# G-E-M Sensor Networks for Mission Critical Surveillance in Hostile Environments

Alexandra Czarlinska
Electrical & Computer Engineering
Texas A&M University, CS-TX
email: czlinska@ece.tamu.edu

William Luh
Electrical & Computer Engineering
Texas A&M University, CS-TX
email: luh@ece.tamu.edu

Deepa Kundur
Electrical & Computer Engineering
Texas A&M University, CS-TX
email: deepa@ece.tamu.edu

***Abstract*—The gathering of surveillance data such as visual intelligence from potentially hostile areas has long played a pivotal role in attaining various safety and security objectives. The methodology of gathering such surveillance is increasingly shifting towards rapid-deployment autonomous networks that limit the need for human exposure, and that cover large unattended areas while operating over extended periods of time. To achieve the surveillance objectives, such networks must be dependable and secure even in the presence of a potentially hostile counter-surveillance opponent. In this work we explicitly model and consider the presence of such an opponent in the form of a hostile sensor network with eavesdropping and actuation capabilities. We present a methodology for addressing the security and dependability issues arising in such extreme settings, which we collectively refer to as *G-E-M*. Specifically, we wish to ensure the legitimacy and authenticity of the *gathered* (*G-E-M*) visual surveillance in the presence of a hostile network engaged in stealthy disinformation activities. We also wish to ensure that the collected surveillance can be *encrypted* (*G-E-M*) for transmission even if keys between the nodes and the sink are temporarily compromised or otherwise unavailable. Finally we wish to ensure that the network design both inherently prolongs the lifetime of the network and also *mitigates* (*G-E-M*) deliberate energy drains. These issues are not typically examined collectively though the dependability of all these components is required to maintain the functionality and longevity of the network. Though developed and presented for the case of an attacker in the form of a hostile network, the methodologies have applicability to networks with a subset of subverted nodes that behave maliciously.**

## I. Introduction and Motivation

The accurate and timely gathering of visual surveillance and intelligence data has long played a central role in attaining objectives that secure public interests and safety. Motivated by current security challenges and technological developments, the gathering of such data is increasingly shifting towards the use of unattended aerial or remote ground networks [1]. The use of such distributed networks limits the need for human exposure while allowing coverage of large and potentially hostile areas over extended periods of time.

To achieve the remote visual surveillance objective, in this work we consider a rapid-deployment heterogeneous ground sensor network. The network is comprised of untethered (wireless-transmission and battery-operated) camera nodes and scalar sensors. Importantly, the network is deployed over a vast area where one or more of the zones may contain a hostile opponent. The surveillance network must thus remain dependable and secure despite disruption and disinformation activities caused by the hostile opponent in this mission critical setting [2], [3].

In this work we explicitly consider the potential availability and use of sensor-actuator networks for hostile disruption activities by an opponent. The use of such sensor-actuator networks may enable new disruption and counter-intelligence possibilities for the attacker [3]. In particular, actuation enables distributed attacks that do not require the physical destruction or jamming of nodes thus enabling attacks that are *stealthy*. In such settings we may no longer assume that the gathered data is legitimate (despite node redundancy), that loss of encryption keys does not disrupt the surveillance mission [4], and that a hostile opponent will not drain the legitimate network's energy deliberately [5]. Based on these considerations, the specific goals of the mission critical sensor network for dependable and secure surveillance are summarized below and collectively referred to as *G-E-M*:

- **G: Gather** authentic and legitimate surveillance data. The network must be able to collect relevant surveillance data even in the presence of a hostile distributed attacker. The hostile attacker may be engaged in disinformation and disruption activities to cause relevant intelligence to be omitted or to lead to the gathering of irrelevant data.
- **E: Encrypt** acquired surveillance data. The network must be able to transmit the acquired surveillance securely (with confidentiality) even if encryption keys between the nodes and the base station are temporarily unavailable or otherwise compromised [4].
- **M: Mitigate** network failure due to resource exhaustion. The network must be able to *inherently* mitigate energy drain caused by the gathering and transmission of *visual* surveillance data *and* to mitigate deliberate energy drain caused by a hostile attacker that may be present in the environment.

### A. Focus & Differences From Prior Work

In this work we present and overview an overall methodology for addressing the *G-E-M* objectives in the presence of a hostile attacker. To secure the data gathering process (*G*), we employ an optimal Neyman-Pearson detector supplemented

This work is supported in part by NSF grants ECCS-0735114 and EEC-0649142 and the Texas Higher Education Board grant.

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

with game theoretic analysis as in [3] to enable study of the attack. However this paper focuses on the previously unexplored relationship between attack *mitigation* and *detection*. The resulting trade-offs are important for system design as well as for energy-drain mitigation ($M$). To achieve encryption ($E$) when keys are unavailable, we employ a keyless scheme based on coding theory that has been extensively developed in [6]. Importantly, the scheme of [6] applies to correlated scalar data and is not readily applicable to images. Thus in this work we develop and test an algorithm that *enables* use of this scheme for *visual* surveillance. The scheme is fully compatible with key-based protocols and is primarily intended for use during times of key unavailability. The scheme mitigates ($M$) energy drain by providing a *distributed* solution that eliminates the need for communication among the nodes and by offering a trade-off between reconstruction quality and redundancy. Thus the proposed *overall* methodology aims to address the fundamental issues of dependable data *gathering* and *encryption*. These issues are not typically studied together though the dependability of both components is collectively required to guarantee the functionality and longevity of the network.

## II. Background

In this work we wish to complement current research interests into the *security* and *dependability* of visual sensor networks [1], [7], [8] in mission critical settings and *hostile* environments [2], [3] over *extended* periods of time [9]. To provide cryptographic services over an extended period, nodes in a sensor network will likely need to manage and update their keys while mitigating excessive energy-use. To address this issue, Eltoweissy *et al.* [9] propose a dynamic key management system based on localized combinatorial keying (LOCK). To address the longevity issue and enable the practical use of such networks by mobile in situ users, Olariu *et al.* [2] describe a novel paradigm for autonomous networked sensor system (ANSWER) to provide QoS and secure information services. Yu *et al.* [10] discuss important trade-offs between the lifetime of an image network and the distortion with which images are transmitted from cameras to a mobile user. In [11], Soro and Heinzelman explore coverage and routing issues for video networks, noting important differences from traditional (scalar) networks.

In this work we wish to address the issue of providing a level of confidentiality in the network when keys are temporarily *unavailable* which might occur during extended-operation in hostile settings [4]. In this context, we focus on the *acquisition* and *enciphering* of visual surveillance data for timely transmission to a *sink* rather than mobile users. In particular we wish to explore the role of a distributed attacker such as a sensor-actuator (or actor) network that may perform a variety of disruptive attacks as in Czarlinska and Kundur [3], [5]. The fundamental assumptions of these attacks as they pertain to the mission critical setting are detailed in Section III.

## III. Mission Critical Surveillance SNs

### A. World Model

We consider a surveillance network comprised of camera nodes and scalar sensors. For rapid deployment in outdoor regions, the camera nodes are untethered in that they are battery operated and transmit their acquired visual surveillance wirelessly to a sink. This heterogeneous network is deployed over a large area comprised of many smaller local zones $z_i$ as shown in Figure 1. We consider the possible presence of a second *hostile* sensor-actuator network deployed throughout one or more of the zones. The hostile network is equipped with actuation capabilities, signifying that it can perturb, disrupt or alter the sensor readings of nearby nodes via micro-actuators (the framework and results of this work are also applicable to the case when nodes *inside* the legitimate network are captured and re-programmed by an attacker to form a hostile sub-network). Importantly, the surveillance network does not know a priori which zones (if any) contain a hostile network (or subverted captured nodes).

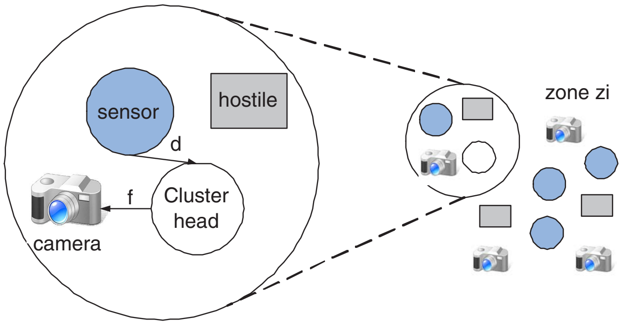

Fig. 1. Zone $z_i$: Upon wake-up, a sensor node sends its (possibly attacked) decision $d$ to the cluster-head while the camera nodes acquire frames. The frames are transmitted or discarded based on feedback $f$ from the cluster-head.

The scalar and visual nodes in the surveillance network *may* all be active (turned-on) to acquire relevant surveillance during an event. However we note that the deployment area is very large and it is not known which zone(s) will contain an event of interest during a given time. Furthermore extended periods of time may elapse before a given region becomes actively of interest. Given the battery operated nature of the network, we assume that the network implements a common sleep/wake-up strategy. For instance, a small subset of the nodes inside each zone become the "cluster-heads" (this task is typically rotated among the nodes to avoid uneven energy drain) [12].

In this work we assume that the remaining scalar and visual nodes inside a zone are asleep until awakened by their cluster-head(s). The cluster-head(s) trigger the wake-up when their input exceeds a given (application-dependent) threshold $T_h$. We note that given the PDF or PMF (probability distribution function or probability mass function) of the phenomenon (monitored by the scalar sensors) and a threshold $T_h$, an input exceeds $T_h$ with some probability $p$ where $p$ is the area of the PDF to the right of $T_h$. To verify the presence of

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

an event through redundancy and to localize the event, each awakened scalar sensor makes a decision based on $T_h$ ("event present" $1$ or "event absent" $0$) and transmits this decision to the cluster-head(s). The awakened cameras continue to capture the possible event and each camera either transmits or disregards its frames based on feedback from the cluster-head(s) regarding the presence or absence of the event in the area. Thus the scalar sensors are utilized as a support system for the camera nodes that capture the surveillance. In the mission critical setting however, the redundancy provided by the scalar sensors may not be sufficient to ensure a dependable data-gathering process in the presence of a hostile attacker as will be discussed in Section III-B.

### B. Attack Goals and Model

In *mission critical* surveillance settings the opponent may engage in *stealthy* counter-intelligence activities that disinform or disrupt the surveillance gathering while minimizing the chance of attack detection. To this effect the opponent may rely on a sensor-actuator network to perform seemingly legitimate sensing while covering one or more zones in the area. With such deployment, the hostile network may engage in a variety of attacks designed to misguide, drain and eavesdrop on the surveillance network as shown in Figure 2.

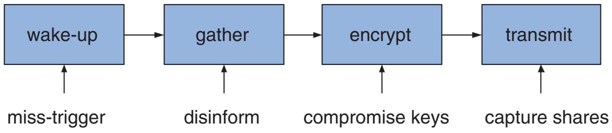

Fig. 2. Surveillance task: the nodes must wake-up during an event, gather the relevant surveillance, encrypt it and transmit it to the sink. A distributed hostile sensor-actuator network may interfere with one or more of these tasks during an attack.

For instance during the wake-up cycle of the nodes, *each* hostile sensor-actuator node (SAN) may actuate in its local vicinity to alter the sensor readings of a neighboring scalar node [5]. The *effect* of the actuation is to alter a decision $1$ (event present) to a $0$ (event absent), or vice versa. Without communication among the hostile nodes (communication may presumably be detected and adds to the energy drain), each SAN actuates with some probability $q$. Importantly, this probability $q$ can be selected to minimize the probability of being detected even if the hostile network does not know the probability $p$ (probability of a scalar node registering an event which depends on $T_h$) [3]. Thus this attack is referred to as a *stealthy actuation* attack. Based on the stealthy actuation attack, the hostile network may miss-trigger and disinform the surveillance network.

The physical deployment of the hostile network throughout one or more zones may enable the hostile network to compromise encryption keys through node capture [4]. Such a compromise might reveal part of the gathered surveillance to the attacker. Furthermore, the ensuing re-keying effort in the network (such as in static key management systems [9]) utilizes energy and might cause delays in surveillance transmission. The wireless nature of the transmission may also allow a *distributed* attacker to intercept a fraction of the encrypted shares from $m < n$ camera nodes while they are transmitted to the sink. Thus a form of protection (i.e. encryption) is always required to transmit the surveillance even when keys are not available.

We note that in practice other important attacks on wireless networks such as radio jamming or denial of service attacks must also be considered [13]. Though important, these attacks are generally not *stealthy* in that the service disruption leads to noticeable effects and thus ultimately to attack detection. In this work we focus on a class of stealthy attacks that have traditionally received less attention despite their significance and despite their possible implementation via micro-actuator networks.

## IV. Proposed GEM Solution for Mission Critical Surveillance Sensor Networks

We now detail methodologies suitable for the system described in Section III to address the reliability of gathering ($G$) and encrypting ($E$) surveillance while mitigating ($M$) energy drains.

### A. Surveillance Gathering (G) and Drain Mitigation (M)

In harsh but otherwise non-hostile environments, node redundancy may provide sufficient resilience against occasional sensor errors [1]. Node redundancy alone however is no longer sufficient in the case of a distributed hostile opponent capable of sensing and actuation [5]. Indeed as discussed in subsection III-B, the hostile network may alter the decisions of scalar sensors in a way that makes the overall data appear legitimate and reasonable given the phenomenon surveyed by the sensors.

To secure the data gathering process in the scenario of stealthy actuation, we wish to verify if the scalar sensor decisions $d_i$ for $i \in \{1, n\}$ collected by the $n$ scalar sensors are legitimate or if they have been altered through actuation. Thus ideally we wish to distinguish between the hypothesis $\mathcal{H}_0$ where the $d_i$ have not been tampered with and the hypothesis $\mathcal{H}_1$ where the $d_i$ have been altered. In the case of $\mathcal{H}_0$ the random variables $d_i$ should come from the Bernoulli distribution $Bern(p)$ where $p$ is the probability of an event. The case of $\mathcal{H}_1$ presents a challenge since the actions of the hostile network are unknown. If the hostile nodes actuate with some probability $q$, then based on the model of actuation, $d_i$ will come from $Bern(r)$ where $r = p + q - 2pq$ but where $q$ (and thus $r$) still remain unknown.

Despite the missing information, attack detection and mitigation can still be achieved. If the hostile network wishes to remain stealthy in the attack, then $q$ has to be chosen such that the scalar data received by the cluster-head appears plausible. This signifies that the scalar decisions $\mathbf{d}$ where $\mathbf{d} = [d_1, ..., d_n]$ should have a weight (number of 1s) that is plausibly close to $np$ (especially for large $n$ where the actual weight approaches $np$ on average). Since the attacker does not know the exact value of $p$ (since $p$ depends both on the PMF of the phenomenon and the threshold $T_h$), the optimal choice

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

of $q$ can be determined based on game theoretic analysis [3]. The analysis reveals important facts about the optimal value of the attack parameter $q$ and the cluster size $n$.

In general terms, the attacking network must select a value of $q$ that is *small* and that *decreases* with increasing cluster size $n$ in order to be stealthy. More specifically, the game theoretic analysis allows the *specific* optimal value of $q$ for the attacker to be determined for any $n$. This analysis is thus important for two reasons. First it provides a value for the parameter $q$ that was missing from the $\mathcal{H}_1$ hypothesis. Second, it provides guidance in the selection of the cluster size. Specifically, the expected fraction of nodes affected by actuation is $n \cdot q(n)/n = q(n)$ where the attacker's optimal $q$ is a function of $n$ and can be determined from the analysis. As an example, for $p = 0.1$ and $n = 30$, the optimal value of $q = 0.074$ which is also the expected fraction of scalar sensors giving faulty readings on average [3]. Selecting the appropriate cluster size is thus an important part of attack *mitigation*. Attack *detection*, that is, performing some form of check on the received data is also crucial. This can be seen from the fact that if the network does not perform any verification, then effectively the hostile network may perform *any* actuation without fear of detection. When a check is performed, the hostile network must adopt the stealthy model.

We thus now consider the problem from the point of view of attack detection where $\mathcal{H}_1$ is the attack hypothesis and $\mathcal{H}_0$ is the non-attack hypothesis. The optimal Neyman-Pearson (NP) detector to distinguish between the two hypotheses is given by Eq. 1 where $w$ is the weight of the data $\mathbf{d} = [d_1, ..., d_n]$ and $\mathcal{T}$ is a threshold chosen based on a desired probability of false alarm $\alpha$. Importantly as shown in Eq. 1, while $\mathcal{T}$ can be determined without knowledge of the attack parameter $q$, the resulting probability of detection $\beta$ cannot be determined without it. Thus use of game theoretic analysis provides mitigants through cluster size selection and provides the missing parameter required to determine the performance of the optimal detector.

$$w \overset{H_1}{\underset{H_0}{\gtrless}} \mathcal{T}(p, \alpha) \quad \text{where} \quad \alpha(p), \beta(q, p) \tag{1}$$

The above mitigation and validation technique may be employed in a variety of applications and sensor network architectures. For the mission critical surveillance application discussed in Section III, the process may be as follows:

(1) NP test: The threshold of the detector is set based on an application-dependent probability of false alarm $\alpha$ which is generally chosen to be very small. Upon receiving the decisions of the $n$ scalar sensors, the cluster-head employs the NP detector of Eq. 1. The cluster-head proceeds based on the outcome of the test ($\mathcal{H}_0$ or $\mathcal{H}_1$).

(2) $\mathcal{H}_0$ (Non-Attack Hypothesis): In this case the cluster-head trusts the data $d_i$ for $i \in \{1, n\}$. Based on each $d_i \in \{0, 1\}$, the cluster-head notifies each corresponding camera if it should encipher and transmit its surveillance using the techniques of section IV-B or if it should discard the sequence captured to-date.

(3) $\mathcal{H}_1$ (Attack Hypothesis): If the result of the detector is the $\mathcal{H}_1$ hypothesis, then most likely an attack is actually occurring (since $\alpha$ is chosen to be small). Furthermore, based on cluster size selection, it is known that approximately *only* $nq(n)$ nodes are expected to be in error where $nq(n)$ is small. What is not known is *which* nodes are in error and various methods of handling this case could be employed. For the mission critical setup, we may wish to ensure that no *event* frames are *missed* or omitted from transmission despite the attack. Thus the cameras that correspond to a $1$ might transmit their frames while the cameras that correspond to a $0$ might verify if their frames are indeed "empty" (contain no events). This verification may be accomplished through lightweight visual detection based on difference images as in [3], [7].

### B. Surveillance Encryption (E) and Drain Mitigation (M)

In the mission critical setting, we wish to ensure that the visual surveillance captured by the camera nodes can be transmitted wirelessly to the sink even when encryption keys become unavailable. Thus we wish to ensure continued service and confidentiality in the network. To achieve this goal we propose a scheme intended to compliment the key-based solution by replacing it during periods of key unavailability.

The proposed scheme is tailored to the case where $n$ camera nodes in a cluster capture correlated visual surveillance but where some (or all) of them do not have encryption keys with the sink (and/or with each other). During this time of unavailability, the camera nodes should still be able to "encipher" the surveillance. Ideally they should also be able to do so efficiently *without* having to transmit the frames to each other. In other words, a distributed scheme where each camera performs the enciphering separately is desirable. The scheme that we thus develop and overview in this work is *based* on the principles of distributed source coding where correlated data may be compressed separately yet optimally given that some correlation statistics about the data are known. Based on these principles we develop a distributed scheme for *visual* surveillance that provides *confidentiality* even if $m < n$ of the "enciphered" shares are intercepted by the hostile network as shown in Figure 2.

We first overview the basic scheme called S/DISCUS (secure distributed source coding using syndromes) and later discuss the proposed algorithm for using S/DISCUS on *visual* surveillance. Suppose that a cluster contains $n$ nodes (i.e. cameras) where each node $i$ captures surveillance data $U_i$ modeled as a string of $k$ symbols, i.e. the nodes capture $U_1^k, U_2^k, \ldots, U_n^k$ where the symbols are from a finite field.[1] Suppose that these $n$ strings of surveillance are not independent but correlated via a parameter $t$ in the following sense:

$$w(U_1^k + U_2^k + \cdots + U_n^k) \le t, \tag{2}$$

[1] The actual data itself may not appear in the form of a string of symbols. In practice the data collected by a node is grouped appropriately and can be mapped to symbols in a finite field at the discretion of the engineer/designer. For example this is how image and audio are encoded.

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

where $w(\cdot)$ is the weight (i.e. the number of symbols that do not match). The correlation model is expressing the observation that $U_1^k, U_2^k, \ldots, U_n^k$ are similar with only a few differences among the strings. We can see this more clearly if we consider a finite field of order say $2^8$ (for example the number of grayscale levels in a digital grayscale image, or one RGB plane of a digital colored image). In this case the correlation in Eq. 2 restricts the number of different pixels among the $n$ nodes to only $t$ nodes (in practice, *visual* surveillance may not obey this correlation model thus necessitating an appropriate algorithm for its use). Given this model and representation of the surveillance data, each node using S/DISCUS inputs its $U_i^k$ into its own simple shift register circuit (the tap coefficient design is detailed in [6]). This distributed approach using readily implementable shift-registers results in several desirable properties:

(1) The output string of each shift register circuit is shorter than the $k$ input symbols.

(2) The surveillance data is secure against a distributed eavesdropper (such as a hostile network) that captures $m < n$ shares (outputs of the shift registers).

(3) The sink can reconstruct each of the $U_1^k, U_2^k, \ldots, U_n^k$ surveillance data perfectly from the received shares without the use of decryption keys.

Importantly the eavesdropper's ignorance is true *even* if he knows the exact coefficients of all the shift register circuits (such as through node capture). Furthermore, given infinite time and resources, the eavesdropper cannot reduce the cardinality of the message set down to 1, i.e., the eavesdropper cannot solve for the message (surveillance data) [6].

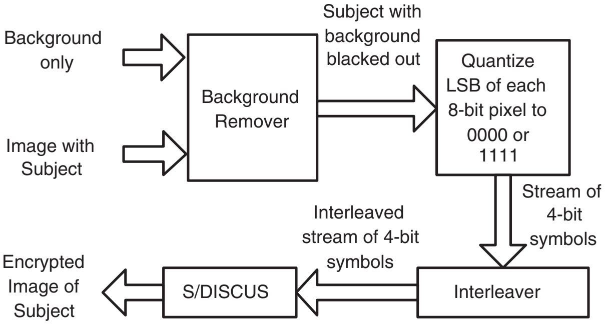
Background only
Image with Subject
Background Remover
Subject with background blacked out
Quantize LSB of each 8-bit pixel to 0000 or 1111
Stream of 4-bit symbols
Interleaver
Interleaved stream of 4-bit symbols
S/DISCUS
Encrypted Image of Subject

Fig. 3. Image Encoder

We now consider the case of visual surveillance data. Normally S/DISCUS performs both lightweight encryption as well as compression when the correlation model of Eq. 2 is satisfied (and does so such that the decoder can perfectly reconstruct all the messages given all the shares). When S/DISCUS is applied to images that depict a common scene from *different* orientations and perspectives, the correlation model of Eq. 2 typically does not hold. One solution is to have the cameras locally register their images prior to using S/DISCUS. Such registration however typically requires (distributed) camera calibrations [8], [14] and may not be desirable for the mission critical setting.

We propose an alternative solution with local preprocessing as outlined in Figure 3. The goal of the preprocessing is to achieve sufficient invariance such that the correlation model of Eq. 2 may be satisfied. Importantly, the invariances and variances need to be distributed uniformly since otherwise some portions of the input stream will satisfy the correlation model, while large portions (particularly important features) will not satisfy the correlation model and will be undecodable.

As shown in Figure 3, the proposed solution requires that a background image of the scene be available for each camera. This background may be periodically captured by the cameras (when events are not detected) and relayed to the sink without encryption. Using the background, a subtraction algorithm (such as the one used in [7]) is applied to an event image with a subject, so that the background pixels can be set to a constant (for example black). This provides a basic source of invariance. To achieve a higher guarantee of invariability, the 4 least significant bits (LSB) of each 8-bit pixel are also quantized. The reasoning is that *adjacent* pixels of images will likely get quantized to the same LSB value thus providing further invariance (though the quantization process introduces some irreversible distortion, in practice the distortion is not prohibitive as shown experimentally in Section V). Once the invariance has been obtained, it must be spread across the input which is accomplished through the use of an interleaver that permutes the pixel positions. This interleaver is deterministic in practice and may be known to the enemy without compromising the security since its only purpose is to transform the input stream into one that better satisfies the correlation model. Finally S/DISCUS can be applied to the input stream as shown in Section V.

## V. G-E-M Performance & Discussion

For data gathering in the stealthy actuation scenario, it is important to both mitigate possible attacks *and* to detect an attack if it is occurring. In Section IV-A we discussed how the former and the latter can be accomplished through cluster size selection and use of the optimal NP detector respectively. Importantly, mitigation and detection are actually *related* in this problem due to the attacker's attempt at *stealth*. Conceptually, as the cluster size increases (there are more data points taken), the attacker's *optimal* attack parameter $q$ decreases. This signifies that picking a larger cluster reduces the (average expected) fraction of attacked nodes. However as $q$ becomes smaller, it is harder for the optimal NP detector to detect the attack. Thus there is an inherent trade-off in the process of cluster size selection that affects mitigation and detection simultaneously.

The relationship between detection and mitigation is depicted in Figure 4(a) for a commonly used value of probability of false alarm $\alpha = 0.1$ (other $\alpha$'s yield similar plots). The plot shows results for various probabilities of an event $p$ for $p \in \{0.05, 0.1, 0.2, 0.3, 0.4, 0.5\}$ (results for $1-p$ are identical due to symmetry). For each $p$, the cluster size $n$ is varied over $n \in \{1, 2, 3, 5, 10, 20, 30, 40, 50\}$. For each $(p, n)$ pair, the optimal attack probability $q$ is determined from [3] and the

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

corresponding probability of detection is found from Eq. 1 and [5]. The horizontal axis thus depicts the optimal attack parameter *and* also corresponds to the (average expected) *fraction* of attacked nodes (recalling that each $q$ corresponds to a different $n$). We observe that the detection performance $P_D$ is best for small probabilities of an event $p$ (which might be the case in the surveillance setting over long periods of time). Whether $p$ is known or unknown however, for a desired $\alpha$ we can examine the $P_D$-$q$ curve and select a suitable trade-off point (or region) from which the required cluster size $n$ can be determined for energy-drain and attack mitigation.

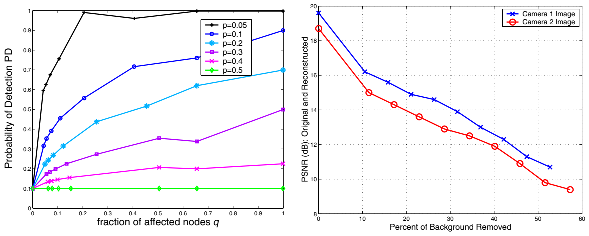

Fig. 4. (a) Probability of Detection $P_D$ (vertical) vs. *optimal* attack $q$ (horizontal) for various probabilities of an event $p$ for $\alpha = 0.1$. (b) Trade-off between Reconstruction Quality (vertical) and Background Redundancy (horizontal).

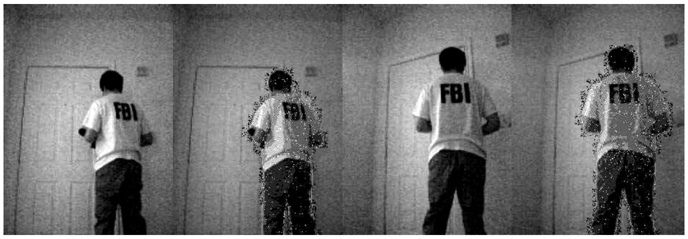

Fig. 5. Original image from (a) camera 1 and (c) camera 2. Reconstructed images at the sink (b) PSNR of 19.59 dB (d) PSNR of 18.69 dB.

Next we wish to examine the performance of the S/DISCUS paradigm for enciphering correlated images collected from cameras using *different perspectives* without image registration. The experiments were performed using the S/DISCUS scheme with *two* cameras and input blocks of 15 4-bit symbols (where the 4 LSB of each 8-bit pixel are quantized). The original images were captured in poor lighting conditions as shown in Figures 5(a) and (c) and reconstructed at the sink with PSNR (peak signal to noise ratio) of 19.59 dB and 18.69 dB as shown in Figures 5(b) and (d) respectively. Importantly, these PSNR values correspond to the *full* use of the background to achieve invariance and thus correspond to the case of *full background redundancy*. As shown in Figure 4(b) however, the PSNR and redundancy characteristics may be traded-off by selecting the percent of background material that is removed (i.e. not utilized to achieve invariance). The ability to trade-off the desired PSNR and redundancy is an important characteristics for the mission critical setting with untethered cameras. Finally we note that the encryption achieved with the low-complexity S/DISCUS for the images in Figure 5 confounds an eavesdropper by giving approximately 36 possible pixel values for *each* pixel. Based on its distributed enciphering and PSNR/redundancy flexibility, the S/DISCUS scheme may be well-suited for certain mission critical surveillance applications where keys are temporarily unavailable due to hostile or challenging conditions.

## VI. Conclusions

In this work we overviewed a methodology for addressing the *data-gathering*, *encryption* and energy drain *mitigation* issues arising in mission critical surveillance networks with a hostile opponent. The methodology proposed for dependable data-gathering offers trade-offs between mitigation and detection that are important in network design. The proposed methodology for enciphering correlated visual surveillance can be performed in a distributed manner without the use of keys or inter-node communication. The overall proposed approach mitigates inherent and deliberate energy drains and might thus be well-suited for certain untethered rapid-deployment surveillance applications.

## References

[1] I. Akyildiz, T. Melodia, and K. Chowdhury, “A survey on wireless multimedia sensor networks,” *Computer Networks*, vol. 51, no. 4, pp. 921–960, March 2007.

[2] S. Olariu, M. Eltoweissy, and M. Younis, “ANSWER: Autonomous networked sensor system,” *Journal of Parallel and Distributed Computing*, vol. 67, no. 1, pp. 111–124, 2007.

[3] A. Czarlinska and D. Kundur, “Reliable Event-Detection in Wireless Visual Sensor Networks through Scalar Collaboration and Game Theoretic Consideration,” *IEEE Transactions on Multimedia, Special Issue on Multimedia Applications in Mobile/Wireless Contexts, accepted.*, available: www.ece.tamu.edu/˜czlinska/TMM08/WVSN.pdf, 16 pages.

[4] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” *IEEE Security and Privacy*, pp. 197–213, 11-14 May 2003.

[5] A. Czarlinska and D. Kundur, “Attack vs. failure detection in event-driven wireless visual sensor networks,” in *ACM Multimedia & Security Workshop (MM&Sec’07)*, Dallas, TX, 20-21 September 2007, 6 pages.

[6] W. Luh and D. Kundur, “Secure distributed source coding with side-information,” *IEEE Communications Letters*, 2008, accepted, 3 pages.

[7] M. Wu and C. Chen, “Collaborative image coding and transmission over wireless sensor networks,” *EURASIP Journal on Advances in Signal Processing*, no. 70481, 2007.

[8] D. Devarajan, R. J. Radke, and H. Chung, “Distributed metric calibration of ad hoc camera networks,” *ACM Trans. on Sensor Networks*, vol. 2, no. 3, pp. 380–403, August 2006.

[9] M. Eltoweissy, M. Moharrum, and R. Mukkamala, “Dynamic key management in sensor networks,” *IEEE Communications Magazine*, vol. 44, no. 4, pp. 122–130, April 2006.

[10] C. Yu, S. Soro, G. Sharma, and W. Heinzelman, “Lifetime-distortion trade-off in image sensor networks,” *IEEE ICIP*, vol. V, pp. 129–132, 16-19 Sept 2007.

[11] S. Soro and W. Heinzelman, “On the coverage problem in video-based wireless sensor networks,” *IEEE Broadband Networks*, vol. 2, pp. 932–939, 3-7 October 2005.

[12] S. Bandyopadhyay and E. Coyle, “An energy efficient hierarchical clustering algorithm for wireless sensor networks,” in *INFOCOM 2003*, 30 March-3 April 2003, pp. 1713–1723.

[13] D. Raymond and S. Midkiff, “Denial-of-service in wireless sensor networks: Attacks and defenses,” *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, Jan-March 2008.

[14] A. Barton-Sweeney, D. Lymberopoulos, and A. Savvides, “Sensor localization and camera calibration in distributed camera sensor networks,” in *Proc. of IEEE BaseNets*, San Jose, CA, October 2006, 10 pages.

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