HoLiSTiC: Heterogeneous Lightweight Sensornets for Trusted Visual Computing

Deepa Kundur, Unoma Ndili Okorafor and William Luh
Department of Electrical & Computer Engineering
{deepa, unondili, luh} @ece.tamu.edu

Abstract

This paper introduces a novel "HoLiSTiC" framework for visual sensor networks (VisSNs) and studies security issues within this context. The HoLiSTiC paradigm, which encompasses many existing VisSN proposals, effectively exploits heterogeneous wireless sensing and communications for more flexible, practical and scalable visual surveillance. Security aspects of HoLiSTiC are considered by highlighting open research problems. Secure routing issues in unidirectional optical free-space sensor networks that form the foundation of the HoLiSTiC transport network are discussed. In addition, a novel distributed security paradigm based on independent media sharing is presented to demonstrate how the interaction of signal processing, networking, and cryptography can benefit VisSNs.

1 Introduction

Wireless sensor networks (WSNs) are comprised of unattended groups of sensors that observe, communicate wirelessly, coordinate and actuate to collectively achieve high-level tasks within an observation environment. WSNs must be densely distributed, collaborative, autonomous, hierarchical, and secure. VisSNs are a class of WSN in which a subset of the nodes collect visual data. Such perceptually rich data is more accessible to human *sinks* for greater interactivity. For applications such as healthcare surveillance and environmental monitoring visual data provides crucial signatures. In addition, VisSNs are a convenient framework to interface emerging scalar WSNs with existing video surveillance infrastructure.

The objective of this paper is two-fold. First, we introduce a new class of VisSNs entitled Heterogeneous Lightweight Sensornet for Trusted Visual Computing (HoLiSTiC) that applies to [1, 4] and generalizes [5] existing VisSN proposals. Second, through introduction of the HoLiSTiC framework we identify two open research problems that demonstrate the growing need for research in securing such systems.

2 The HoLiSTiC Paradigm

We consider the following HoLiSTiC setting that encompasses the salient features of many proposed VisSNs in the research literature. Specifically, the paradigm, incorporates the necessary high speed wireless networking between communicating nodes [2, 4] via free space optical (FSO) communications [6]. In addition, heterogeneity, commonly observed in VisSN proposals [1, 4], is employed such that network elements fall in classes with distinct power, sensing and communication capabilities for improved scalability and energy management.

Fig. 1 summarizes the basic network model. All nodes are wireless for ease of (re-)deployment. Three types of network entities are assumed to exist: 1) a powerful wireless trusted BS that initiates network set-up, maintains secure system operation, and is directly connected to the network *sink*; 2) static digital camera nodes that acquire (event-driven) visual data and have basic image processing capabilities including compression; 3) wireless static homogeneous transport nodes having FSO communication capability as modeled in [6]. As demonstrated by recent VisSN proposals, the natural hierarchy of this setup is essential for scalability given the high bandwidth of the sensed visual data [2]. The predominant traffic patterns occur between each transport node and the BS for network maintenance, from each camera to the BS for data transport, and between adjacent cameras for coordination.

There are compelling research efforts that demonstrate the potential of FSO communications for broadband WSNs that can transmit video [6]. The FSO transport subnet receives data from the cameras and leverages the BS for secure networking. The associated nodes are randomly and densely deployed for convenience and connectivity.

2.1 Security and Privacy

Ensuring security and privacy of VisSNs is crucial to achieving wide-spread use. An effective solution requires that protection mechanisms be designed during system inception. A distinguishing assumption in threat models of WSNs is the possibility of insider attack; the rationale is that the physical vulnerability of the low-cost nodes allows attackers to access secret keying information to effectively deploy alien nodes or corrupt existing nodes. The corruption of even a single node has the potential to cause significant network damage [7]. Conventional security primitives cannot adequately function when keying information is lost creating a need to study novel approaches of security.

Proceedings of the 2006 International Conference on Intelligent
Information Hiding and Multimedia Signal Processing (IIH-MSP'06)
0-7695-2745-0/06 $20.00 © 2006 IEEE

The high levels of redundancy and irrelevancy within VisSN systems provides a rich environment to explore solutions that effectively integrate signal processing and networking. The redundancy, designed originally for fault-tolerance, can be exploited, in part, to protect against forms of denial-of-service (DoS) attacks. The irrelevancy, characteristic of visual data (which is 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.

This paper introduces the following open research problems, particular to securing VisSNs, within the HoLiSTiC context: 1) secure routing challenges for the FSO transport subnet, and 2) secret sharing approaches applied at the VSs for distributed trust and privacy.

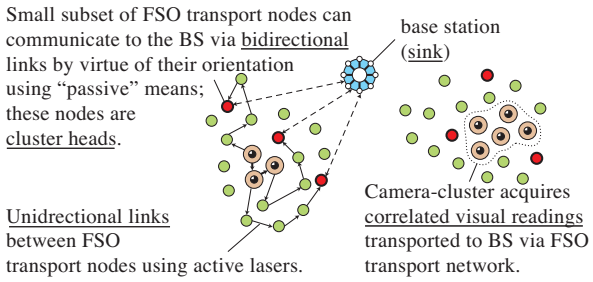

Figure 1. HoLiSTiC Model.

3 Secure Routing in the FSO Subnet

One open avenue of research involves securing the FSO transport subnet. FSO transmission is characterized, in part, by directionality of communications. These requirements are elucidated in Fig. 2(a) where node S_i is arbitrarily deployed scanning an angle of α degrees (where $\alpha \leq 40°$ in practice) via a radius of communication r to communicate with another node S_j (with omnidirectional receiving capability) that lies within the communicating sector highlighted. This forms a one-way communication link from S_i to S_j. Because of the angle of S_j, it is clear from Fig. 2(a) that S_j cannot communicate directly back to S_i.

This unidirectional communication model creates a network topology that can be modeled as a directed random scaled sector graph [3] shown in Fig. 2(b). Here, it is clear that S_j can communicate back to S_i via other network nodes. It has been found experimentally that if node density is great enough, a return path is very likely [3].

The FSO nodes as modeled in [3, 6, 11, 12] contain active laser and passive corner cube retro-reflector (CCR) hardware for communications. Internode communicate is active. Those FSO nodes with CCRs facing the BS communicate with the BS bidirectionally via passive means taking on the role of cluster heads (CHs); this creates a hierarchical architecture as illustrated in Fig. 1.

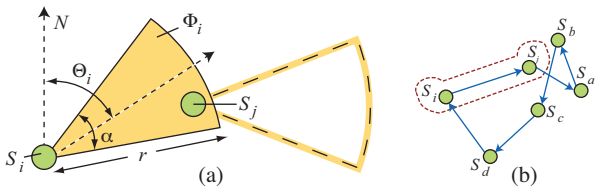

Figure 2. Random scaled sector graph model.

Application of traditional approaches for bidirectional or mixed unidirectional/bidirectional RF networks are inappropriate for primarily unidirectional link networks, such as in HoLiSTiC, because of the high overhead from network asymmetry and multihop reverse routes.

In [11, 12], Okorafor and Kundur have developed novel heuristics and algorithms for efficient topology discovery in an event-based hierarchical FSO sensor network. The method incorporates a new *circuit-based* approach to routing to account for the natural hierarchy and prevalent traffic between nodes and BS in the FSO network. Fig. 3 illustrates the proposed notion of a *BS-circuit*, which is a sequence of unidirectional links between transport nodes with a path leading away from and back to the BS (via CHs), thus forming a directed loop. The BS-circuit provides each associated node with a uplink and downlink path to and from the BS, respectively. Topology discovery identifies BS-circuits 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 forwards them back to the BS.

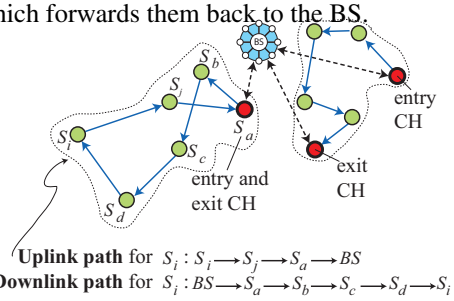

Figure 3. Two Possible BS-circuits.

After the BS obtains the beacons, it can form an approximate network topology and is responsible for determining the most promising routing paths. In order to select specific circuits for routing (either single or multiple for more robust routing), specific BS-circuits must be selected from those identified. Some of the identified paths may be more vulnerable to routing attacks than others due to factors such as geographical placement or centrality. For this reason, one open research problem is to employ an energy- and security-aware cost function for route selection of, say, the form:

$$\mu(B_i^*) = \frac{\sum_{S_j \in B_i^*} E_{ij}}{\sum_{S_j \in B_i^*} \Gamma ij} \qquad (1)$$

where B_i^* is a BS-circuit for S_i, and E_{ij} and Γij are the transmission energy/bit and *trust factor* for the link from S_i to S_j, respectively. One idea is to assign a value to Γij as a function of the centrality of node S_j; the philosophy is that

Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06)
0-7695-2745-0/06 $20.00 © 2006 IEEE

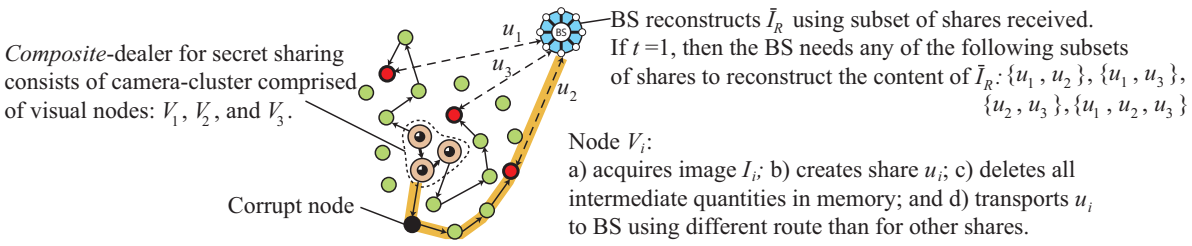

Figure 4. Distributed share generation, transport and reconstruction at the BS (for t=1).

an attacker prefers to target nodes that are more connected within the network lowering its trust.

Another promising area of work is to identify practical methods to reroute packets in the face of mild topological changes due to addition of nodes or identification of corrupt/dead nodes. Theoretical connectivity analysis of such networks will also provide useful design insights for practical deployment of such systems.

4 Visual Secret Sharing for Distributed Privacy

Another novel security problem in VisSNs involves visual security in the presence of insider attacks. Consider a camera-cluster of N densely deployed visual sensor (VS) nodes, denoted V_i, $i = 0, 1, \ldots, N-1$ that communicate via FSO. Node V_i captures $P_x \times P_y$ grayscale image I_i. Due to the dense deployment, the images $I_i, \forall i$ are correlated; this is modeled as, $I_i = \overline{I}_R + W_i$ where $\overline{I}_R$ is a *representative image* of the scene, and W_i is random noise modeling imaging variations among the different VSs.

Each VS encrypts its content transmitting the result to the BS. To overcome insider (node corruption) attacks that allow trivial eavesdropping, this work focuses on distributing trust. One traditional approach to distributing trust is threshold *secret sharing* (SS). Here, a secret originating from one source, the *dealer*, is separated into N distinct *shares* such that for a fixed $t < N$, $\geq t+1$ shares can be combined to produce the original secret. Similarly, a digital image can be separated using *visual secret sharing* [10], in which $\leq t$ shares cannot reveal the semantics of the image, but $\geq t+1$ can reconstruct a salient approximation.

In [8, 9], Luh and Kundur adapt the spirit of SS for distributed VisSNs such that shares are created by a composite-dealer comprised of the set of camera-cluster VSs (using limited internode communication). This way, if $\leq t$ shares are intercepted by an attacker during transport to the BS, it is not possible to determine $\overline{I}_R$. At the same time, if $\leq t$ VSs are physically captured (revealing cryptographic keys) or stop working, content privacy and reconstruction at the BS are possible. In Fig. 4, node V_i encypts I_i resulting in the share u_i, which is sent to the BS via a route R_i that is physically distinct from all other shares' paths. For $t = 1$, the corrupt node eavesdrops to obtain u_2, which is insufficient to determine $\overline{I}_R$. Moreover, if the corrupt node severs the highlighted route via a blackhole attack, the two remaining shares received at the BS are sufficient to reconstruct $\overline{I}_R$.

In keeping with the FSO networking paradigm, the VSs are assumed to communicate with one another in a unidirectional fashion that forms a *chain-like* structure shown in Fig. 5. This relationship can be guaranteed with careful camera deployment. Direct neighbors in this chain are assumed to have *pairwise keys* for secure communications.

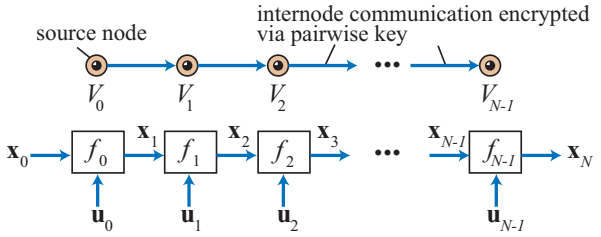

Figure 5. Chain-like Paradigm.

The chain-like structure lends itself to evolutionary algorithms that make use of state equations of dynamical systems. Such systems are privileged with well-known control methods that are robust to noise modeling inexact camera calibration and DoS attacks. Dynamical systems can be used for low-cost algorithm design, provide robustness to incidental error and intentional DoS attack on a subset of the nodes, and provide a framework in which to design algorithms that provide compromises amongst competing objectives such as compression and security.

A discrete-time dynamical system Σ_p is described by the following state equation:

$$\Sigma_p : \quad \mathbf{x}_{k+1} = f_k(\mathbf{x}_k, \mathbf{u}_k, \mathbf{w}_k) \tag{2}$$

The $P_x \cdot P_y \times 1$ column-vectors $\mathbf{x}_k$, $\mathbf{u}_k$ and $\mathbf{w}_k$ are the state, external control (representing the share generated by V_k), and random noise, respectively. The camera-cluster agrees ahead of time on a starting VS, called the *source node* that contains a randomly generated initial state $\mathbf{x}_0$ that is independent of $\overline{I}_R$ either through pre-programming or some key distribution protocol. Node V_i is given information only about f_i and $\mathbf{x}_i$ (the latter via encrypted internode communication). From this information, a control $\mathbf{u}_i$ (which is a vector representing the share u_i of V_i) is computed with the goal of driving the state in the next iteration $\mathbf{x}_{i+1}$ (generated by V_{i+1}) closer to the desired representative state $\overline{\mathbf{x}}_R$

Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06)
0-7695-2745-0/06 $20.00 © 2006 IEEE

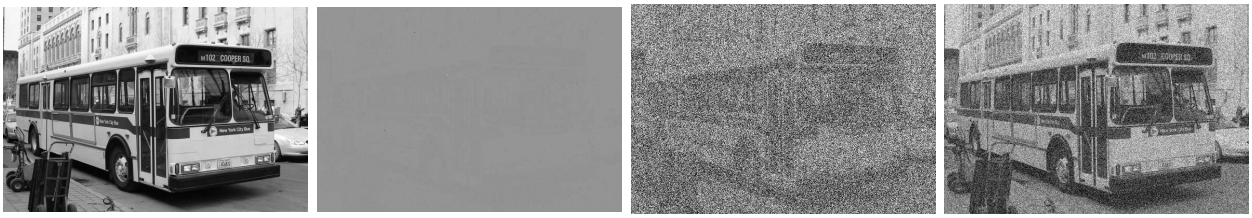

Figure 6. (a) Original; (b) sample share; (c) decryption via 10 shares; (d) decryption via 40 shares.

(the column-wise vector representing $\overline{I}_R$). This is done in the presence of constraints that reduce the size of the shares and obfuscate the signal to facilitate security without significant bandwidth expansion.

Given knowledge of $\mathbf{x}_0$, the BS builds an estimate of $\overline{I}_R$ by repeatedly applying the subset of shares received (from the overall set $\{\mathbf{u}_k\}$, $k = 0, 2, \ldots, N-1$) to drive the state from $\mathbf{x}_0$ to $\mathbf{x}_N$, an approximation of $\overline{\mathbf{x}}_R$. When a share is not known, it is substituted with $\mathbf{0}$. The technique is naturally robust; it can be proven that absence or tampering of $\leq t$ shares guarantees a reasonable reconstruction of $\overline{I}_R$ [9].

To demonstrate the potential of this framework for effective algorithm synthesis, the Luh and Kundur have designed two algorithms for distributed VisSN privacy called MarS [8] and TANGAM [9]. This involves designing Σ_p as well as a cost function incorporating the competing system objectives of security and compression that provides a methodology to compute the shares. Results for $N = 60$ and the following lightweight system: $\Sigma_p : \mathbf{x}_{k+1} = \mathbf{x}_k + \mathbf{u}_k$ (where $\mathbf{u}_k = -\text{sgn}(\mathbf{x}_k - \overline{\mathbf{x}}) \odot \mathbf{R}_k^+$ and the $P_x \cdot P_y \times 1$ vector $\mathbf{R}_k^+$ has randomly generated elements with mean less than $\epsilon \cdot 2|\mathbf{x}_k - \overline{\mathbf{x}}|$) demonstrate that for a reasonable fraction of shares, reconstruction of a perceptual approximation of $\overline{I}_R$ is likely [9]. Figure 6 shows the original bus image (© come.to/torontobus) $\overline{I}_R$ along with a typical share produced by one VS. Also shown is reconstruction at the BS using 10 shares versus 40 shares. Thus, an attacker who has compromised ≤ 10 nodes or who has accessed ≤ 10 shares will not be able to decrypt an intelligible signal. In the presence of a DoS attack in which approximately 20 shares are lost, reconstruction at the BS is still possible.

Open research problems involve selecting parameters and functions for this paradigm that provide improved results for practical VisSN systems. For example, system design for improved obfuscation for higher levels of visual security is of interest. In addition, integrating the paradigm into well-known compression standards, an essential requirement in VisSNs, is critical.

5 Conclusions

This paper presents the HoLiSTiC paradigm for visual sensor networking. VisSN security presents a rich research environment for creative solutions that integrate signal processing, networking and cryptography.

References

[1] 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 International Conference on Pervasive Computing and Communications Workshops*, pages 385–389, Kauai Island, Hawaii, March 2005.

[2] W. c. Feng, J. Walpole, W. c. Feng, and C. Pu. Moving towards massively scalable video-based sensor networks. In *Proc. Workshop on New Visions for Large-Scale Networks: Research and Applications*, March 2001.

[3] J. Díaz, J. Petit, and M. Serna. A random graph model for optical networks of sensors. *IEEE Transactions on Mobile Computing*, 2(3):186–196, July-September 2003.

[4] M. Gerla and K. Xu. Multimedia streaming in large-scale sensor networks with mobile swarms. *ACM SIGMOD Record*, 32(32):72–76, December 2003.

[5] R. Holman, J. Stanley, and T. Őzkan-Haller. Applying video sensor networks to nearshore environment monitoring. *IEEE Pervasive Computing*, 2(4):14–21, October-December 2003.

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

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

[8] W. Luh and D. Kundur. Distributed privacy for visual sensor networks via markov shares. In *2nd IEEE Workshop on Dependability and Security in Sensor Networks and Systems*, pages 23–34, Columbia, Maryland, April 2006.

[9] W. Luh, D. Kundur, and T. Zourntos. A novel distributed privacy paradigm for visual sensor networks based on sharing dynamical systems. *EURASIP Journal on Applied Signal Processing, Special Issue on Visual Sensor Networks*, to appear late 2006.

[10] M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology - EUROCRYPT '94. Workshop on the Theory and Application of Cryptographic Techniques. Proceedings*, pages 1 – 12, 1995.

[11] U. N. Okorafor and D. Kundur. Efficient routing protocols for a free space optical sensor network. In *Proc. IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pages 251–258, Washington, DC, November 2005.

[12] U. N. Okorafor and D. Kundur. Opsenet: A security enabled routing scheme for a system of optical sensor networks. In *Proc. International Conference on Broadband Communications, Networks, and Systems (BROADNETS)*, San Jose, California, October 2006.

Proceedings of the 2006 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06)
0-7695-2745-0/06 $20.00 © 2006 IEEE