α, with $r = 0.1$ km. Figure 3 (b) illustrates plots of LE decreases with increasing p_{CH} and α.

b) Average Hop Count: To study the communication overhead of SIRLoS, we observe average hop count $\overline{HT}$, (computed by averaging HT values of CDB's received by the BS) versus α with r set to 0.1 and 0.2, and corresponding p_{CH} of $0.1, 0.2$ and 0.3. We observe from Figure 3 (c), that increasing r yields greater improvements in $\overline{HT}$ than a corresponding increase in p_{CH}, showing it more beneficial to focus resources on increasing r and α rather than p_{CH}.

VI. Attack Analysis

In this section, we consider attacks to circumvent and undermine the security advantage due to path diversity.

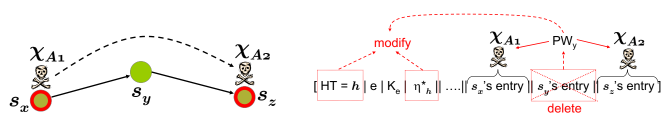
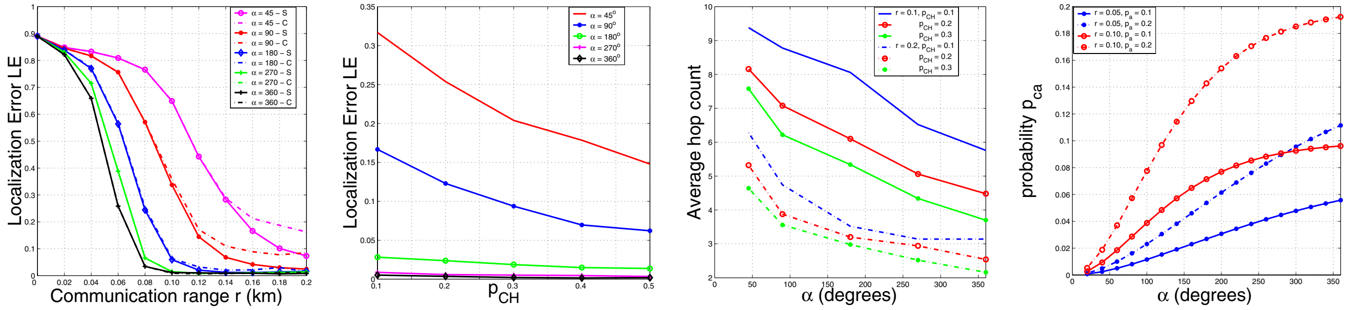


Fig. 4. BS-circuit collusion attack.

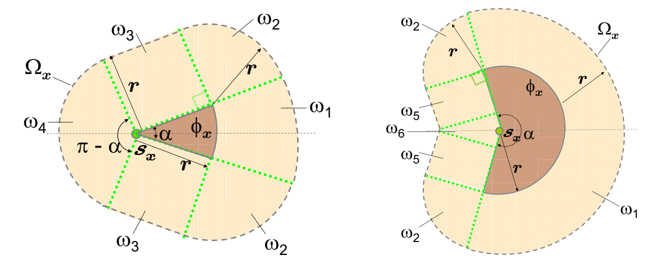
A. *BS-Circuit Collusion Attack*

We introduce a novel attack for DOMCNs termed the *BS-circuit collusion attack* in which insider nodes collude to place themselves both at the downlink and uplink of a target node s_y, thereby breaking the authenticity of the represented BS-circuit, as depicted in Figure 4 (a). The motivation for this wormhole-type [14] insider attack is to disrupt routing by deciphering PW_y, as similarly described in problem case II of section IV, and then successfully dropping s_y's entry from any CDB, as illustrated in Figure 4 (b). For tractability, we only consider here the case with two colluding invaders χ_{A1} and χ_{A2} attempting a 2-hop attack targeting s_x and s_z, both 1-hop from/to node s_y, respectively. We state the collusion attacker's problem by asking: Given that χ_{A1} has successfully



(a) LE versus r with $p_{CH} = 0.1$. (b) LE versus p_{CH}, $r = 0.1$ km. (c) Average hop count versus α. (d) p_{ca} versus α.

Fig. 3. Simulation results show improvements in LE with increasing r, α, p_{CH}, and the vulnerability to collusion attack for large α.



(a) $\alpha < \pi$ (b) $\alpha \geq \pi$

Fig. 5. Depicting the region of possibility where s_x's successor falls.

invaded s_y's predecessor s_x, what is χ_{A2}'s probability p_{ca} of invading a second node s_z that is one of s_y'successors?

We determine the search region Ω_x where χ_{A2} attempts an invasion to be the *locus* of points at a fixed distance r from Φ_x, delineated by the dotted line around the shaded region in Figures 5 (a) and (b) for $\alpha < \pi$ and $\alpha \geq \pi$ respectively. The probability p_{ca} of χ_{A2} invading node $s_z \in \Phi_y$ given $s_y \in \Phi_x$ is: $p_a \sum_{z=0}^{n-1}(1 - \Pr[s_z \notin \Phi_y | s_z \in \Omega_x \mid Z_y = z]).\Pr[Z_y = z]$:

$$
\begin{aligned}
p_{ca} &= p_a \sum_{z=0}^{n-1} \left(1 - (1 - \frac{A(\Phi_y)}{A(\Omega_x)})^z\right) \frac{e^{\frac{-n\alpha r^2}{2}} \left(\frac{n\alpha r^2}{2}\right)^z}{z!} \\
&= p_a \left(1 - e^{-\frac{n\alpha r^2 A(\Phi_k)}{2A(\Omega_k)}}\right) \quad \text{for} \quad n \to \infty, \qquad (4)
\end{aligned}
$$

where $A(\lambda)$ is the area of λ. Simplifying steps in Equation 4 follow similar steps in Equation 3 and $A(\Omega_k)$ given as:

$$
\begin{aligned}
A(\Omega_k) &= r^2 \left[2 + \frac{3\alpha}{2} + \pi\right] \quad \text{for} \quad \alpha < \pi \\
&= r^2 \left[2(1+\alpha) + \frac{\pi}{2} - \sin(\frac{\alpha - \pi}{2})\right] \quad \text{for} \quad \alpha \geq \pi
\end{aligned}
$$

is the sum $\sum_i A(\omega_i)$ of the areas of the six regular-shaped partitions of the composite shape Ω_x as depicted in Figure 5, with $A(\omega_1) = \frac{\alpha r^2}{2}$, $A(\omega_2) = \frac{\pi r^2}{4}$, $A(\omega_3) = r^2$, $A(\omega_4) = \frac{(\pi-\alpha) r^2}{2}$, $A(\omega_5) = 2r^2[1 - \sin\frac{(\alpha-\pi)}{2}]$, and $A(\omega_6) = r^2[\sin\frac{(\alpha-\pi)}{2}]$.

Figure 3 (d) illustrates p_{ca} versus α (from Equation 4) for $r = 0.05,\ 0.1$, and $p_a = 0.1,\ 0.2$. Note that p_{ca} increases with α, verifying the directionality security benefit for DOMCMs.

B. Wormhole Attack

A particularly devastating outsider attack, the *wormhole attack*, has been widely studied for sensor networks [1], [11], [13]. Aimed at disrupting routing, a low metric route is established between two network locations through which the attacker tunnels packets recorded at one end of the wormhole to the other end where he replays them in a timely manner. Two common models, long range and short range wormholes [14], are typically considered. For both models, the ROC test similar to [14] serves to detect the wormhole.

VII. Conclusion

We introduced SIRLoS, a lightweight algorithm for integrated secure network discovery and localization for DOMCNs, anchored at the trusted BS. SIRLoS exploits hierarchy, link directionality and circuit based routing to detect security violations. We have provided security and attack analysis to show superior performance of the proposed scheme.

References

[1] C. Karlof and D. Wagner, Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proc. IEEE SNPA*, pp 113–127, 2003.
[2] J. M. Kahn, R. H. Katz, and K. S. J. Pister. Next century challenges: Mobile networking for smart dust. In *Proc. ACM SIGMOBILE*, 1999.
[3] 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. 186-196, July–September 2003.
[4] P. Papadimitratos and Z. Haas, Secure routing for mobile ad hoc networks, in *Proc. SCS CNDS*, 2002.
[5] W. Luh and D. Kundur, Distributed Privacy for Visual Sensor Networks via Markov Shares. In *Proc. 2nd IEEE DSSNS*, April 2006.
[6] M. Penrose, Random Geometric Graphs, Oxford University Press, 2003.
[7] T. Ernst and W. Dabbous, A Circuit-based Approach for Routing in Unidirectional Networks, *INRIA research report 3292*, Nov, 1997.
[8] U. Ndili Okorafor and D. Kundur, On the Connectivity of Hierarchical Directional Optical Sensor Networks. *Proc. of IEEE WCNC*, Mar 2007.
[9] H. Chan and A. Perrig Security and Privacy in Sensor Networks . In *IEEE Computer Magazine*, October 2003.
[10] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. SPINS: Security protocols for sensor networks. *Proc. ACM SIGMOBILE*, 2001.
[11] L. Lazos and R. Poovendran, SeRLoc: secure range-independent localization for wireless sensor networks, in *Proc. of ACM WiSE*, 2004.
[12] N. Cressie, Statistics for Spatial Data, *John Wiley & Sons*, 1991.
[13] Y. Hu, A. Perrig and D.B. Johnson, Wormhole Attacks in Wireless Networks, in *IEEE JSAC, Vol 24, No 2, February 2006.*
[14] R. Poovendran and L. Lazos, A Graph Theoretic Framework for Preventing the Wormhole Attack in Wireless Ad Hoc Networks, *ACM Transactions on Networking*, vol 2, number 3, 2007. pp325–358.

978-1-4244-2219-7/08/$25.00 (c)2008 IEEE