Lightweight Security Principles for Distributed Multimedia Based Sensor Networks

Deepa Kundur, Takis Zourntos and Nebu John Mathai
Department of Electrical Engineering
Texas A&M University
3128 TAMU, College Station, Texas 7784-3128 USA
{deepa, takis, mathai}@ee.tamu.edu

***Abstract*— This paper investigates the application of multimedia security principles for the protection of emerging distributed sensor networks (DSNs). The authors assert that for DSNs to be successfully deployed in a variety of applications, security development must become an inherent part of the overall DSN system design process. In particular, we argue that multimedia security principles provide an effective means for lightweight protection that is compatible with distributed in-network processing. We propose a novel low-cost secure data converter architecture for DSNs that has fingerprinting and encryption capabilities.**

I. Introduction

The field of multimedia security has matured in the last decade to provide a class of tool-sets and design insights for the protection and enhancement of digital media under a number of diverse attack scenarios. Research into multimedia security was first motivated, in part, by the increasing use of digital means to communicate, store and represent entertainment information such as music and video. The digital form allowed the perfect duplication of information and almost-seemless manipulation and tampering of the data. This created new types of security attacks not (as seriously) addressed in the past by the entertainment industry. The paradigm shift from analog to digital multimedia for entertainment has had an enormous impact for artists, publishers, copyright holders and consumers alike providing flexible and more accessible business models.

We are in the midst of yet another transformation in the way we use information. This is evidenced by the increasing activity in the field of distributed sensor networks. The ultimate goal of such low-cost networks is not to communicate sensor data, but to conduct application-specific inference tasks; communication in such networks is a necessary intermediate step in order to attain the overall objective. Many applications for sensor networks fall within the category of surveillance for security and protection. This may include monitoring of expansive physical areas such as geographical terrain or manufacturing plants, and even the human [1]. It is therefore, imperative that such networks of sensors need to be protected from cyberattacks. Given the fundamental resource constraint issues related to these sensors, security must be judiciously designed and implemented during the development phase of such systems.

This paper asks the question: *Are there lessons learned from multimedia security that we can easily adapt and apply to DSN cybersecurity?* To address this issue, we present the following contributions:

1) An overview of the role of multimedia security in current digital rights management (DRM) and surveillance applications leading to a discussion of its potential role in emerging sensor network applications.
2) The application of multimedia security design insights to sensor node protection by proposing a low-cost data converter (analog-to-digital or digital-to-analog) architecture that produces authentic digital sensor readings.

The remainder of the paper is organized as follows. In Section II we discuss and compare the goals of multimedia security to sensor network protection in order to assess the design insights that hold potential for sensor cybersecurity. Section III provides a problem formulation for secure sensor node design involving the development of a data converter architecture that addresses the dual the problem of digitizing and authenticating the raw sensed reading. Preliminary results are presented in Section IV followed by a discussion and conclusion in Section V.

II. Multimedia and Sensor Network Security

A. Multimedia Security

Multimedia security is a form of modern information protection that focuses, in particular, on the digital security of multimedia data. The solutions to address this problem must take into account not only the traditional characteristics of good security design, but also the inherent attributes of multimedia information. The associated technologies protect multimedia information from attacks such as piracy, tampering, forgery and eavesdropping. The associated primitives that are widely used include digital watermarking, encryption algorithms, one-way functions and signal processing transforms such as the discrete cosine transform (DCT) or discrete wavelet transform (DWT).

Successful research in the field of multimedia security has worked at the interface of signal processing and traditional information security leading to a multidisciplinary perspective of the problem. Common tool-sets have included cryptography,

digital signal processing, communication theory, information theory, and psychology. The challenges of multimedia security therefore reflect this diverse perspective and focus on reducing computational complexity, enhancing error resilience, ensuring compatibility with standards, and providing security, robustness and perceptual integrity. Perceptual integrity for video encryption requires that the enciphered data be significantly different visually than the original; whereas for digital watermarking applications perceptual integrity constrains the hidden watermark payload to be imperceptible within the host media. Thus, many of these measures are application-dependent.

B. Multimedia Security in Digital Rights Management

One popular application of multimedia security has been in the field of DRM. DRM is the digital management of user rights to content. Here, multimedia security must be incorporated in a dynamic and multidisciplinary environment. The dynamism comes, in part, from the constantly changing objectives and business models of the digital media entertainment industry. As a result, security technologies must be flexible, granular and adaptable. Furthermore, the timely interaction among the legal, business and technological sectors of DRM gives the field a unique breadth [2], [3].

The legal aim of DRM is to legislate and enforce the "fair" exchange and processing of content. The primary business objective is to keep the product (i.e., entertainment media) commercial viable. The technological goals include engineering mechanisms and systems that enforce well-defined protection measures. Therefore, for the effective design of DRM, these, often competing, goals must be collectively addressed [3]. Multimedia security provides a set of both active and passive security tools to aid in achieving the composite goals of DRM. Other technological DRM challenges include (a) persistence, the continual management and enduring security of the media through the distribution and consumption chain, (b) interoperability, the ability for different DRM systems to operate in conjunction with one another using effective protocols, signal processing, software and hardware, and (c) implementation, the robust and reliable physical realization of theoretically secure DRM architectures.

Of the work in DRM-based multimedia security, digital watermarking for copy control and tracking has received the greatest attention to date [4], [5].

C. Multimedia Security in Surveillance

Digital watermarking for authentication and tamper detection is also receiving increased use in video surveillance applications. Here, multimedia security must work within a networked environment of video cameras that relay their information to a centralized end-station that interprets the information and makes application-specific decisions. Security must be embedded into the video sensors themselves for real-time protection, and the security-related processing must not interfere with communication protocols. One goal of such systems is to be able to differentiate between live and false video feed to the end-station.

Commercial video surveillance technologies adopting digital watermarking authentication technology include Skyway Security [6] and Sentry Security Systems [7].

D. Distributed Sensor Networks and Security

The overall objective of a DSN is to provide an application-dependent inference of the physical location in which the sensors reside. This inference can be a binary answer to a given question (e.g., is there an intruder in the area?), or may result in a composite data signal that contains the most salient aspects of the sensor data collected. Video sensors are useful when rich visual signatures are required for inference. For instance, video cameras are used for environmental monitoring in oceanographic [8] applications, and for unmanned vehicle navigation [9].

One significant difference between a video sensor network and a collection of video cameras used for traditional surveillance applications is that the former involves distributed processing of the sensed information. This means that the data can be aggregated locally to decrease communication bandwidth to the end-station. Much of the processing that takes place at the end-station in normal surveillance networks is now performed in intermediate stages locally within each video sensor. Therefore, security processing must work with and not significantly hinder this "in-network" processing. For instance, if several video sensors communicate their readings in encrypted form to a neighboring sensor that aggregates (i.e., fuses) the information, a complete decryption of the data is required before fusion. This requires that secure key exchange among the sensors be possible and that the decryption and re-encryption required to transmit the aggregated result not create significant delay or power consumption.

We assert in this paper that multimedia security design approaches that are often characterized by their use of passive and active security mechanisms for persistent protection and lightweight complexity can contribute to the field of sensor network security. In particular, the security services of confidentiality, authentication and tracking may be effectively addressed.

E. Multimedia Security for Distributed Sensor Networks

DSNs are commonly characterized in the research literature by a number of distinct properties. These networks are envisioned to be (a) distributed, involving localized processing such as in-network data aggregation before information is sent to the end-station, (b) data-centric, in which network processing is dependent on 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) application-specific, requiring data aggregation to produce contextual and meaningful data about the observation area, (e) resource-constrained, necessitating the sparing use of communication bandwidth, memory and computation to reduce exhaustion of the often portable power source, as well as (f) autonomous, (g) redundant, and (h) hierarchical.

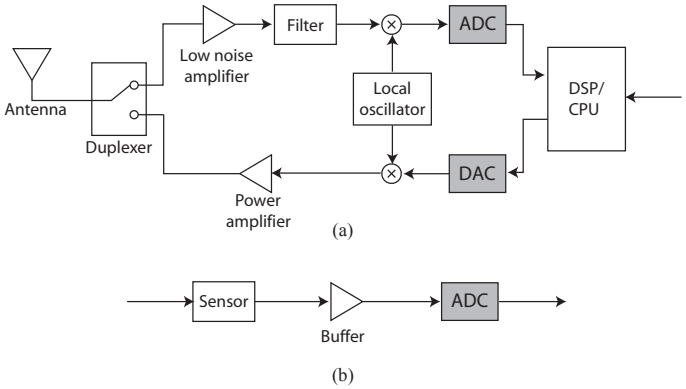

Fig. 1. (a) ADC and DAC placement in a sensor node transceiver. (b) ADC in a sensor node data acquisition system.

These characteristics imply that DSN security must prioritize power and memory efficiency by, for example, securing as much as is needed. In addition, the security mechanisms and protocols must be compatible with application-specific processing. Furthermore, security must be robust to error and partial network attack as a subset of the sensors may be physically available for inspection and tampering by unwanted parties. Based on these assertions, we believe that multimedia security approaches hold potential for DSN security.

Multimedia security techniques can be categorized into the following basic philosophical classes: (a) methods that scale down the security primitives by, for instance, employing "weak" encryption algorithms, (b) mechanisms that secure less information, say, by employing partial encryption, and (c) approaches that merge security processing with signal processing tasks such as digital watermarking integration with media coding standards.

In this paper, we focus on application of the third design philosophy for sensor networks. In particular, we focus on the use of this approach to design a data converter that simultaneously digitizes and authenticates sensor readings.

III. Towards a Secure Analog to Digital Converter for Sensor Network Applications

A typical sensor node is comprised of one or more of the following components: a sensor, a processor, memory modules, a transceiver and a power generator [10]. A data converter exists in almost every sensor node implemented and envisioned. For example an analog-to-digital converter (ADC) and a digital-to-analog converter (DAC) can be found in the sensor node transceiver as shown in Figure 1(a). In addition, an ADC can be found as a part of the sensor reading acquisition system as summarized in Figure 1(b).

Thus, in this work we consider a hardware modification to a well-known data converter in order to provide a secure digitized sensor reading. We hope that this work holds potential for a large class of DSN applications.

A. Problem Formulation

The delta-sigma ($\Delta\Sigma$) modulator is the most widely employed data converter for high precision signal processing applications. This modulator has the following interesting features that we exploit to create a system that also authenticates sensor readings. The $\Delta\Sigma$ modulator

1) represents a deterministic nonlinear system [11],
2) produces an output that contains much "irrelevancy" in the *quantization band* [12], and
3) exhibits "complex" behavior that is suited for some cryptographic applications.

The last point is salient for security applications. Even small deviations in filter parameters, initial conditions, or the input signal can lead to rapid divergence of the output from an expected sequence. The objective of this research is to determine an inexpensive method to modify the $\Delta\Sigma$ modulator and exploit the above characteristics for "reasonably" secure sensor reading digitization. In particular, we look to embed an authenticator payload into the modulator output such that it is not easily extractable without access to the secret key, and can be used to verify the integrity of the sensor reading.

We assume that each sensor node uses lightweight key exchange protocols [13] in order to exchange secret keys for authentication embedding and verification. Depending on the application, verification can be done by a neighboring sensor node, by a "cluster head" in the network, or by the base station so that an appropriate symmetric key exchange protocol is needed.

The next section discusses the proposed architecture for embedding authenticated information into the $\Delta\Sigma$ stream and empirically discusses its performance and security capabilities. The work presented in this section of the paper is preliminary in nature and the authors are currently analyzing the secured $\Delta\Sigma$ modulator architecture to formally assess its security strength and data conversion ability. We present some "outstanding challenges" to stimulate further investigation in addition to concepts for low-complexity sensor-node security.

B. Proposed Architecture

The standard $\Delta\Sigma$ modulator is highlighted in Figures 2 and 3. It is comprised of a linear time invariant (LTI) filter H and a coarse quantizer denoted $Q(\cdot)$. The $\Delta\Sigma$ modulator is used as a basis for developing our novel *embedding* and *extracting* modulators for data conversion and authentication. The embedding modulator inserts an authenticator into the output data stream as shown in Figure 2. The input sensor reading is hashed using the hash function G and then "noise-band encoded" by pushing it into the high frequency spectrum with a non-LTI block T to mask its presence in the output data stream. The output of T is then added to the less significant bits of the output stream of the modulator to create the authenticated and digitized sensor reading.

While it is possible to use a "dither channel" as in [14], we find that dither-embedding of the payload complicates extraction since the output stream becomes more difficult to predict. It is important to note that successful extraction in our proposed scheme relies on *matching* between the embedding

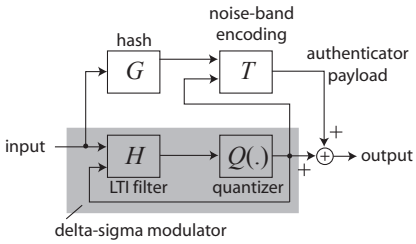

Fig. 2. The embedding modulator.

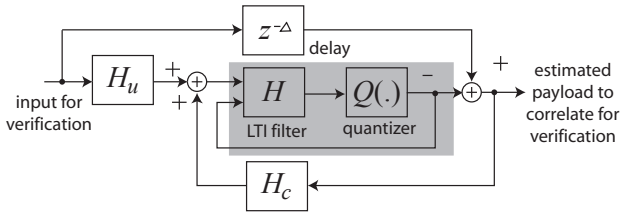

Fig. 3. The extracting modulator.

and extraction modulator[1]. This means that the parameters of the filter H (as well as its initial conditions) must be (nearly) the same for the embedding and associated extracting modulator, or it becomes impossible to extract the payload. We, therefore, allow the parameters of H to be the secret key for security.

Specifically, after key exchange, each data converter is "loaded" with the secret key that forms the parameters of LTI filter H. Through analog adaptive filtering techniques [15], it is possible to realize a wide range of filters H for different key values. Essentially, passive component networks can be designed with analog switches to permit variability in the filter characteristic. In addition, we can incorporate a range of initial conditions for H that act as an expanded key space for greater computational security.

The quantization noise, shaped by the filter H, has the additional purpose of masking the presence of the embedded authenticator payload. As mentioned, the output signal (or sequence) of the delta-sigma modulator is difficult to predict, and is extremely sensitive to variations in filter parameters or the input signal. While this characteristic is favorable for the generation of unpredictable data useful to camouflage the embedded authenticator, it also complicates the extraction process since "locking" of the "authenticator" information and "embedding" modulator can be difficult to accomplish.

In Figure 3, an FIR filter H_u extracts the original input signal from the output generated by the embedding modulator. This introduces some group delay, Δ, which must be employed to align the outputs of the embedding and extracting modulators for payload estimation. The outputs of the modulators are subtracted to yield a payload estimate. In principle, the function of the extracting modulator is to reproduce the output sequence that would have been generated by the embedding modulator had no payload been introduced. To help ensure synchronization of the output streams, an error-feedback connection, with a low-pass filter H_c, can be used to offset deviations in the output streams. The output of the extracting modulator is correlated with the hash and T-filtered version of the output of H_u to verify authentication and data integrity. The details have been omitted for brevity.

IV. Preliminary Results

We investigate the performance of the embedding and extraction procedures shown in Figures 2 and 3. Simulations are based in Matlab and Simulink [16] and incorporate several functions from the delta-sigma toolbox developed by Schreier [**?**] which are helpful in the design/realization of the loop filter, H. The number of samples for these discrete-time simulations is 65536, and a manually-generated authenticator payload of is used. Figure 4 shows the input signal and payload sequence used for our simulations here.

In Figure 5, we show that, given an accurately extracted input signal, the estimated payload degrades with small deviations in the coefficients of H parameters. It is this aspect of our approach that is attractive for sensor-node security: the coefficients of H are, in effect, a security key.

V. Discussion and Conclusions

Although preliminary results appear promising, there are a number of issues that need to be investigated before the practicality of the proposed security scheme is determined. First, it is not exactly known to what extent the modulators in the embedding and extracting procedures can be matched, as this depends on the semiconductor processes available for manufacturing (although better-than one-percent coefficient matching is often readily achieved with conventional fabrication). Second, it is quite challenging to achieve "tracking" of the embedding modulator output stream even with an accurately matched extracting modulator, since the output streams (and filter states) can deviate for even small errors in the estimation of the input signal. While we have made use of observers and special techniques (not fully described here) to improve tracking, this aspect of the scheme requires further research. Finally, we note that what makes this scheme good for security also makes it difficult to implement, namely, the sensitivity of the delta-sigma modulator. More research is needed to evaluate different approaches to exploit the complex behavior of the delta-sigma modulator for lightweight security applications.

We believe that the field of DSN security can benefit from the lessons learned by the multimedia security research community. Straightforward application of multimedia security tools can benefit multimedia-based sensor networks. In addition, design insights for lightweight protection as in the proposed secure data converter holds promise for simpler forms of sensor readings. As we push the limits of power and complexity as in the design of sensor networks, the application and the examination of new paradigms are essential.

[1]We have made some use of Luenberger observer techniques to "synchronize" data streams of the modulators, but are not discussed here for brevity.

References

[1] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proc.*

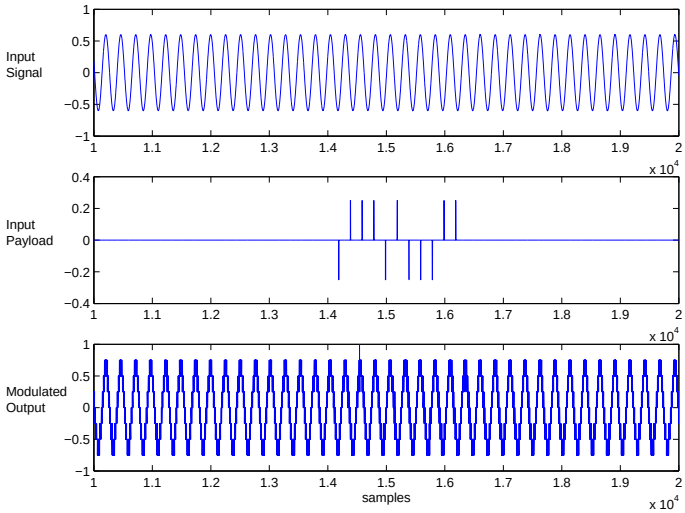

Fig. 4. Input signal, payload sequence shown in top two plots. A representative output corresponding to the embedding delta-sigma modulator is shown in the bottom plot.

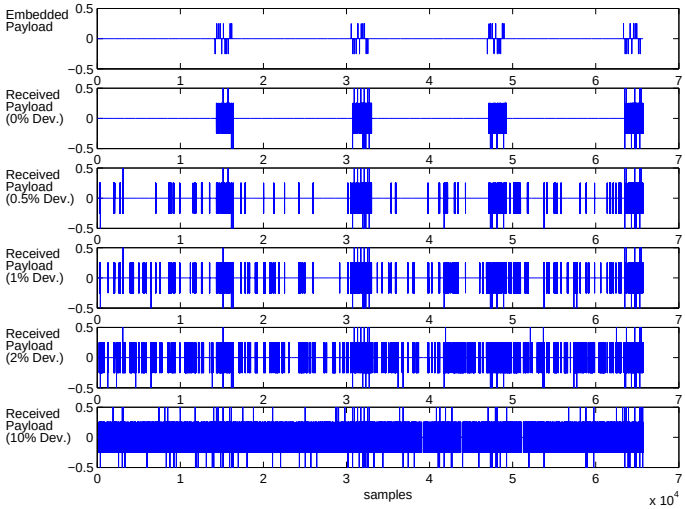

Fig. 5. Simulated payload and extracted payloads under varying deviations in the parameters of H.

ACM/IEEE International Conference on Mobile Computing and Networking, August 1999, pp. 263–270.

[2] R. Akalu and D. Kundur, "DRM and the courts: Lessons learned from the failure of CSS," *IEEE Signal Processing Magazine*, vol. 21, no. 2, pp. 109–117, March 2004.

[3] D. Kundur, H. H. Yu, and C.-Y. Lin, *Content Delivery in the Mobile Internet*, chapter Security and Digital Rights Management for Mobile Content, John Wiley & Sons, 2004.

[4] D. Kundur and K. Karthik, "Digital fingerprinting and encryption principles for digital rights management," *Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management*, vol. 92, no. 6, pp. 918–932, June 2004.

[5] I. Cox, M. Miller, and J. Bloom, *Digital Watermarking: Principles & Practice*, Morgan Kaufmann, 2001.

[6] "Skyway Security," URL: http://www.skywaysecurity.com/.

[7] "Sentry Security Systems," URL: http://www.cctvsentry.com/.

[8] R. Holman, J. Stanley, and T. Özkan-Haller, "Applying video sensor networks to nearshore environment monitoring," *IEEE Pervasive Computing*, vol. 2, no. 4, pp. 14–21, October-December 2003.

[9] G. Kogut, M. Blackburn, and H. R. Everett, "Using video sensor networks to command and control unmanned ground vehicles," in *Proc. AUVSI Unmanned Systems in International Security*, September 2003.

[10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, August 2002.

[11] R.W. Adams and R. Schreier, "Stability theory for $\Delta\Sigma$ modulators," in *Delta-Sigma Data Converters: Theory, Design and Simulation*, S.R. Norsworthy, R. Schreier, and G.C. Temes, Eds., pp. 141–164. IEEE Press, 1997.

[12] S. R. Norsworthy, "Quantization errors and dithering in $\Delta\Sigma$ modulators," in *Delta-Sigma Data Converters: Theory, Design and Simulation*, S.R. Norsworthy, R. Schreier, and G.C. Temes, Eds., pp. 75–140. IEEE Press, 1997.

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

[14] A. J. Magrath and M. B. Sandler, "Encoding hidden data channels in sigma-delta bitstreams," in *Proc. IEEE Int. Symposium on Circuits and Systems*, May-June 1998, pp. 385–388.

[15] D. A. Johns and K. Martin, *Analog Integrated Circuit Design*, Wiley, 1997.

[16] The Mathworks Inc., "Matlab (Version 6.5.0.185000, Release 13)," June 2002, URL: http://www.mathworks.com.

[17] R. Schreier, "The delta-sigma toolbox (version 2.0)," January 2000, URL: http://www.mathworks.com (search author's last name "Schreier" in Matlab Central file exchange).