INVITED PAPER

Security and Privacy for Distributed Multimedia Sensor Networks

In systems where small, dispersed video-audio sensors feed data to a central observation station, power available for signal processing, networking and cryptography is severely limited and must be conserved.

By Deepa Kundur, *Senior Member IEEE*, William Luh, *Student Member IEEE*, Unoma Ndili Okorafor, *Student Member IEEE*, and Takis Zourntos, *Member IEEE*

ABSTRACT | There is a critical need to provide privacy and security assurances for distributed multimedia sensor networking in applications including military surveillance and healthcare monitoring. Such guarantees will enable the widespread adoption of such information systems, leading to large-scale societal benefit. To effectively address protection and reliability issues, secure communications and processing must be considered from system inception. Due to the emerging nature of broadband sensor systems, this provides fertile research ground for proposing more paradigm-shifting approaches.

This paper discusses issues in designing for security and privacy in distributed multimedia sensor networks. We introduce the Heterogeneous Lightweight Sensornets for Trusted Visual Computing framework for distributed multimedia sensor networks. Protection issues within this architecture are analyzed, leading to the development of open research problems including secure routing in emerging free-space optical sensor networks and distributed privacy for vision-rich sensor networking. Proposed solutions to these problems are presented, demonstrating the necessary interaction among signal processing, networking, and cryptography.

KEYWORDS | Free-space optical sensor networks; multimedia sensor networks; secret sharing; security and privacy; video sensor networks

Manuscript received November 9, 2006; revised April 4, 2007.

The authors are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843-3128 USA (e-mail: deepa@ece.tamu.edu; luh@tamu.edu; unondili@ece.tamu.edu; takis@tamu.edu).

Digital Object Identifier: 10.1109/JPROC.2007.909914

I. INTRODUCTION

In a battlefield scenario, entrenched terrorists concealed in a complex urban environment are surprised by overhead United Nations (UN) aircraft deploying thousands of small objects that appear on the surface to be explosives but are a new type of ordnance—the components of a robust and secure distributed multimedia sensor network (DMSN). The bits and pieces of the network are numerous and scattered so densely within the terrorists' stronghold that they are embedded and inextricable. A UN peacekeeping force captain activates a handle-held hypermedia pad wirelessly linked to a base station (BS) gathering tactical information from the DMSN. With these data, the captain surveys the observation regions, selecting points of interest to zoom in on visual and audio terrorist action, identifying weaknesses in opponent activity. The captain can plan a decisive strategy to bring the conflict to a quick end with minimal loss of life.

Meanwhile, thousands of miles away from the conflict, an embedded DMSN monitors patient activity in a geriatric facility, checking for gait anomalies, collapsed patients, or visual cues marking the early onset of disease. Patient data are relayed to robustly and securely transmit information to a central medical monitoring BS.

These are examples of how multimedia surveillance with embedded sensor network systems can revolutionize both military and civilian applications. The densely deployed nodes of the DMSNs must communicate (often) wirelessly and self-organize in order to acquire and communicate data effectively to the BS. It is critical for many applications that network data be protected from

intentional loss, modification, or unwanted access, creating a need for the design of secure and privacy-enhancing DMSNs.

A. Multimedia Sensor Networks

Classically, wireless sensor networks (WSNs) have been envisioned to consist of groups of lightweight sensor *nodes* that observe scalar data, communicate wirelessly, and are distributed in a physical region. The region contains a phenomenon of interest, which is to be monitored and possibly controlled. WSNs possess many of the following distinctive features [1]–[3]. They are:

a) *distributed,* in order to improve the performance and geographical range of sensing functions;
b) *data-centric*, in which network processing and control are dependent on the nature of the sensed data instead of the particular identity of the node at which it was observed;
c) *collaborative,* making use of the coordination of *localized* algorithms to achieve a global task with better scalability;
d) *redundant,* using distributed densely deployed sensor nodes to obtain more accurate and complete readings of observed events;
e) *autonomous,* for adaptability to change in network topology and fault-tolerance without requiring servicing over long periods of time;
f) *application-specific,* requiring in-network processing, such as data aggregation (aka fusion), to produce meaningful data about the observation area;
g) *hierarchical,* through the localized clustering of sensor nodes into "subnetworks" to improve network scalability;
h) *resource constrained,* necessitating the sparing use of communication bandwidth, memory, and computation to reduce exhaustion of the often portable power source. Resource constraints represent one of the biggest design challenges for WSNs.

When the sensor nodes collect diverse types of information such as temperature, humidity, and acoustic and visual data simultaneously, they are termed "multimodal sensors." Multiple types of sensing can occur within the same node through the use of distinct sensing technologies or across different nodes, each having a single but distinct sensor type. Multimodal sensors that collect multimedia information such as digital images, video, and audio form a DMSN [4].

DMSNs are an emerging form of WSN in which a subset of sensors collect higher bandwidth content; DMSNs that sense and process visual information will play a critical role in societal advancement, security, and wellbeing. For example, in both tactical battlefield and healthcare surveillance, visual and other forms of broadband data are crucial for monitoring. These emerging sensor systems can also interface with previously deployed video surveillance hardware, extending their capabilities.

DMSNs have been proposed for a variety of applications. They are used in critical tasks often performed by humans such as the monitoring of sick patients [5]. For oceanographic monitoring, DMSNs provide a cheap alternative to characterize full water columns from the visual signatures of associated surface currents [6]. The use of low-cost nodes along with video information makes DMSNs attractive for the structural health monitoring of bridges [7]. In situations where the network *sink* is a human observer, processed visual data from the network can enhance user interactivity; for example, for unmanned ground or aerial vehicles, DMSNs provide the feedback necessary for human operators for make critical motion and target decisions [8]. The proliferation of low-cost portable off-the-shelf media sensing devices has motivated the recent development of vision-rich DMSN architectures, systems, and test beds [5]–[18]. Akyildiz *et al.* [19] provide an excellent recent survey.

The most significant technical challenges in the development of DMSNs involve obtaining the necessary intranode communication speeds while conserving power. For this reason, recent effort has also been focused on developing small low-cost sensors employing free-space optical (FSO) communications that can transmit broadband (multimedia capable) information with significantly lower energy in comparison to traditional omnidirectional radio-frequency (RF) nodes [20]–[23]. A well-known FSO sensor node is the Berkeley Smart Dust mote of [20]. Networking issues for such optical sensor networks are also a topic of current interest [22]–[27]. Recently, the Heterogeneous Lightweight Sensornets for Trusted Visual Computing (HoLiSTiC) paradigm for DMSNs based on FSO communications has been proposed [28].

B. Organization of This Paper

This paper provides an overview of security issues in emerging DMSNs, which are motivating the need for research in this field of societal importance. The next section addresses security research in general WSNs, leading to a discussion and survey of methods to protect vision-rich DMSNs. Section III reviews the HoLiSTiC setting for DMSNs, discussing the importance of emerging paradigms of directional wireless communications and distributed security. We next focus on two key problems of interest—secure routing in unidirectional sensor networks and distributed visual privacy—for emerging DMSNs. In particular, OPSENET, a circuit-based security-enabled routing approach, is introduced in Section IV; and TANGRAM, a lightweight distributed encryption algorithm, is presented in Section V. This paper concludes with final comments on the importance of the field of DMSN security.

II. SECURITY AND PRIVACY FOR MULTIMEDIA SENSOR NETWORKS

The broad applicability of DMSNs to both military and civilian applications makes the study of security and privacy in these networks of critical importance. While in a tactical battlefield scenario the robustness of a UN DMSN to stealthy terrorist attack may be of paramount importance, other forms of protection such as privacy guarantees are essential for situations such as patient monitoring in a geriatric facility. In both of these settings, the key to maximizing the utility of surveillance is ubiquity, necessitating government and public approval. Establishing trust in DMSNs, therefore, requires that security and privacy issues be effectively studied and addressed, leading to societal acceptance and large-scale adoption.

It is also vital to consider security and privacy design from system inception to provide the most effective built-in protection. If security is applied as an afterthought, it may provide only superficial protection, often leading to the need for repeated system upgrade, for which there is little opportunity in autonomous DMSNs. Given the emerging nature of DMSNs, it is critical that security and privacy be studied in a timely manner during the system specification and creation.

A. Wireless Sensor Networks and Security

In order to specify the types of protection needed by a WSN, a *trust model* and *threat model* must be specified. The trust model defines the level of trust (which may be binary or of a statistical nature) for the various network entities. For WSNs, it is conventional to assume that the BS is trusted and that a small subset of low-cost nodes is possibly corrupt. The threat model is often tied to the specific WSN application. In a battlefield, one possible threat is of the opponent's deploying his/her own "alien" sensor nodes in order to disrupt network operation. For healthcare monitoring, eavesdropping of private patient information by visitors to the geriatric facility is a risk.

One common distinguishing assumption in threat models of WSNs is the high likelihood of physical compromise of the low-cost sensor nodes; the rationale is that it is infeasible to incorporate expensive tamper-resistant hardware, making it possible for an attacker to physically access secret keying information to corrupt existing nodes or to effective deploy new ones. The corruption of even a single node has the potential to cause significant network damage due to the collaborative nature of the network entities. Conventional security primitives cannot adequately function when keying information is lost, especially in the face of the resource constraints of WSNs.

For this reason, much research into WSN security has focused on addressing both traditional *outsider* attacks, in which an opponent does not have keying information, and *insider* attacks, in which an opponent has gained access to keying information. The fundamental challenge in the design of security mechanisms to prevent outsider attacks is to provide a reasonable level of protection while not consuming significant node and network resources such as power, memory, computational load, and bandwidth overhead. For this reason, initial work in the field of WSN security studied low-cost symmetric security primitives and strategies [29]–[31] and key management [32]–[35]. The threat of insider attacks led to research in fields including resilient signal processing in which data redundancy was exploited to overcome "bogus" data sets inserted by corrupt nodes [36]–[40], "watchdog" approaches in which nodes are assigned a reputation value based on their behavior [41], [42], and countermeasures for denial-of-service (DoS) attacks on network services such as routing [43], [44].

B. Prior Art in DMSN Protection

Measures to protect DMSNs, to date, have focused on the problem of providing privacy in vision-rich systems. Lo *et al.* [13] introduce an automated homecare monitoring system for the elderly named UbiSense. The UbiSense DMSN system employs low-cost video sensors embedded in the environment along with body sensors and radio-frequency identification (RFID) in order to conduct gait and posture recognition of the elderly. Monitoring changes in gait and posture provides telltale signs of the onset of a physical accident or disease, providing an automated way to alert necessary caregivers when needed. To address the invasive nature of this approach, image processing is conducted directly at the camera that converts the video information into abstractions containing only shape and outline information necessary to recognize gait and posture anomalies. Only the abstractions are communicated and processed within the network, providing a form of privacy.

Fidaleo *et al.* [14] introduce the networked sensor tapestry (NeST) architecture designed for the secure sharing, capture, distributed processing, and archiving of multimedia data. The NeST hardware and software infrastructure is developed to facilitate the fast prototyping and deployment of DMSNs for a wide variety of surveillance applications including battlefield assistance and structural monitoring. To facilitate societal trust in DMSNs, the authors introduce the notion of "subjective privacy" in video where the behavior, but not the identity, of an individual under surveillance is conveyed. Their approach to privacy involves processing of the raw sensor data in order to remove personally identifiable information. The resulting data, approved for public viewing, are communicated in a network that employs the secure socket layer protocol and client authorization for network-level protection.

Wickramasuriya *et al.* [5] present a privacy-preserving video surveillance system that monitors subjects in an observation region using video cameras along with localized sensors. The localized sensors include RFID

tags that subjects wear and motion detectors placed within the observation environment. The motion detectors are used to trigger the video cameras on or off, and the RFIDs of the subjects provide authorization information in order to specify which individuals are entitled to privacy. The information from the various sensors is fused with the video data, resulting in a video stream with only authorized subjectsbeing masked through image processing. The current test bed makes use of the extensible access control markup language for specifying its security policies.

The proposed methods suggest a growing need for the design of security and privacy as an inherent part of DMSN system development. Because the security of a system is only as strong as its weakest link, we assert in this paper that for protection mechanisms to be effective, there must be a successful interaction among signal processing, networking, and cryptography. Furthermore, it is important to study paradigm-shifting security and privacy approaches due to the distinct nature of DMSNs.

C. The Need for New Paradigms

DMSNs possess unique characteristics that make design of protection mechanisms challenging. In contrast to scalar WSNs, DMSNs require high-speed hierarchical networking capabilities to transport broadband data. Furthermore, power conservation is a significant issue due to the volume and diversity of information being communicated and processed. For this reason, there has been recent activity on the design of sensor nodes that transport multimedia data directionally via FSO means [20], [21]. The physical communication characteristics of these emerging multimedia transport networks are distinct from traditional RF nodes, resulting in much interest in improving physical layer optical communications. For DMSNs, significantly less research focus has been placed on FSO networking level issues such as routing and security. We argue that it is essential to study network-level security issues of FSO DMSNs during the development phase of these systems.

DMSNs are also distinct from traditional scalar WSNs because they often exploit the resilience of multimedia data loss, making only elastic quality-of-service guarantees; this way, if the network sink is a human observer, the perceptual system's ability to be "forgiving" of select information loss can be exploited. This advantage also facilitates more cost-effective security and privacy solutions for DMSNs.

We next focus on an emerging model for WSNs that has received recent interest for multimedia transport. Through this paradigm, we study two important protection issues unique to and imperative for DMSNs: secure routing in unidirectional networks and distributed visual privacy. We focus on these problems because their relevance to DMSNs in contrast to issues such as key management, communications security protocols offering authentication and encryption, and intrusion detection that are applicable to and addressed by the general WSN security community.

III. HoLiSTiC: HETEROGENEOUS LIGHTWEIGHT SENSORNET FOR TRUSTED VISUAL COMPUTING

The HoLiSTiC paradigm encompasses the salient features of many proposed DMSNs in the research literature. Fig. 1 summarizes the HoLiSTiC model. Three types of network entities exist and are described next: the BS, the transport nodes, and the visual sensors.

a) *Base Station:* The powerful BS initiates network setup and maintains secure system operation. Using a common light source, the BS broadcasts information to all network entities that have appropriately oriented photoreceivers. It also contains several photodetectors for wide-angle reception. As conventionally assumed, the BS is a central trusted authority.

b) *Transport Nodes:* The lightweight wireless (battery-operated) transport nodes are equipped with

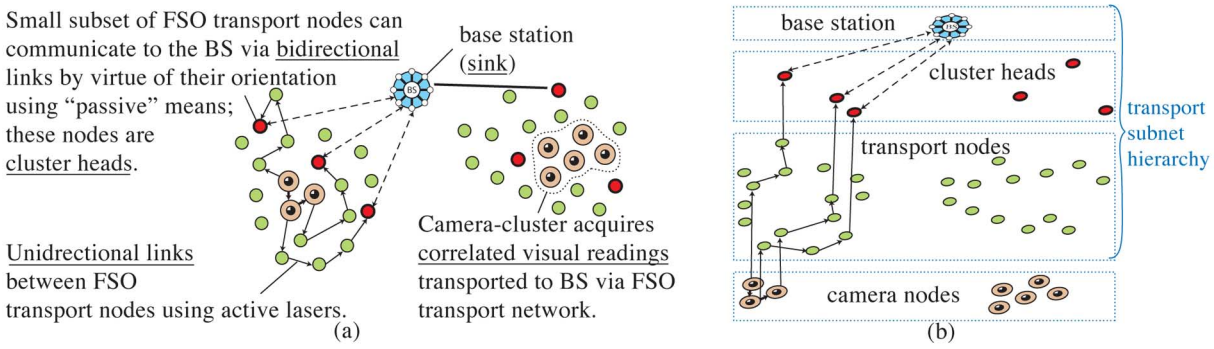


Fig. 1. *HoLiSTiC model. Camera nodes, FSO transport nodes, and BS communicate hierarchically.*

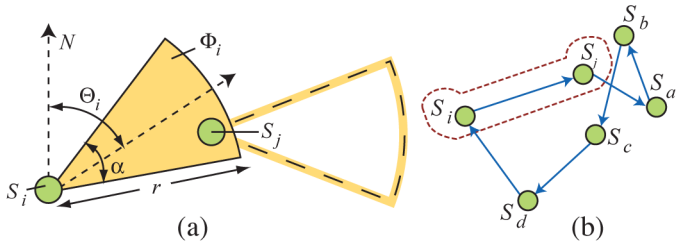


Fig. 2. *(a) The LoS communication model for FSO nodes. Node S_i can transmit to S_j because S_j is in the communication sector of S_i (denoted Φ_i) and S_i lies in the reception sector of S_j (denoted $\hat{\Phi}_j$). (b) Although S_i can communicate directly to S_j, S_j must communicate multihop to S_i via neighboring nodes S_a, S_b, S_c, S_d with appropriately aligned communication and reception sectors.*

FSO capabilities for both *active* laser transmission to other transport nodes and cameras and *passive* corner-cube retroreflector (CCR)-based bidirectional communications capabilities with the BS [20]. The nodes are randomly (using a uniform distribution for both position and orientation) and densely deployed to form an ad hoc network; in Fig. 2(a), n FSO transport nodes S_i, $i = 0, 2, \ldots, n-1$, are randomly deployed in a normalized 1×1 m^2 area. As illustrated in part of Fig. 2(a), each node S_i, with an active laser communication range r, has a random position (x_i, y_i) and random directional orientation Θ_i, and can orient its transmitting laser to cover a contiguous sector $-(\alpha/2) + \Theta_i \leq \Phi_i \leq (\alpha/2) + \Theta_i$ of radius r. Node S_i can, therefore, send data over a randomly oriented sector Φ_i of $0 < \alpha \leq 2\pi$ rad; typically, $\alpha \approx (2\pi/9)$ rad [22]. Node S_i's photodetector can receive data from all angles. Thus, for a node S_j to actively receive data from node S_i, $(x_j, y_j) \in \Phi_i$ must hold. This physical-layer line-of-sight (LoS) communication model results in unidirectional links at the networking level, depicted in Fig. 2(b); here S_i can communicate directly to S_j, but S_j must communicate via a multihop unidirectional backchannel $S_j \rightarrow S_a \rightarrow S_b \rightarrow S_c \rightarrow S_d \rightarrow S_i$ to return transmission to S_i. FSO nodes facilitate a *hierarchical* networking topology illustrated in Fig. 1(b). All transport nodes can receive information from the BS through their photoreceivers, but only those nodes with their CCRs facing the BS can reflect the common light source back to the BS, forming a bidirectional communication link. Therefore, the subset of transport nodes with their CCRs facing the BS is assigned the role of *cluster head* (CH). The CH often performs local aggregate computations for a localized set of nodes forming a cluster; in the HoLiSTiC setup, the CH is a gateway for information transfer between the nodes in the associated cluster and the BS. When randomly deployed, approximately 10% of nodes can become CHs [45]. Transmission via the CCRs is extremely low-cost (at 1 nJ/bit), ensuring that CHs do not significantly consume power [20]. The transport nodes (and CHs) are a target of attack by opponents.

c) *Camera Nodes:* The camera nodes $V_0, V_1, V_2, \ldots, V_{N-1}$ are deployed in a cluster and acquire visual data of interest. They are calibrated for proper sensing and communicate wirelessly (for ease of repositioning) in a delimited observation region. These visual sensors, equipped with the FSO capabilities described above, can communicate with the transport nodes. Depending on the application, the cameras can be line-powered or battery-operated. For example, in tactical battlefield applications, rapid and dynamic network configuration is required, necessitating the use of batteries and random localized positioning in an area of interest. For healthcare surveillance in a geriatric facility, the cameras can easily be line-powered and manually positioned to optimize viewing making system upkeep easier.

A. Networking and Key Management

The overall broadband hierarchical networking topology is illustrated in Fig. 1(b). The BS and CHs have bidirectional communication links. The camera and transport nodes have unidirectional links. Therefore, the unidirectional link transport network communicates data through multihop links to the CHs that then pass the resulting information to the BS. In contrast to general ad hoc networks where network-layer traffic is commonly between any nodes, the predominant traffic patterns of optical sensor networks occur between each sensor node and the BS for network maintenance, from each node to the BS for data transport, and between adjacent nodes for

coordination of data acquisition requiring novel communications and security perspectives.

Key management in the network requires that each network node have an *individual* key that is shared with the BS and that *pairwise* keys be available between adjacent visual nodes in a cluster. In addition, every network entity has two predeployed *network-wide* keys. All keys are employed for symmetric cryptography to provide a variety of security services. A number of proposed key management schemes in the WSN literature have potential to facilitate the necessary key exchange and update [32]–[35].

B. Free-Space Optical Sensor Networking and Security

FSO is a wireless LoS communication technology that transmits light beam signals, using the air as a transmission medium. FSO can achieve gigabit/second data rates over a range of a few kilometers. Lasers and light-emitting diodes are typically used for the transmission of light beams. Current optical sensor nodes employ 1550 nm (infrared, eye-safe) lasers and can achieve up to 2.5 Gbps over distances up to 6 km [20]. The laser beam can steer up to an angle of $2\pi/9$ rad, but if randomly deployed, the node's orientation and angular range limit the direction of communication transmission. An on–off keying modulation scheme is employed for communications that is amenable to lower power operation than the equivalent RF schema. The antenna gain of FSO is roughly seven orders of magnitude greater than RF, mainly due to the use of an optical divergence beam for transmissions instead of an isotropic radiator for RF.

RF communications is well understood, but FSO for sensor networks is still an emerging field with many open questions. Table 1 provides a flavor of the differences between conventional omnidirectional RF and FSO sensor nodes. The ultrahigh bandwidth, lower power consumption, smaller size, and convenience of deployment given the unrestricted nature of the frequency spectrum makes FSO an attractive means of communications for DMSNs. Furthermore, the compactness of the laser beam makes it difficult for an attacker to intercept communications in comparison to omnidirectional RF WSNs.

There are also many open challenges for FSO communications, resulting in much activity in physical-layer issues such as reduced bit rates encountered in adverse atmospheric conditions such as fog, heavy snow, and rain. Additionally, solar interference is a case where light from nonnetwork sources such as direct and intense sunlight may hamper the effectiveness of the system. Another limitation of FSO pertains to physical obstructions or uneven terrain that may cause communication interruptions. These issues are ongoing research challenges, the results of which will ultimately aid in deciding whether FSO or RF WSNs are appropriate for given application.

In this paper, we examine the implications of FSO to network-level services such as routing. Here, the LoS requirement along with the random nature of deployment creates unidirectional links amongst most nodes; our simulations suggest that 99% of nodes have unidirectional links, implying possible challenges with connectivity and routing. Because sensor nodes are restricted to be low cost, low power, and of small physical dimension, state-of-the-art device design can only accommodate a single laser with limited beam-steering range. Moreover, the ad hoc nature of the network does not allow for manual alignment of transmitters and receivers for bidirectional optical communications. One way to address this issue is for each node to employ an accurate point-and-track beam-steering actuator (i.e., the transceiver of a node is a mobile unit capable of swivel motion). Given the low-cost requirement and density of transport nodes, we opt to exploit the high level of redundancy and hierarchy in the network for connectivity.

C. Distributed Multimedia Security

It is well known that data security is best applied end-to-end in multimedia content networks in which there is a high degree of content adaption via compression or aggregation [46]. Furthermore, protection mechanisms

Table 1 Comparison of Omnidirectional RF WSNs to Undirectional FSO WSNs

	RF WSNs	FSO WSNs
Transmit energy	100 nJ/bit over 10 – 100 m	10 pJ/bit over 10 – 100 m
Receive energy	30 – 50 nJ/bit	Negligible
Frequency spectrum	Gov't Licensed, expensive	Unregulated, free
Bandwidth	up to 1 Mbps	0.045 – 1.25 Gbps
Size	$O(1)$ cm^3	$O(1)$ mm^3
Commun. channel	Broadcast, omnidirectional	Line-of-sight, directional
Commun. range	$>$ 100 km	$<$ 6 km
Interference	Electromagnetic and RF jamming attacks	Physical obstruction, weather, and solar interference

must be designed in conjunction with the adaptation processes to be transparent to networking.

The field of multimedia security has traditionally addressed the problem of application-level end-to-end security in multimedia networks. However, to account for the strong likelihood of insider attack and the limitations of wireless communications, multimedia security approaches along with effective cryptographic and networking paradigms are needed. To address these issues for privacy protection of visual data, we consider the problem of distributing trust via a novel decentralized variant of secret sharing in a multimedia security framework.

The high levels of redundancy and irrelevancy within DMSN systems in comparison to other forms of ad hoc networks and multimodal surveillance provides a rich environment to explore solutions for distributed multimedia security. The redundancy, designed originally for fault-tolerance, can be exploited not only for privacy but also to protect against forms of DoS network attacks. The irrelevancy, a characteristic of visual data, which is often exploited for lossy compression, can be used to provide a margin of tolerance for some forms of attack or in lieu of reducing security overhead.

IV. SECURE ROUTING IN THE FSO TRANSPORT NETWORK

We present a novel paradigm for secure unidirectional routing for DMSNs such as HoLiSTiC, in which security of topology discovery and routing against outsider attacks is achieved through low-cost cryptographic primitives. The inherent structure of the network and routing approach make it robust to many traditional insider routing attacks. These attacks, especially serious in battlefield networks, in which nodes are in the physical presence of opponents, have been analyzed primarily for omnidirectional RF sensor networks.

A. The Need for Secure Unidirectional Routing Paradigms for Sensor Networks

Routing in WSNs is receiving considerable recent attention; the heavy resource constraints, scale, and distinct traffic patterns of sensor networks make the direct application of Internet protocol (IP)-based protocols as well as ad hoc networking approaches inappropriate. Much of the existing sensor network routing research is based on the implicit assumption that sensor nodes communicate via omnidirectional RF and have bidirectional links, making it inapplicable for unidirectional sensor networks.

Research on routing in unidirectional networks can be grouped into that dealing with mixed bidirectional/unidirectional link networks and with purely unidirectional link networks. For mixed networks, the routing design is intrinsically tied to the network architecture; it is assumed that a small fraction of links are unidirectional in comparison to bidirectional, making use of approaches such as *tunneling* [47]–[52]. Adaptation of these techniques for almost purely unidirectional link networks is either not possible or will result in impractically high overhead from having to account for multihop reverse routes. For purely unidirectional ad hoc networking research, a *circuit* route paradigm is often employed [53]–[55]. A circuit is a sequence of unidirectional links starting from an initial node and propagating through a unique set of nodes to end at the initial node, thus closing the "loop." In Fig. 2(b), a circuit is shown for the following nodes: S_i, S_j, S_a, S_b, S_c, and S_d, making it possible for any of these nodes to communicate to each other. The spirit of this paradigm is adapted for our hierarchical system of sensor nodes, although it is not directly applicable because such techniques assume traditional many-to-many traffic models.

Given the unique characteristics of the secure routing problem in hierarchical unidirectional networks, we design a specific solution from scratch using the experience built from existing routing protocols. The new routing philosophy for FSO unidirectional sensor networks is to heavily leverage hierarchy and the powerful BS pushing complexity and processing to this sink; the additional overhead that traditionally comes with unidirectional routing can then be somewhat avoided by the individual sensor nodes. Furthermore, it is known that the overhead for circuit-based approaches can be reduced to lowering the length of the circuits [51], so we propose to leverage hierarchy in order to shorten the circuit length and avoid scalability issues.

Before we discuss the new routing paradigm, we briefly discuss the issue of connectivity for unidirectional sensor networks. Connectivity of the network refers to the ability of any node to communicate with any other in the

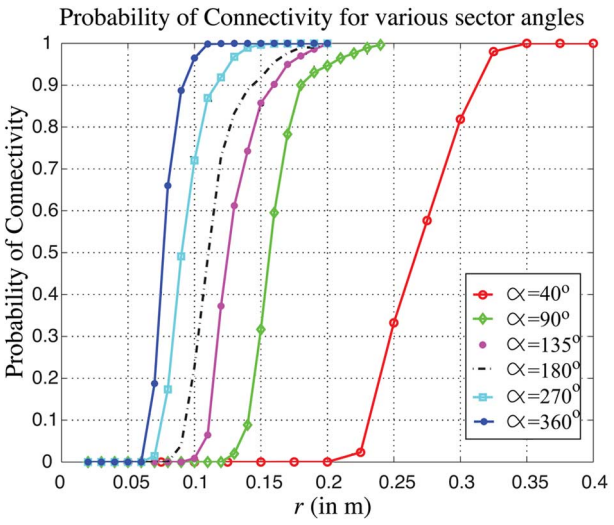


Fig. 3. ***Probability of network connectivity (i.e., all network nodes are connected) for various values of node communication radius r and sector angle*** α.

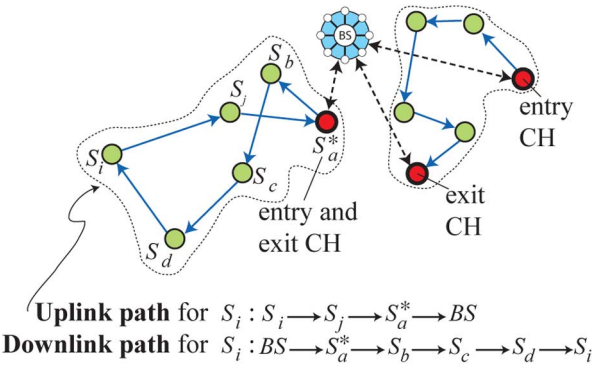


Fig. 4. *Two BS-circuits are shown with and without the same entry/exit CHs.*

network. The connectivity of the flat network topology is a necessary condition for successful routing performance. Fig. 3 demonstrates the characteristics of connectivity for $n = 500$ randomly deployed transport nodes modeled as in Fig. 2. The probability that all nodes are connected in the network is empirically estimated for varying communication radius r and sector angle α. Each simulation point was determined by repeating random deployment scenarios 1000 times for a given parameter set (r, α). The results demonstrate how connectivity of most nodes is feasible in such networks, underscoring the potential for successful routing.

B. Circuit-Based Unidirectional Routing

We propose a circuit-based approach to unidirectional DMSN routing that exploits the inherent hierarchy and power of the BS. Fig. 4 illustrates the proposed notion of a *BS-circuit* for our HoLiSTiC paradigm; we define a BS-circuit as a sequence of unidirectional links between transport nodes with a path leading away from and back to the BS (via CHs), forming a directed loop. CHs always start and end a BS-circuit and are marked with a superscript $*$, such that if the ith node is a CH, it is denoted S^*_i. The BS-circuit provides each associated node with an uplink and downlink path to and from the BS, respectively. If every node has a BS-circuit, then, communication to and from every network node is possible; some local communication is possible within a given BS-circuit and more general, global communication is possible via the BS that can pass information from one circuit to another. Identifying sufficient numbers of BS-circuits via topology discovery is essential to establish effective routing. We present a routing approach that employs BS-circuits in Section IV-D.

C. Goals and Additional Assumptions

Our objectives for secure sensor network routing follow.

1) From a performance perspective, for lightweight DMSNs, the routing approach must be energy-efficient, scalable, and capable of in-network processing.
2) From a security standpoint, the routing protocol must discourage/detect:
   a) fabrication of routing signals;
   b) malicious alteration of routing signals;
   c) formation of routing loops/route redirection; and
   d) DoS attacks during message routing such as sinkhole and blackhole attacks.

Within the HoLiSTiC framework, we additionally assume that the nodes are capable of symmetric cryptography, which is less costly than asymmetric mechanisms and thus more attractive for DMSNs. All nodes are assumed to know their location and to avoid message collisions after running localization and synchronization algorithms introduced in [22].

It is assumed that key exchange has occurred and that each node S_i shares a distinct *individual key* K_{S_i} and counter C_i with the BS, and has two pre-deployed *network-wide keys* K^1_1 and K^* employed for authentication and confidentiality, respectively. A microtesla mechanism is leveraged for BS broadcast authentication, as similarly proposed in [29]. The keys $\{K^1_e\}$ for $e = 1, 2, \ldots, E$ form a microtesla *key chain* with the following relationship: $K^1_e = F(K^1_{e+1})$ for $e = 1, 2, \ldots, K-1$, where $F(\cdot)$ is a one-way function and e indexes the particular broadcast era. The network-wide key K^1_1, also known as the key chain commitment, is used to verify a message is legitimately from the BS. Essentially, the BS broadcasts the key K^1_e in the eth era, which can be authenticated by any member in possession of K^1_1 by repeatedly applying $F(\cdot)$ (to K^1_e) $e-1$ times (denoted $F^{e-1}(K^1_e)$) and verifying that the result is equal to the commitment K^1_1; further details are provided in [26].

Our trust model assumes that the BS is trusted. Within our associated threat model, we assume the following.

1) The opponent can deploy alien nodes to launch eavesdropping attacks and the injecting of replayed and false routing signals.
2) The opponent can compromise a "small" fraction of nodes to obtain keying information to control a node in an arbitrary way to facilitate sinkhole or blackhole DoS attacks.
3) The opponent is constrained to similar hardware limitations as the transport nodes.

D. OPSENET: Topology Discovery and Secure Routing

We present an overview of OPSENET, a secure routing protocol that provides BS-circuit discovery, establishes routes proactively, and achieves per hop authentication, BS broadcast authentication, and cluster group secrecy; this effectively assures nodes of the original and integrity of routing signals. This protocol protects routing signals, specifically, and does not address data payload protection.

The general philosophy behind the design of OPSENET is to leverage the inherent hierarchy of the network introduced via a combination of active and passive communications. The hierarchy not only allows a more scalable system for routing but lends itself to leveraging the BS for some types of processing in order to save energy at the individual nodes. Furthermore, the more global picture of the network established at the BS, with the use of location information, provides a more effective means to identify blackhole and sinkhole attacks. OPSENET reduces consumed network energy and byte overhead by merging the processes of broadcasting and information gathering that are separated in existing directional sensor network routing work [22] into one step. Security primitives are incorporated in a way that keeps processing and communication overhead low.

Topology discovery starts by identifying CH nodes. Specifically, the BS floods light into the network and then CHs (i.e., all transport nodes that have their passive communication hardware facing the BS) respond by initiating a challenge–response protocol to authenticate the CHs. Then BS-circuits are identified for each non-CH transport node by employing selective flooding of secure routing beacons from the BS into the network via the CHs. The beacons act as agents that selectively traverse the network, gathering secure routing data as they propagate. Beacons are terminated when they reach a CH node, which then forwards them back to the BS.

We use the following notation to describe our security protocols: $M|M'$ denotes the concatenation of message M with message M', where M and M' are data from the same node; similarly, $M\|M'$ is used when M and M' are data from different nodes. $E_K(M)$ and $D_K(M)$ denote the encryption and decryption of message M with symmetric key K, respectively, while $MAC_K(M)$ is the message authentication code (MAC) of M using the symmetric key K.

After key predistribution and deployment, the BS broadcasts circuit discovery packets (CDPs) via the CHs. The format of a new CDP in the eth broadcast era is $[HT = 0|K_e^1|E_{K^*}(\text{nonce})]$, where HT is the *hops traversed* field and the nonce is randomly generated for data freshness; note that all initial CDPs are deployed with the same nonce sequence from the BS, so that, in a given era, the BS does not individually have to keep track of CDPs along different routes.

Upon receiving a CDP from the BS, a CH S_a^* verifies that $F^{e-1}(K_e^1) = K_1^1$. If the verification passes, it decrypts the nonce using the prestored K^*, XORs the nonce with its counter value C_a, increments the HT field by one, and signs (reencrypts) the (incremented) nonce to the CDP before broadcasting to all its immediate one-hop successors.

The CDPs for the first three hops of era e through $BS \rightarrow S_a^* \rightarrow S_b \rightarrow S_c$ are shown in Fig. 5(a). Individually signed nonces provide per hop authentication on the routes, while the MACs ensure that malicious nodes cannot tamper with a previous node's personal information entry.

To avoid routing loops, each non-CH node in receipt of a CDP first examines the sequence of appended IDs to ensure that it has not received this particular CDP from the same link. If it has not and $HT \leq \delta$, where δ is a network-dependent maximum hop threshold, the node processes the CDP in the same manner described above. Otherwise, it simply drops the CDP. When a CDP with $1 < HT \leq \delta$ reaches a CH, its route discovery task is terminated by the CH who closes the BS-circuit and forwards the packet back to the BS. The density of BS-circuits discovered in the above phase is high. In all simulations we conducted, the number of outlier nodes was negligible for $n \geq 50$ and primarily existed at the edges of the observation region.

Using the aggregate CDP information, the BS obtains the authentication information and uses the location information to form an approximate network topology,

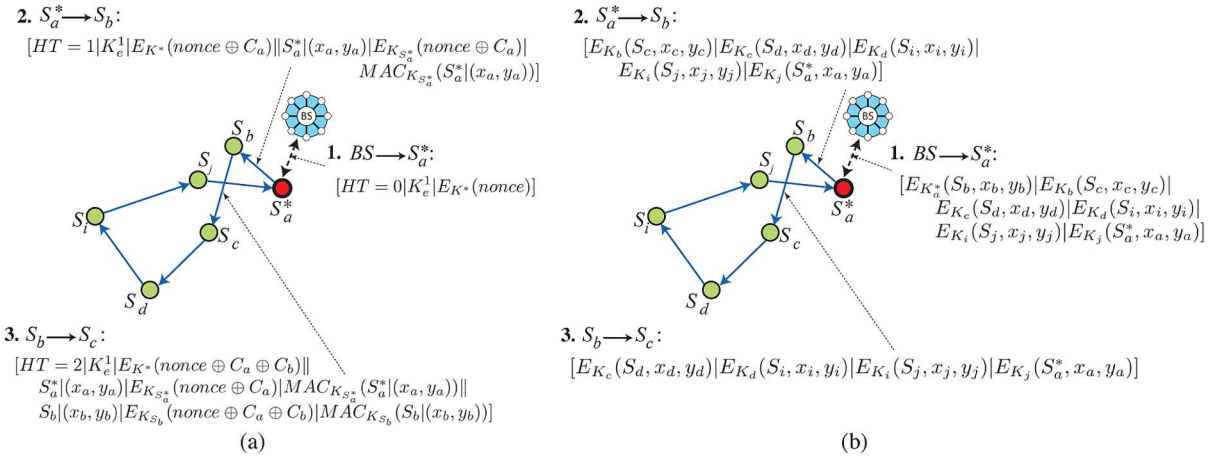


Fig. 5. *(a) Circuit discovery packets in BS broadcast era e for topology discovery; individual and network-wide keys are used for packet encryption/decryption. (b) Associated route information packets transmitted after topology discovery and BS processing.*

which is useful in defending against some types of routing attacks. The BS also processes the information to identify valid BS-circuits for routing via energy and security optimizations; further details can be found in [26]–[28].

For each valid BS-circuit, the BS constructs a route information packet (RIP) consisting of the uplink and next hop information for each associated node. The BS authenticates and successively encrypts the RIP with each node's individual key, so that (unnecessary) future routing information is not revealed to other nodes. This prevents a malicious node from altering routing information of subsequent nodes in the circuit. Each node can only extract its uplink successor ID and location from the RIP and passes the remaining data to this successor.

Fig. 5(b) illustrates the RIPs for the first three hops $BS \rightarrow S_a^* \rightarrow S_b \rightarrow S_c$. Each node progressively extracts, decrypts, and caches his own part of the routing information from the RIP and forwards the packet (minus its entry) to the next successor on the BS-circuit by aligning its laser according to the location information provided. The RIP will prove authentic since only the BS can generate correctly encrypted data with each node's individual key. It is to a malicious node's disadvantage to misrepresent its location data, since it will no longer receive packets from a predecessor, unless the goal is an intentional blackhole attack. Route maintenance discussed by the authors in [26] and [27] aids with this task. Here, the BS is alerted by individual nodes of suspicious activity via route maintenance requests that are address with route maintenance queries initiated by the BS to nodes along the associated BS-circuit.

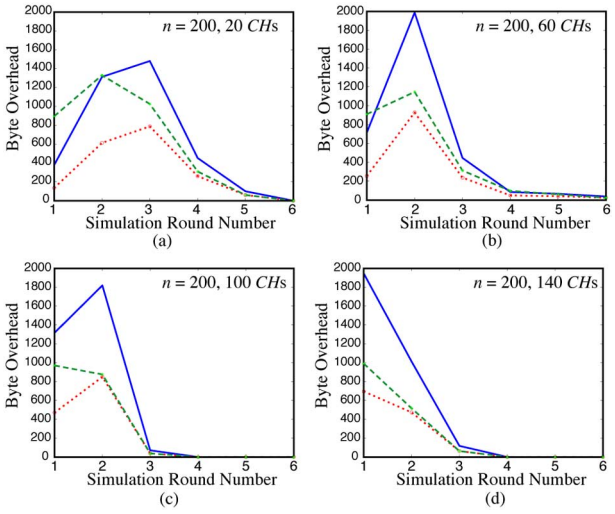


Fig. 6. *Protocol byte overhead simulations for $n = 200$ and $\alpha = 2\pi/9$ for (a) 20 CHs, (b) 60 CHs, (c) 100 CHs, and (d) 140 CHs. This solid line corresponds to secure OPSENET, the dotted line to unsecure OPSENET (i.e., without security overhead), and the dashed line to the combined* `simple-bro`/`simple-gather` *algorithms of [22].*

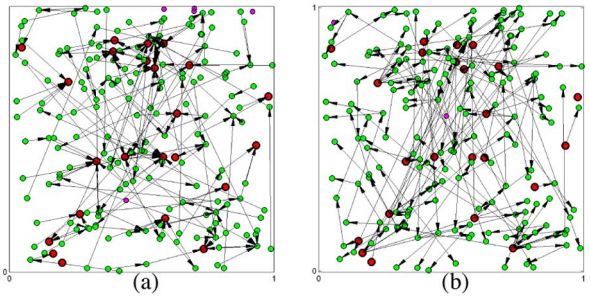


Fig. 7. *Optimal energy (a) uplink and (b) downlink paths; $n = 200$, $\alpha = 2\pi/9$; bolded (red) circles represent CHs.*

Fig. 6 provides a performance analysis of the proposed OPSENET in comparison to the `simple-bro` and `simple-gather` algorithms proposed in [22]. Since `simple-bro` and `simple-gather` do not consider security as a part of their design, we also compare this with an unsecured version of OPSENET without the keying and MAC data in the CDP fields. The performance is measured in terms of byte overhead, which is the overall number of bytes generated by the protocol, which may be used to evaluate, in part, the energy requirements of the protocols. For measuring byte overhead, the following assumptions were made: the key length is 64 bits, the nonce and counter lengths are 8 bits, the *HT* field is assumed to be $\lceil \log(\delta) \rceil$ bits, and a node's ID and position coordinates are each represented with $\log n$ bits. The algorithm finishes topology discovery in a reasonable number of simulation rounds. In addition, the OPSENET philosophy of combining information broadcasting and gathering into one circuit-based protocol reduces overhead, as seen when assessing the performance of unsecured OPSENET. The security functionality does result in additional overhead, which quickly dies down in time.

Fig. 7 illustrates the energy optimized uplink and downlink paths for $n = 200$, $\alpha = 2\pi/9$, and using the energy model of [20] and a Dijkstra-type algorithm. As can be seen, almost all nodes having uplink and downlink paths to the BS via CHs and OPSENET provide an effective means for establishing network connectivity.

E. Attack Analysis

In this section, we consider common routing attacks in the DMSN scenario; similar routing attack analysis for traditional RF sensor networks has been performed in [43], [56], and [57]. The integrated security of OPSENET ensures that it prevents outsider attacks such as unauthorized participation in route establishment, spoofed routing signaling, and alteration of routing messages and provides key freshness via the lightweight cryptographic mechanisms embedded in the protocol. A detailed analysis is found in [26].

Insider attackers are more difficult to detect and prevent since they act on behalf of authorized network participants. Traditional solutions often employ intrusion detection strategies [56] to adequately respond and recover. The main security goal against insider attacks is to have graceful degradation of network performance with the number of nodes compromised. We analyze the following well-known types of DoS attacks that affect DMSNs such as HoLiSTiC, which we argue are the most significant for routing in sensor networks because of their inherent nature to disrupt information flow in cooperative networks. The development of additional attacks targeting the unidirectional framework is a topic of ongoing research.

1) Type I: Sinkhole Attacks: A sinkhole involves a malicious node striving to illegally attract traffic through itself by giving other nodes the impression that a high-quality route exists through it to the BS. Once this is accomplished, the corrupt node can then launch selective forwarding, spoofing, packet altering, or eavesdropping. The two ways a malicious node may launch a sinkhole attack are the following.

a) *Wormhole Attacks:* A wormhole is a powerful form of sinkhole that involves two colluding nodes. The first node (typically with a cheaper/faster link to the BS) tunnels packets through a low-latency link to the second node, which resides in another part of the network in which such packets may not have reached following the normal network routes. It is then easy for the second node to launch a timely replay attack. The attack achieves a sinkhole by making the second wormhole node appear to have an efficient path back to the BS. The attack exploits the structure of reverse path routing in which link bidirectionality is assumed and the uplink and downlink paths are symmetric involving the same nodes. This does not hold for the directional circuit-based routing setup, thereby invalidating its effect; specifically, because a downlink path of OPSENET is different than its uplink path, a wormhole has limited effect in suggesting an attractive reverse route.

b) *Sybil Attacks:* In keeping with its namesake, the popular 1970s book *Sybil* on multiple personality disorder, in a Sybil attack [44] a single node presents multiple (false) identities for the purpose of confusing the routing scheme and leading to a possible sinkhole. A parallel attack involves identity fabrication or theft. In OPSENET, a malicious node may not fabricate or steal any other identity different from its own since the protocol requires each node to sign a MAC of its appended identity using its individual key shared with the BS. Furthermore, XORing its counter value (known only to itself and the BS) with the cumulative counter propagating along the route adds an additional layer for source authentication.

2) Type II: Blackhole Attacks: A blackhole entails a malicious node illegally attracting traffic to a nonexistent route so that packets attempting to traverse such hops are not received by any node and are therefore dropped. We discuss three blackhole attacks.

a) *HELLO Flood Attacks:* In a HELLO flood attack, opponent nodes broadcast high-powered long-range HELLO packets to deceptively announce themselves as neighbors to a much larger coverage area than can be attained using the required maximum RF communication range of a standard network node. Assuming the opponents to be neighbors, legitimate nodes will attempt to route data to the BS. In reverse path routing, this involves legitimate nodes routing data to the BS via the out-of-range opponents leading to "in air" packet dropping. In OPSENET, application of this attack will not have a relevant effect since routing is conducted through "successor" nodes that provide an uplink path to the BS. The opponent will be considered a "predecessor" neighbor who is part of the downlink path not used by the legitimate node for routing.

b) *Identity Replication Attacks:* Identity replication, in which the same identity is used many times in multiple locations, can be performed and defended against by the OPSENET protocol. By centrally registering each node's identity and location, the BS easily detects that the same identity exists in multiple locations. Another feasible approach is for the BS to centrally count the number of connections of each node using the network's adjacency matrix, and revoke those with more connections than an allowable maximum.

c) *Location Misrepresentation Attacks:* Another possible attack by a malicious node involves misrepresenting its location information to fool the routing protocol by causing its neighbors to route data away from legitimately receiving nodes thereby wasting resources. Such an attack in our DMSN scenario is easily identifiable by the BS, as the network topology is available to validate a node's location. Moreover, such an attack has negative implications that are emergent from the structure of OPSENET. In particular, since the uplink and downlink paths of a node are distinct, the malicious node cannot be selective and stealthy in which neighbors it misrepresents its position to. This implies that such an attack would effectively cut the malicious

node off from the network since its predecessors will incorrectly orient their laser in the wrong for that node. The periodical route maintenance schemes described in [26] will also detect and reroute for the resulting broken link.

3) Type III: Other Denial of Service Attacks:

a) *Neglect and greed*: In this attack, the malicious node neglects to route some or all messages passed to it. The subverted or malicious node can still participate in lower level protocols such as route maintenance but drops messages on a random or arbitrary basis or may give undue priority to its own messages. Packet acknowledgments are normally employed to ensure data are appropriately received in unreliable networks. Such paradigms are also useful for identifying this attack. However, if a node is stealthy, it may pass so-called acknowledgments to a node whose signals it has not passed, appeasing it. For unidirectional networks, the success of such an attack is limited because the malicious node cannot exist in both the uplink and downlink paths of a legitimate node; this additional level of diversity in multihop routing makes it possible for a malicious node to either control data flow but not acknowledgments, or vice versa, alerting intrusion detection mechanisms.

b) *Homing attack:* Homing attacks are based on traffic analysis, where an attacker sniffs packet headers in order to decipher where they come from and where they are going. For the optical sensor network scenario, such an attack may aim to obtain the network topology by observing routed packets and use such information to launch more harmful attacks. Given the passive nature of eavesdropping, such an attack is not easily detectable. However, in comparison to omnidirectional RF networks where communication is broadcast-based, FSO beams are physically more inaccessible, requiring that an attacker distribute itself and providing a higher level of effort, possibly deterring such opponent activity.

c) *Misdirection attacks:* These are similar to (victim-directed) sinkholes in which the attacker forwards messages along a wrong path with the intention of flooding its victim's link. One way to achieve this is for the attacker to forge replies to route-discovery requests, including the victim's ID in the spoofed routes. OPSENET guards against this attack and other route spoofing attacks by requiring that all nodes append their ID along with their MACs (encrypted with their individual keys, using the nonce as freshness).

The above analysis gives a flavor of the advantages and novelty that directional communications provides for routing security. The higher overhead required for directional routing is, in part, offset by its capability to naturally protect against traditional types of routing attacks based on reverse path routing as well as traditional eavesdropping due to the directed nature of the communication beam. In addition, the circuit-based routing anchored at the trusted BS provides additional security. The BS acts as the watchdog for the network, as it possesses the global picture of the network topology. Our ongoing research includes quantitatively assessing routing attacks to measure the robustness and degradation of the optical sensor network for this emerging paradigm. Our proposed solutions leverage redundancy, in part, to mitigate catastrophic network failures. As we see in the next section, redundancy can also be employed at the application layer to mitigate against higher level DoS attacks.

V. VISUAL SECRET SHARING FOR DISTRIBUTED PRIVACY

Although DoS in WSNs have received significant attention, there is still concern over protection against traditional passive attacks such as eavesdropping to provide the level of confidentiality and flexibility essential for applications such as geriatric monitoring. The decentralized data acquisition process in DMSNs and nature of multimedia offer opportunities to exploit the redundancy and distributed nature of the network.

We consider a novel distributed privacy paradigm for DMSNs, in which confidentiality is achieved in a decentralized manner. Fig. 8 illustrates the general scenario. Visual sensors V_0, V_1, V_2 in a cluster observe

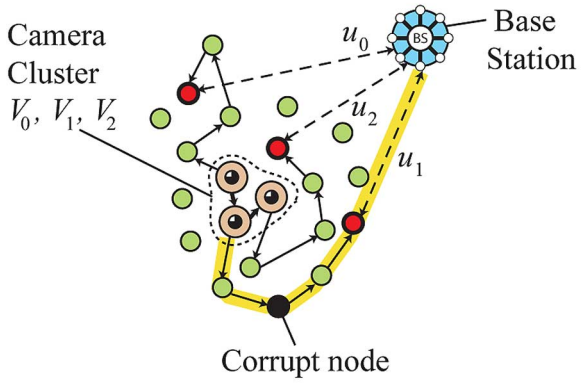


Fig. 8. ***Distributed privacy paradigm. Each visual sensor in a cluster acquires correlated data and generates a share that is transmitted to the BS along disjoint multihop paths. The BS is able to reconstruct an aggregate given most of the shares, while a corrupt node cannot, given its limited access to a small fraction of shares.***

correlated data, and each node V_i individually computes what is known as a *share* u_i from its observations; as shown, the cluster's shares are then individually transported along *disjoint* paths to the BS. The BS, having received all shares u_0, u_1, u_2, is able to reconstruct a representation or aggregate of the correlated data set from V_0, V_1, V_2. Suppose a corrupt node, shown in black in Fig. 8, is able to eavesdrop on all information communicated through it. Hence, the share u_1 transmitted along the highlighted routing path does not have confidentiality. Given that this eavesdropper has access only to u_1 (or, more generally, a small fraction of shares), it cannot fully deduce the content being sent. As a secondary security benefit, if the corrupt node does more than passively eavesdrop and instead actively tampers with or drops a share, given that enough uncorrupted shares reach the BS, it is able to reconstruct a representation of the data originating from the cluster. In this section, we detail the necessary node processing (i.e., share-generation) to achieve our security and privacy goals. Research on identifying disjoint routes is beyond the scope of this paper but is a topic of current research [58].

A. The Need for Distributed Secret Sharing

The approach we consider is reminiscent of the traditional problem of *secret sharing*. In secret sharing, a trusted central authority, called a *dealer*, shares a *single* secret $K \in \mathbb{F}$ (where $\mathbb{F}$ is a finite field) by distributing N shares to N individuals, called *participants*. The dealer would like to create shares such that only $t+1$ shares or greater can reveal $\overline{I}_R$ but t shares or fewer cannot reveal $\overline{I}_R$. The well-known Shamir scheme [59] illustrates an elegant solution to this problem. Here, *unconditional secrecy* is achieved through the dealer's use of random parameters for share generation that are known only to the dealer; not even the participants have access to these values. Generalizations of the Shamir scheme [60], [61] demonstrate unconditional secrecy in the same way.

There are several obstacles with direct application of conventional secret sharing solutions for privacy in DMSNs. First, given the centralized nature of secret sharing, where a single dealer entity creates the shares, one straightforward adaptation is to have the visual sensors in a cluster communicate their information to a single node, the "representative dealer," that then performs share generation. However, given the high likelihood of insider attack, this solution suffers from a single point of failure, whereby an opponent would need only to physically compromise the dealer node to eavesdrop.

Secondly, secret sharing is designed to create shares from a single unique secret. In the case of DMSNs, each visual sensor has a correlated reading of the others representing a composite secret; direct application of secret sharing to each component of the composite secret would be bandwidth-inefficient, making it crucial to devise a nontrivial method to account for correlations. Moreover, if each visual sensor in the cluster becomes its own dealer, each node would necessarily have to share the random parameters needed traditionally by the single dealer, making it once again easier for an eavesdropper to obtain the values by compromising any one of the visual sensors.

Last, traditional paradigms for secret sharing require that the $t+1$ or greater shares be able to perfectly reconstruct the original secret $\overline{I}_R$. This stringent requirement has been relaxed in the more modern formulation of the *visual secret sharing* problem applicable to digital images. Similarly, in the case of DMSNs, this forgiving nature of the human perceptual system to multimedia data loss can be exploited. This property along with the high levels of content redundancy within the network allows greater flexibility to design a distributed low-cost and robust solution suitable for DMSNs.

Thus we develop a new paradigm suitable for decentralized environments such as DMSNs; secret sharing and visual secret sharing are well-known concepts, but a *distributed* variant of the visual secret sharing paradigm is innovative. Our approach requires that private random parameters be used for secure share generation. However, each node is allowed to carry only a small subset of these critical parameters. Thus, if a single visual sensor node is compromised, the extent of critical parameters stored on-board is insufficient for an attacker to fully discover the secret $\overline{I}_R$. In addition, our approach allows for share-generation of different but highly correlated secrets $I_0, I_1, \ldots, I_{N-1}$ instead of assuming all sensors have the same secret $\overline{I}_R$ or independent secrets.

Our proposed algorithm sacrifices unconditional secrecy to provide a lightweight security solution realizable for lower cost sensors. We use a visual secrecy measure that degrades proportionally to the number of shares in possession by an eavesdropper. Such a relaxed definition of secrecy is based on an eavesdropper's perceived distortion and has been proposed in the theoretical literature [62]. The definition reduces the complexity of pixel-by-pixel computations and reduces the size of the shares in comparison to traditional visual secret-sharing solutions [63] reducing storage and bandwidth complexity, which are of paramount importance in DMSNs.

B. Goals and Assumptions

Our above discussion motivates the following goals for a distributed privacy system.

1) There is limited communication between visual sensors.
2) Each visual sensor must create its own share without the need for a central authority.
3) Each share must be smaller in size than the original secret I_i.
4) Capturing a single visual sensor and obtaining its contents will not degenerate the secret sharing nature of the system.

The first objective conserves bandwidth and discourages collaboration amongst camera cluster nodes as well as the use of key management that consistently refreshes the secret random parameters employed by each node. The second requirement makes it necessary to employ a distributed approach with the use of the traditional single dealer. The third promotes cost-effective processing and network share-communication and precludes the use of straightforward (symmetric or asymmetric) encryption for share generation. Since each visual node in a cluster has correlated information, it is essential that this similarity be used for reducing the data size. The last goal protects the overall system from an attacker who may gain access to the static contents of a node from reconstructing a secret from a share.

Our threat model follows.

1) The opponent can eavesdrop on only a small subset t of DMSN communication paths leading from the camera cluster to the BS.
2) If a camera cluster node is hijacked, revealing secret and share information, then it is removed from the cluster.
3) An active attack on data (e.g., corruption of share) is performed at a transport node and not at visual sensors within the camera cluster.

The first attack assumption reflects a reasonable, but limited, level of capability on the part of the attacker. To eavesdrop on a significant number of FSO links, an attacker must be physically distributed across a significant part of the network, which would be impractical and not stealthy. The second and third attack requirements make it impossible for a corrupt visual sensor or external opponent to "poison" the other nodes during share generation.

In addition, we assume that there exists disjoint physically separate paths from sensors within a cluster to the BS in the DMSN; shares from within a camera cluster are transmitted on these disjoint paths, making it impossible for an eavesdropper to collect all the shares by compromising a small subset of links in the network. Furthermore, we assume that pairwise keys between adjacent visual sensors exist in order to securely communicate intermediate share-generation information.

C. Visual Security and Fidelity Model

It is well known that the human visual and auditory systems can tolerate significant levels of perceptual noise on multimedia data still maintaining the semantics of the content. Using this liberal assumption for visual information, we relax the security requirement of perfect reconstruction of $\bar{I}_R$ at the BS. Following [64] and as shown in Fig. 9, our security and reconstruction requirements are relaxed by defining two image-dependent hyperspheres (defined in the vector space of all images) that are of different radii and centered about the true image. Any point within the smaller hypersphere is considered to be a reasonable representation of the true image, making it possible to understand the image semantics. Any point lying outside the larger hypersphere is considered to be incomprehensible. These relaxed conditions allow for a robust and efficient lightweight distributed privacy design.

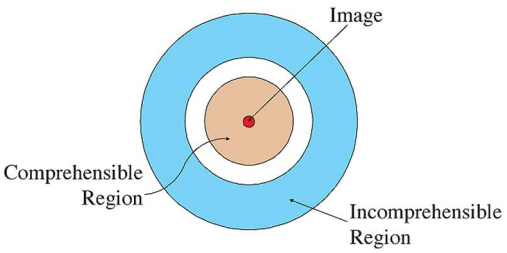


Fig. 9. ***Comprehensible and incomprehensible regions for a particular image in an image space.***

If an eavesdropper's shares collectively provide an image lying in the incomprehensible region, we shall say that the image is still confidential. Not every noisy image in the incomprehensible region will provoke the same level of uncertainty in an attacker; therefore, this scheme shares similar security principles to those of "ramp schemes" proposed by Blakely and Meadows [65].

D. The Distributed Visual Secret Sharing Paradigm

With these requirements in mind, we consider N visual sensor nodes $V_0, V_1, V_2, \ldots, V_{N-1}$ in a DMSN that would like to share N correlated surveillance images modeled as $I_i = \bar{I}_R + W_i$ for $0 \leq i \leq N-1$, where $\bar{I}_R$ is a *representative image* in column-vector form and W_i is random noise modeling imaging variations amongst the different nodes. Our general paradigm detailed in [64] and applied in two different ways in [64] and [66] relies on distributing dynamical systems over the N nodes. An attacker capturing one node only learns part of the system but requires either more knowledge of the system to succeed in breaking one share or simply needs more shares. Specifically, critical parameters are *spread out* across different nodes, so that if some nodes are captured, the critical parameters from these captured nodes do not provide enough information to reveal the secret fully.

In keeping with the FSO networking paradigm, each visual sensor node is assumed to communicate with its neighbor in a unidirectional manner. Pairwise keys between neighboring camera nodes are used to communicate intermediate information.

The paradigm is based on a discrete-time dynamical system Σ_p described by the following state equation:

$$\Sigma_p : \mathbf{x}_{k+1} = f_k(\mathbf{x}_k, \mathbf{u}_k, \mathbf{w}_k). \quad (1)$$

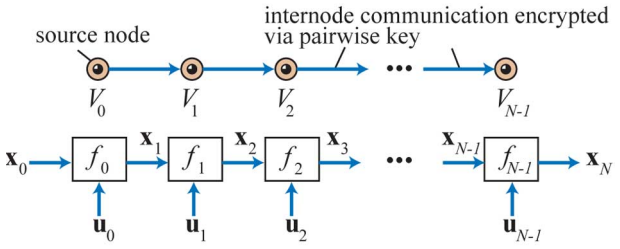


Fig. 10. ***Nodes drive initial state to representative image by controlling a Markov chain dynamical system; the controls represent shares.***

The column vectors $\mathbf{x}_k$, $\mathbf{u}_k$, $\mathbf{w}_k$ represent the state (which is an intermediate signal communicated between visual nodes in our algorithm), external control (which corresponds V_k's share), and random noise, respectively. One node is designated the *source node* (which we denote as V_0) that will start the sharing process. This node is also special because it contains (either through secure communications with the BS or by preloading) an initial state $\mathbf{x}_0$, which is not known by the other nodes, but by the BS. The goal of the visual sensors is to drive the dynamical system starting with the initial state $\mathbf{x}_0$ to the representative state $\bar{I}_R$, using a control law such that the magnitude of each external control is small and the external control's resemblance to the representative image is minimal. Each observing node will, in fact, observe I_i instead of $\bar{I}_R$, so each node must treat its own I_i as $\bar{I}_R$. The difference between each I_i and $\bar{I}_R$ is accounted for through the use of the random vector $\mathbf{w}_k$ in the model. Each node applies its own control independently, given the previous state from its neighbor in the chain; this control is considered to be a share and transmitted to the BS. Fig. 10 depicts this chain-like paradigm. Algorithm 1 summarizes the share generation procedure.

Algorithm 1 Share Generation

Require: Initial state $\mathbf{x}_0$ (known by the BS) loaded into node 0 and partial system f_i for each node i; node i observes I_i, treating it as $\bar{\mathbf{x}}$

Ensure: Shares $\mathbf{u}_i$, $0 \leq i \leq N-1$

1: **for** $k = 0$ to $N-1$ **do**
2: {Each iteration is performed by a different node, i.e., node k}
3: **if** $k \neq 0$ **then**
4: Receive and decrypt $\mathbf{x}_k$ from node $k-1$
5: **end if**
6: $\mathbf{u}_k \Leftarrow g_k(\mathbf{x}_k, \overline{\mathbf{x}})$ {To be designed to drive states to $\overline{\mathbf{x}}$}
7: **if** $k \neq N-1$ **then**
8: $\mathbf{x}_{k+1} \Leftarrow f_k(\mathbf{x}_k, \mathbf{u}_k)$
9: Encrypt and send $\mathbf{x}_{k+1}$ to node $k+1$
10: Destroy $\mathbf{x}_{k+1}$ {So if this node is captured, attacker does not have this}
11: **end if**
12: **if** $k \neq 0$ **then**
13: Destroy $\mathbf{x}_k$ {So if this node is captured, attacker does not have this}
14: **end if**
15: Send $\mathbf{u}_k$ to the BS {This is node k's share}
16: **end for**

The BS receives all shares (i.e., the external controls generated by each node) $\{\mathbf{u}_k\}_{k=0}^{N-1}$, has $\mathbf{x}_0$, and knows the entire dynamical system (i.e., f_k). The BS can then use (1) to retrace the state evolution. The BS does not need to know $\bar{I}_R$; using only knowledge of the shares/controls sent by the nodes, and the entire plant (not fully known to the eavesdropper), the BS can derive $\bar{I}_R$. The final state derived by the BS using controls and plant parameters is approximately equal to $\bar{I}_R$, since this was the design goal of the control law. Algorithm 2 summarizes the reconstruction algorithm used by the BS. Notice that using the initial state $\mathbf{x}_0$, plant parameters f_k, and shares/controls alone suffices for reconstruction.

Algorithm 2 Reconstruction at Base Station

Require: All shares $\mathbf{u}_i$, $0 \leq i \leq N-1$ received by BS(s), and BS(s) have all f_i, $0 \leq i \leq N-1$ and $\mathbf{x}_0$

Ensure $\mathbf{x}_N = \overline{\mathbf{x}}$

1: {Loop performed by a central unit at the BS}
2: **for** $k = 0$ to $N-1$ **do**
3: $\mathbf{x}_{k+1} \Leftarrow f_k(\mathbf{x}_k, \mathbf{u}_k)$
4: **end for**

If a share is missing, or blatantly tampered with (i.e., if the magnitude of that share is too large, violating the goal of a small magnitude control), the BS replaces it with $\mathbf{0}$; this does not dramatically affect the convergence of the state evolution since the controls have a magnitude close to zero, and hence this $\mathbf{0}$ approximation can be seen to be a noisy version of the true control, which can be handled by a robust (i.e., noise-resilient) control law.

E. Illustration of Our Paradigm Using TANGRAM

This framework is demonstrated using two different control laws: MarS in [66] using dynamic programming and TANGRAM in [64] using a random control law, with the latter being more effective security-wise. We shall briefly illustrate TANGRAM now. Here, the system is simple and linear, represented by $\Sigma_p : \mathbf{x}_{k+1} = \mathbf{x}_k + \mathbf{u}_k$. The security comes from the generation of $\mathbf{u}_k$ randomly. The mathematical details can be found in [64]. Intuitively, the share/control $\mathbf{u}_k$, randomly created by node V_k, uses a probability distribution such that when all shares

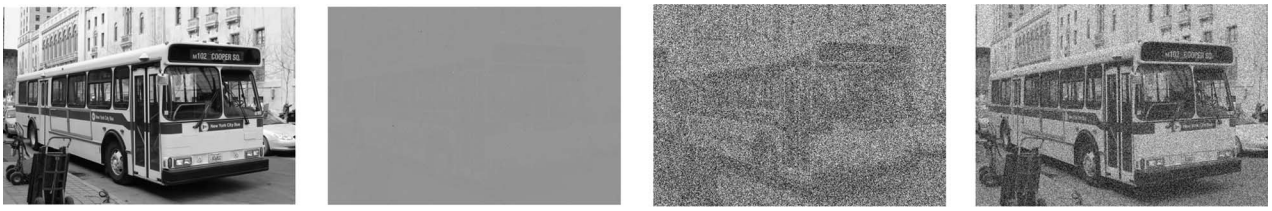


Fig. 11. *(a) Original, (b) sample share, (c) combining ten shares, (d) combining 40 shares.*

are combined, the probability that the resulting image is inside the comprehensible region is high. At the same time, if only a few shares are available to an eavesdropper, the probability that the resulting image from this smaller subset of shares is in the incomprehensible region is also high. These two conditions on the probability distribution give the scheme both reconstructability at the BS as well as visual security, as described earlier. In practice, the exact parameters of the probability distribution need to be determined via simulation depending on how many shares are to be created and how many shares the eavesdropper is allowed to have.

Fig. 11 shows the original bus (come.to/torontobus), a sample share, combining ten shares, and finally combining 40 shares, all for $N = 50$. It can be seen that combining ten shares is very noisy and not very useful to an attacker. On the other hand, if the BS combines 40 shares, it has a workable image.

For a more quantitative analysis, we first empirically determine the thresholds for the comprehensible and incomprehensible regions, based on Euclidean distance. Fig. 12 shows the probability that some number of shares will be in the comprehensible region. Depending on a variance parameter, 40–50 shares are required for the BS to decode. On the other hand, Fig. 13 shows the probability that some number of shares will be in the incomprehensible region. Again, depending on the variance parameter, about 20 shares (Fig. 13) can be captured by the eavesdropper such that the eavesdropper has an image still in the incomprehensible region.

Fig. 14 shows the peak signal-to-noise ratio (PSNR) in decibels as a function of the number of shares combined. This graph shows how the visual quality (in terms of PSNR) improves as a function of the number of shares available. One can see that as more shares are combined, the quality of the reconstruction "ramps up". This result matches with both Figs. 12 and 13 since the comprehensible and incomprehensible regions are determined by fixed thresholds. Therefore, as soon as the PSNR passes the said thresholds, it will transition to the appropriate regions defined by the thresholds creating the performance graphs in Figs. 12 and 13 that jump up to probability one aggressively.

To the best of the authors' knowledge, TANGRAM is the first proposed solution to the problem of distributed visual secret sharing, in which secret parameters, traditionally generated by a single dealer, can now be distributed amongst several nodes without the threat that the capture of a single node will compromise the entire

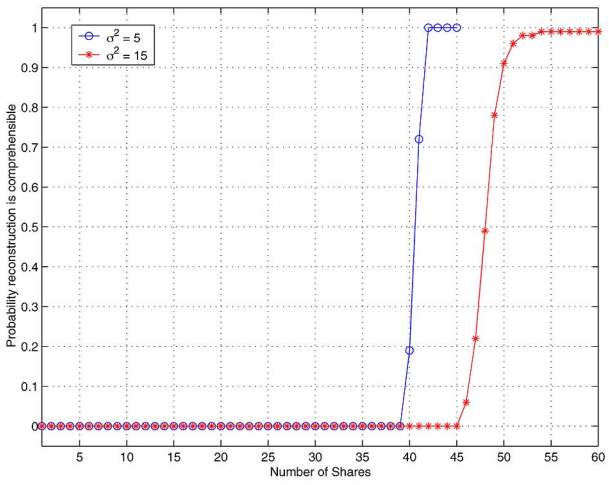


Fig. 12. *Probability that reconstruction with n shares falls in the comprehensible region.*

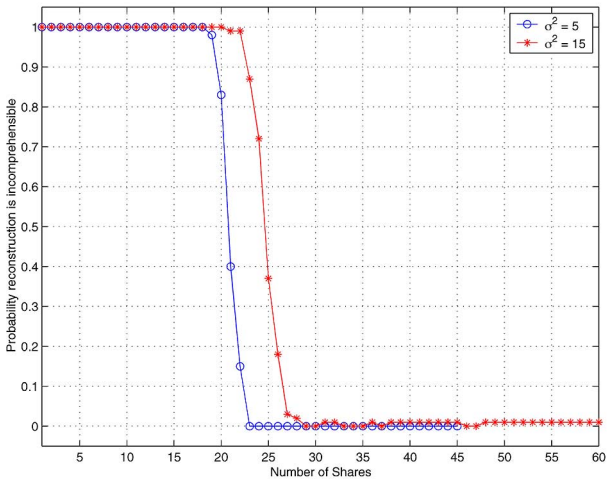


Fig. 13. *Probability that reconstruction with n shares falls in the incomprehensible region.*

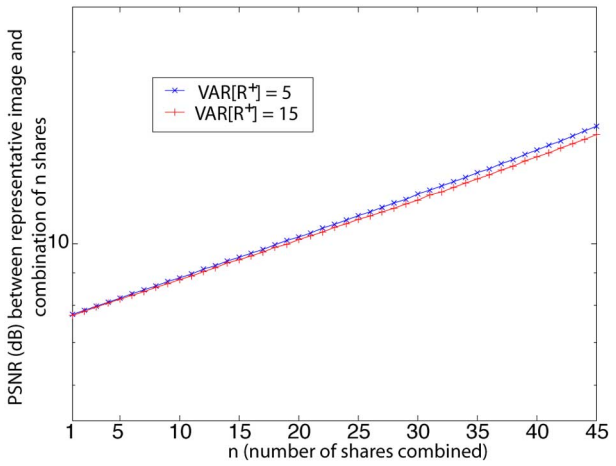


Fig. 14. *PSNR.*

share-generation algorithm. The approach requires limited unidirectional communication between neighbor-hop nodes saving bandwidth. The method of share generation requires simple random number generation and is lightweight. As demonstrated in [64], the shares are much smaller in size than the original image with high probability.

VI. DISTRIBUTED MULTIMEDIA SENSOR NETWORK SECURITY: AN EMERGING FIELD

In the novel *1984*, George Orwell depicts a totalitarian society governed by "Big Brother" in which individuals' lives are dominated by surveillance and controlled through cultural conditioning. Today, widespread surveillance approaches are being explored to protect the rights and to enhance the freedoms of people. To effectively achieve this latter, more holistic goal, it is imperative that both security and privacy issues be simultaneously addressed during the design of such systems. Consider a world in which we can more safely detect, control, or react to natural disasters or terrorist activity through the use of secure lightweight tactical surveillance. Imagine a society in which healthcare for the chronically ill and aging is much more effective and easily accessible by leveraging privacy-enabled state-of-the-art ad hoc broadband information systems.

The research ideas presented in this paper help to reinforce the synergy among signal processing, cryptography, and networking, fostering an interdisciplinary view of protecting modern information systems. Research into protecting DMSN systems is critical to promote the early deployment and long-term adoption of intelligent surveillance mechanisms, revolutionizing the way in which sensor networks can be used for society's benefit. This paper provides a flavor of the research opportunities in the field of DMSN security and privacy. Many open problems still exist and are yet to be discovered. It is the authors' hope that this paper inspires continued research, progress, debate, and increased interaction among the diverse parties involved in the evolution of DMSNs. ■

Acknowledgment

The authors would like to thank Prof. C. K. Madsen, A. Czarlinska, and N. J. Mathai for many useful discussions on the topics of multimedia sensor networks and security, as well as Prof. I. F. Akyildiz for providing a preprint of [19].

REFERENCES

[1] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proc. ACM/IEEE Int. Conf. Mobile Comput. Network.*, Aug. 1999, pp. 263–270.

[2] D. Estrin, L. Girod, G. Pottie, and M. Srivastava, "Instrumenting the world with wireless sensor networks," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, May 2001, vol. 4, pp. 2033–2036.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, pp. 102–114, Aug. 2002.

[4] D. Kundur and W. Luh, "Multimedia sensor networks," in *Encyclopedia of Multimedia*. Berlin, Germany: Springer, 2006.

[5] J. Wickramasuriya, M. Datt, S. Mehrotra, and N. Venkatasubramanian, "Privacy protecting data collection in media spaces," in *Proc. ACM Int. Conf. Multimedia*, New York, Oct. 2004, pp. 48–55.

[6] R. Holman, J. Stanley, and T. Özkan-Haller, "Applying video sensor networks to nearshore environment monitoring," *Pervasive Comput.*, vol. 2, pp. 14–21, Oct.–Dec. 2003.

[7] A. Basharat, N. Catbas, and M. Shah, "A framework for intelligent sensor network with video camera for structural health monitoring of bridges," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Kauai, Hawaii, Mar. 2005, pp. 385–389.

[8] G. Kogut, M. Blackburn, and H. R. Everett, "Using video sensor networks to command and control unmanned ground vehicles," in *Proc. AUVSI Unmanned Syst. Int. Security*, Sep. 2003.

[9] M. Gerla and K. Xu, "Multimedia streaming in large-scale sensor networks with mobile swarms," *ACM SIGMOD Rec.*, vol. 32, no. 32, pp. 72–76, Dec. 2003.

[10] W. C. Feng, J. Walpole, and C. Pu, "Moving towards massively scalable video-based sensor networks," in *Proc. Workshop New Visions Large-Scale Netw.: Res. Applicat.*, March 2001.

[11] J. Pan, Y. T. Hou, L. Cai, Y. Shi, and S. X. Shen, "Locating base-stations for video sensor networks," in *Proc. IEEE Veh. Technol. Conf.*, Orlando, FL, Oct. 2003.

[12] W. C. Feng, B. Code, E. Kaiser, and M. Shea, "Panoptes: A scalable architecture for video sensor networking applications," in *Proc. ACM Int. Conf. Multimedia*, Nov. 2003, pp. 562–571.

[13] B. P. L. Lo, J. L. Wang, and G.-Z. Yang, "From imaging networks to behavior profiling: Ubiquitous sensing for managed homecare of the elderly," in *Adjunct Proc. Int. Conf. Pervasive Comput.*, Munich, Germany, May 2005, pp. 101–104.

[14] D. A. Fidaleo, H.-A. Nguyen, and M. Trivedi, "The networked sensor tapestry (NeST): A privacy enhanced software architecture for interactive analysis of data in video-sensor networks," in *Proc. ACM Int. Workshop Video Surveill. Sensor Netw.*, New York, Oct. 2004, pp. 46–53.

[15] K. Obraczka, R. Manduchi, and J. J. Garcia-Luna-Aveces, "Managing the information flow in visual sensor networks," in *Proc. Int. Symp. Wireless Pers. Multimedia Commun.*, Oct. 2002, pp. 1177–1181.

[16] M. Chu, J. Reich, and F. Zhao, "Distributed attention in large scale video sensor networks," *Inst. Elect. Eng. Intell. Distrib. Surveill. Syst.*, pp. 61–65, Feb. 2004.

[17] C.-F. Chiasserini and E. Magli, "Energy consumption and image quality in wireless video-surveillance networks," in *Proc. IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2002, pp. 2357–2361.

[18] R. Lienhart and I. Kozintsev, "Self-aware distributed av sensor and actuator networks for improved media adaptation," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jun. 2004, pp. 2131–2134.

[19] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Comput. Netw.*, Mar. 2007.

[20] 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. Mobile Comput. Network.*, Seattle, WA, Aug. 1999, pp. 271–278.

[21] J. Llorca, A. Desai, U. Vishkin, C. Davis, and S. Milner, "Reconfigurable optical wireless sensor networks," in *Proc. SPIE Opt. Atmos. Propag. Adapt. Systems VI*, J. D. Gonglewski, and K. Stein, Eds., Barcelona, Spain, Feb. 2004, vol. 5237, pp. 136–146.

[22] J. Díaz, J. Petit, and M. Serna, "A random graph model for optical networks of sensors," *IEEE Trans. Mobile Comput.*, vol. 2, pp. 186–196, Jul.–Sep. 2003.

[23] J. Díaz, J. Petit, and M. Serna, "Random scaled sector graphs," Dept. de Llenguatges i Sistemes Informàtics, Univ. Politècnica de Catalunya, Barcelona, Spain, Tech. Rep. LSI-02-47-R, 2002.

[24] C. Alvarez, J. Díaz, J. Petit, J. Rolim, and M. Serna, "Efficient and reliable high level communication in randomly deployed wireless sensor networks," in *Proc. ACM Workshop Mobility Manag. Wireless Access*, Philadelphia, PA, Sep.–Oct. 2004, pp. 106–110.

[25] U. N. Okorafor and D. Kundur, "Efficient routing protocols for a free space optical sensor network," in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst.*, Washington, DC, Nov. 2005, pp. 251–258.

[26] U. N. Okorafor and D. Kundur, "OPSENET: A security enabled routing scheme for a system of optical sensor networks," in *Proc. Int. Conf. Broadband Commun., Netw., Syst. (BROADNETS)*, San Jose, CA, Oct. 2006.

[27] U. N. Okorafor, K. Marshall, and D. Kundur, "Security and energy considerations for routing in hierarchical optical sensor networks," in *Proc. 2nd Int. Workshop Wireless Sensor Networks Security*, Vancouver, BC, Canada, Oct. 2006.

[28] D. Kundur, U. N. Okorafor, and W. Luh, "Heterogeneous lightweight sensornets for trusted visual computing," in *Proc. IEEE Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Pasadena, CA, Dec. 2006.

[29] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Proc. ACM Int. Conf. Mobile Comput. Network.*, Jul. 2001, pp. 189–199.

[30] J. Undercoffer, S. Avancha, A. Joshi, and J. Pinkston, "Security for sensor networks," in *Proc. CADIP Res. Symp.*, 2002. [Online]. Available: http://www.scholar.google.com/url?sa=U&q=http://www.csee.umbc.edu/cadip/2002Symposium/sensor-ids.pdf

[31] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *Proc. ACM Conf. Embedded Netw. Sensor Syst.*, 2004.

[32] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM Conf. Comput. Commun. Security*, Nov. 2002, pp. 41–47.

[33] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Security Privacy*, May 2003, pp. 197–213.

[34] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *Proc. ACM Conf. Comput. Commun. Security*, Washington, DC, Oct. 2003, pp. 62–72.

[35] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. ACM Conf. Comput. Commun. Security*, Washington, DC, Oct. 2003, pp. 52–61.

[36] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in *Proc. ACM Int. Conf. Embedded Netw. Sensor Syst.*, Nov. 2003, pp. 255–265.

[37] D. Wagner, "Resilient aggregation in sensor networks," in *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks*, Washington, DC, Oct. 2004, pp. 78–87.

[38] B. Krishnamachari and S. S. Iyengar, "Efficient and fault-tolerant feature extraction in wireless sensor networks," in *Proc. Workshop Inf. Process. Sensor Netw.*, Palo Alto, CA, Apr. 2003, pp. 488–501.

[39] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in *Proc. ACM Workshop Security Ad Hoc Sensor Netw.*, Washington, DC, Oct. 2004.

[40] A. Czarlinska and D. Kundur, "Distributed actuation attacks in wireless sensor networks: Implications and countermeasures," in *Proc. IEEE Workshop Depend. Security Sensor Netw. Syst.*, Columbia, MD, Apr. 2006, pp. 3–12.

[41] S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hod networks," in *Proc. Euromicro Workshop Parallel, Distrib.Netw.-Based Process.*, Canary Islands, Spain, 2002, pp. 403–410.

[42] L. Hu and D. Evans, "Secure aggregation for wireless networks," in *Proc. IEEE Symp. Applicat. Internet/Workshop Security Assurance Ad Hoc Netw*, Jan. 2003, pp. 384–391.

[43] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. IEEE Int. Workshop Sens. Netw. Protocols Applicat.*, May 2003, pp. 113–127.

[44] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in *Proc. Symp. Inf. Process. Sens. Netw.*, Berkeley, CA, 2004, pp. 259–268.

[45] F. A. P. P. S. Katzenbeisser, Ed., *Information Hiding Techniques for Steganography and Digital Watermarking*. Reading, MA: Artech House, 2000.

[46] W. Zeng, J. Lan, and X. Zhuang, "Security architectures and analysis for content adaptation," in *Proc. SPIE Security, Steg., Watermark. Multimedia Contents VII*, San Jose, CA, Jan. 2005, pp. 84–95.

[47] W. Dabbous, E. Duros, and T. Ernst, "Dynamic routing in networks with unidirectional links," in *Proc. 2nd Int. Workshop Satellite-Based Inf. Services*, Budapest, Hungary, Oct. 1997, pp. 35–47.

[48] S. Nesargi and R. Prakash, "A tunneling approach to routing with unidirectional links in mobile ad-hoc networks," in *Proc. IEEE Int. Conf. Comput. Commun. Netw.*, Las Vegas, NV, Oct. 2000, pp. 522–527.

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

[50] M. K. Marina and S. R. Das, "Routing performance in the presence of unidirectional links in multihop wireless networks," in *Proc. ACM Int. Symp. Mobile Ad Hoc Network. Comput.*, Lausanne, Switzerland, Jun. 2002, pp. 12–23.

[51] V. Ramasubramanian and D. Mosse, "Statistical analysis of connectivity in unidirectional ad hoc networks," in *Proc. Int. Conf. Parallel Process. Workshops*, Aug. 2002, pp. 109–115.

[52] A. Saha and D. B. Johnson, "Routing improvements using directional antennas in mobile ad hoc networks," in *Proc. IEEE Global Telecommun. Conf.*, Dallas, TX, Nov.–Dec. 2004, pp. 2902–2908.

[53] T. Ernst and W. Dabbous, "A circuit-based approach for routing in unidirectional links networks," Institut National de Recherche en Informatique et en Automatique, Tech. Rep. INRIA Res. Rep. 3292, Nov. 1997.

[54] F. C. M. Lau, G. Chen, H. Huang, and L. Xie, "A distance-vector routing protocol for networks with unidirectional links," *Comput. Commun.*, vol. 23, no. 4, pp. 418–424, 2000.

[55] W. Lou and J. Wu, "A multi-path routing protocol for unidirectional networks," in *Proc. Int. Conf. Parallel Distrib. Process. Tech. Applicat.*, Las Vegas, NV, Jun. 2001, pp. 2021–2027.

[56] Y. Zhang and W. Lee, "Intrusion detection techniques for mobile wireless networks," *ACM/Kluwer Wireless Netw. J.*, vol. 9, no. 5, pp. 545–556, Sep. 2003.

[57] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Commun.*, vol. 11, pp. 38–43, Dec. 2004.

[58] A. Sprintson, I. Guerrero, J. Welch, and S. Rajsbaum, "Applications of network coding in distributed computing," in *Proc. 21st Int. Symp. Distrib. Comput.*, Lemesos, Cyprus, 2007.

[59] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[60] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. Inf. Theory*, vol. IT-29, pp. 35–41, Jan. 1983.

[61] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. Inf. Theory*, vol. IT-32, pp. 387–393, May 1986.

[62] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory*, vol. 43, pp. 827–835, May 1997.

[63] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Adv. Cryptol.—EUROCRYPT '94: Workshop Theory Applicat. Crypto. Tech.*, 1995, pp. 1–12.

[64] W. Luh, D. Kundur, and T. Zourntos, "A novel distributed privacy paradigm for visual sensor networks based on sharing dynamical systems," *EURASIP J. Appl. Signal Process. (Special Issue on Visual Sensor Networks)*, to be published.

[65] G. R. Blakley and C. Meadows, "The security of ramp schemes," *in Proc. Adv. Cryptol. (CRYPTO '84)*, vol. 196, *Lecture Notes in Computer Science*, G. R. Blakley, and D. Chaum, Eds., 1985, pp. 242–268.

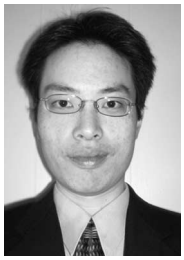
[66] W. Luh and D. Kundur, "Distributed privacy for visual sensor networks via markov shares," in *Proc. 2nd IEEE Workshop Depend. Security Sens. Netw. Syst.*, Columbia, MD, Apr. 2006, pp. 23–34.

ABOUT THE AUTHORS

Deepa Kundur (Senior Member, IEEE) received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively.

In 2003, she joined the Department of Electrical and Computer Engineering, Texas A&M University, College Station, where she is currently an Associate Professor and leads the Sensor Media Algorithms and Networking for Trusted Intelligent Computing (SeMANTIC) Research Group, Wireless Communications Laboratory. Her research interests include security and privacy for scalar and broadband sensor networks, multimedia security, digital rights management, and steganalysis for computer forensics. She has given tutorials in the area of information security at ICME-2003 and Globecom-2003. She is an Associate Editor of *EURASIP Journal on Information Security*.

Prof. Kundur was a Guest Editor of the June 2004 PROCEEDINGS OF THE IEEE Special Issue on Enabling Security Technologies for Digital Rights Management. She is currently Vice Chair of the Security Interest Group, IEEE Multimedia Communications Technical Committee, and an Associate Editor of the IEEE TRANSACTIONS ON MULTIMEDIA and IEEE COMMUNICATION LETTERS.



William Luh (Student Member, IEEE) received the B.A.Sc. degree in computer engineering from the University of Toronto, Toronto, ON, Canada, in 2002 and the M.S. degree in electrical engineering from Texas A&M University, College Station, in 2004, where he is currently pursuing the Ph.D. degree in electrical engineering.

His research interests include multimedia and sensor network security and information-theoretic security.

Unoma Ndili Okorafor (Student Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Lagos, Nigeria, in 1998 and the M.Sc. degree in electrical and computer engineering department from Rice University, Houston, TX, in 2001. She is currently pursuing the Ph.D. degree in the Electrical and Computer Engineering Department, Texas A&M University, College Station.

Her research interests include secure routing and connectivity analysis for directional and broadband wireless sensor networks.

Ms. Okorafor is a Student Member of SPIE, NSBE, and SWE. She received a Sloan Foundation Fellowship for minority Ph.D. students and the AAUW Engineering Dissertation Fellowship.

Takis Zourntos (Member, IEEE) was born in Hamilton, ON, Canada. He received the B.A.Sc., M.A.Sc., and Ph.D. degrees from the University of Toronto, Toronto, ON.

He is currently an Assistant Professor in electrical and computer engineering at Texas A&M University, College Station. His research is centered on the application of nonlinear systems and control theory to a wide range of problems, including behavior generation for autonomous agents, integrated analog circuits, and signal processing. He is a Licensed Professional Engineer with the Province of Ontario.