Chapter 14

# SECURITY IN SENSOR NETWORKS: WATERMARKING TECHNIQUES

Jennifer L. Wong
*University of California, Los Angeles*
*Los Angeles, CA 90095*
jwong@cs.ucla.edu

Jessica Feng
*University of California, Los Angeles*
*Los Angeles, CA 90095*
jessicaf@cs.ucla.edu

Darko Kirovski
*Microsoft Research*
*Redmond, WA 98052*
darkok@microsoft.com

Miodrag Potkonjak
*University of California, Los Angeles*
*Los Angeles, CA 90095*
miodrag@cs.ucla.edu

**Abstract** The actual deployment of the majority of envisioned applications for sensor networks is crucially dependent on resolving associated security, privacy, and digital rights management (DRM) issues. Although cryptography, security, and DRM have been active research topics for the last several decades, wireless sensor networks (WSN) pose a new system of conceptual, technical, and optimization challenges.

In this Chapter we survey two areas related to security in WSN. First, we briefly survey techniques for the protection of the routing infrastructure at the network level for mobile multi-hop (ad-hoc) networks. Secondly, we discuss

the first-known watermarking technique for authentication of sensor network data and information. We conclude the Chapter by providing a short discussion of future research and development directions in security and privacy in sensor networks.

**Keywords:** Wireless sensor networks, Security, Privacy, Digital Rights Management

## 14.1 INTRODUCTION

Wireless ad-hoc sensor networks (WSN) are distributed embedded systems where each unit is equipped with a certain amount of computation, communication, storage, and sensing resources. In addition each node may have control over one or more actuators and input/output devices such as displays. A variety of applications for sensor networks are envisioned, starting from nano-scale device networks to interplanetary scale distributed systems. In many senses, WSN are a unique type of systems which have unique technical and operational challenges. Among these, security and privacy are most often mentioned as the key prerequisite for actual deployment of sensor networks.

There are at least three major reasons why security and privacy in WSN is such an important topic. The first one is that sensor networks are intrinsically more susceptible to attacks. They are often deployed in uncontrolled and sometimes even hostile environments. Wireless communication on a large scale can be easily observed and interfered with. WSN nodes are both complex component systems with numerous weak points from a security point of view. In addition, they are severely constrained in terms of energy and therefore extensive on-line security checking is not viable. Finally, sensors can be manipulated even without interfering with the electronic subsystem of the node and actuators can pose strong safety and hazard concerns.

The second argument that emphasizes the role of security in WSN is the importance of protecting typical applications. WSN can not only have data about one or more users, but can also contain a great deal of information about their past and even future actions. In addition, they may contain significant amounts of information about a users physiological and even psychological profiles. Furthermore, once the sensors are equipped with actuators both the sensors and the environment can be impacted in a variety of ways.

The third reason for security in WSN is, in a sense, the most scientific and engineering based reason. WSN require new concepts and a new way of thinking with respect to security, privacy, digital rights management, and usage measurement. The Internet was a great facilitator of computer and communication security on a large scale. Note that the Internet itself created opportunities for new types of attacks such as denial of service (DoS) and intrusion detection. It also created new conceptual techniques on how to defend the Internet infras-

tructure. For example, Honeypots are now widely used to obtain information about the behavior and thinking of an attacker [33]. It is easy to see that WSN will further accentuate these trends. For example, denial of sleep attacks will be brought to a new level of importance.

In this chapter we present two case studies: how to leverage on mobility to provide security, and how to develop and evaluate watermarking schemes for the protection of data and information in sensor networks. We conclude the chapter with a section on future directions where we identify eight security dimensions that we expect to be of high importance for both research and practical deployment of WSN.

## 14.2 CASE STUDY: MOBILITY AND SECURITY

In this Section, we discuss the interplay between mobility and security. More specifically, we focus on security and mobility with respect to multihop wireless networks. This area of research is still in the very early phases of its development and only a few research results has been reported. We expect very rapid growth in this direction in the near future.

It is expected that a large percentage of wireless networks will be mobile. There are two main reasons for this prediction. The first is that in many applications one can achieve significantly higher performance if mobility is provided and exploited. For example, sensors nodes may move closer to the phenomenon or event of interests. The second reason is even more compelling: sensor networks associated with individual users, cars, trains, airplanes and other transportation vehicles are intrinsically mobile.

It is not clear whether mobility makes security in wireless sensor networks easier or more difficult to be achieved. From one point of view, it makes it easier because one can leverage on conducting specific security tasks on the nodes of interest which are in favorable locations. From the other point of view, it makes it more difficult due to the dynamic structure of the topology and potential introduction and departure of any given node.

Until recently, mobility received relatively little attention in wireless ad-hoc networks. The main reason for this is that the majority of standard tasks in wireless ad-hoc networks are easier to address in the static scenario. Even more importantly, there experimental data that would enable realistic modeling of mobility does not exist. Essentially all current models are of random statistical nature [7]. Notable exception include [27, 32].

While a number of notable research results have been reported on security in mobile ad hoc networks [8, 18, 19, 24, 30], we will focus our attention on the first paper to address using mobility to assist in the security of mobile networks [9]. Capkun et al. consider a self-organized mobile wireless network with no security infrastructure. Therefore, there is no central authority, no centralized

trusted party, and no other centralized security service provider. Due to this fact, the approach can be applied at any network layer, and will allow for the addition of new nodes into an existing and operating network. Each node in the network is given the same role in the security exchange, and there for there is no single point of failure for the system (as there is with a central security certification authority).

The focus of the work is on one of the most critical phases in establishing secure communication: exchange of cryptographical keys. Their underlying and main assumption is that when nodes are in close vicinity of each other they can communicate using a secure side channel, such as infrared or wired communication. Under this assumption, no middle man attack that would alter any communication between them at this point is possible. However, their scheme does not require that secrecy of the initial message is guaranteed, due to the fact that they are focusing on public key cryptography schemes. However, their scheme is general and can be applied to secret key schemes too. An additional assumption in their scheme is that each node can generate cryptographic keys and verify signatures.

Under these assumptions they assume that two types of security associations can be created between nodes in the network. The first association is a direct association. In this case, when nodes come in contact with each other they can physically verify each other. At this point, the nodes both consciously and simultaneously exchange cryptographic keys. The second type of association is an indirect association, which they introduce in order to expedite the key establishment throughout the network. An indirect association is established through a "friend". Two nodes are friends if they trust each other to always provide correct information about themselves and about other nodes that they have encountered/established associations with and they have have already established a security association between each other. A friend can interchange security information (i.e. public keys) between two nodes if it has a security association with both nodes that want to establish a security association. Through this process, all nodes do not have to come into contact directly with each other, but only with a node who has already established an association with another node. This process in not transitive beyond a chain that consists of more than one friend. Their scheme protects against attacks in the form of eavesdropping on communications, manipulation of messages, and nodes with misrepresented identity.

They evaluated their approach under the random walk mobility approach [7] and demonstrated that almost all nodes in the network can establish security associations in a relatively short period of time. It is important to note that the mobility model crucially impacts this conclusion and that in more realistic cases where nodes have limited mobility ranges this will not be the case. We

believe that inclusion of Internet gateway points or bases stations would greatly enhance the applicability of the approach.

Specifically, for WSN this type of approach has both advantages and limitations. No central authority is needed, however each node in the network must be able to generate and verify public keys. The use of public and private key cryptography in sensor networks is questionable due to heavy computation requirements. The notion of using mobile nodes in conjunction with static nodes in sensor networks to establish secure relationships between static nodes would be a possible approach. However, these types of relationships may not be applicable for WSN deployed in hostile environments. In the very least, this work and other security approaches for mobile ad hoc networks have not only potential for direct application in WSN but also provide foundations for new techniques.

## 14.3 CASE STUDY: REAL-TIME WATERMARKING

One of the major security issues in the Internet is digital right management (DRM). It is easy to see that DRM will also play a major role in wireless sensor networks. In addition, data authentication will be exceptionally important. To address these problems, Feng et al [14] have developed the first watermarking techniques for cryptologically embedding an authorship signature into data and information acquired by a WSN.

### 14.3.1 RELATED WORK: WATERMARKING

The notion of intellectual property protection and specifically watermarking has been widely studied for items such as text [3], audio/video [37], and circuit designs. Specifically, watermarking techniques have been proposed for two domains: static artifacts and functional artifacts.

Static artifacts [34, 17] are artifacts that consist of only syntactic components which are not altered during their use, ie. images [36] and audio [12, 23]. Watermarks can also be placed in graphical objects such as 3D graphics [28] and animation [15]. The essential property of all watermarking techniques for static artifacts is that they leverage the imperfection of human perception. The main objectives of watermarking techniques for static artifacts include requirements for global placement of the watermark in the artifact, resiliency against removal, and suitability for rapid detection.

Watermarking for functional artifacts, such as software and integrated circuits design have also been proposed. The common denominator for functional artifacts is that they must fully preserve their functional specifications and therefore can not leverage on the principles for watermarking static artifacts. Functional artifacts can be specified and therefore watermarked at several levels of abstraction such as system level designs, FPGA designs [25], at

the behavioral and logic synthesis levels, and the physical design level [20, 21]. These approaches leverage on the fact that for a given optimization problem, a large number of similar quality solutions exist which can be selected from in order to have certain characteristics which match a designer's signature. More complex watermarking protocols, such as multiple watermarks [25], fragile watermarks [16], publicly detectable watermarks [31] and software watermarking [29], have also been proposed. Techniques have also been developed for watermarking of DSP algorithms, sequential circuits, sequential functions [10], and analog designs.

Additionally, other techniques for intellectual property protection such as fingerprinting [2, 6], obfuscation [5], reverse engineering [4], and forensic engineering [22] have been proposed.

In sensor networks, watermarking and other intellectual property protection techniques can be applied at a variety of levels. The design of the sensor nodes and the software used in the network can be protected using functional techniques. Additionally, both static and functional watermarking can be applied on the data collected from the network depending on the types of sensors and actuators deployed (i.e. video, audio, measured data). In the remainder of this section, we survey work which proposes the first watermarking technique for the protection of data collected in a sensor network.

### 14.3.2 REAL-TIME WATERMARKING

Real-time watermarking aims to authenticate data which is collected by a sensor network. The first watermarking technique for cryptologically watermarking data and information acquired by a WSN has been developed by Feng et al [14].

The key idea of their technique is to impose additional constraints to the system during the sensing data acquisition and/or sensor data processing phases. Constraints that correspond to the encrypted embedded signature are selected in such a way that they provide favorable tradeoffs between the accuracy of the sensing process and the strength of the proof of authorship. The first set of techniques embeds the signature into the process of sensing data. The crucial idea is to modulate by imposing additional constraints on the parameters which define the sensor relationship with the physical world. Options for these parameters include the location and orientation on sensor, time management (e.g. frequency and phase of intervals between consecutive data capturing), resolution, and intentional addition of obstacles and use of actuators. In particular, an attractive alternative is to impose constraints on intrinsic properties (e.g. sensitivity, compression laws) of a particular sensor, therefore the measured data will have certain unique characteristics that are strongly correlated with the signature of the author/owner.

The second technique is to embed a signature during data processing, either in the sensor or control data. There are at least three degrees of freedom that can be exploited: error minimization procedures, physical world model building, and solving computationally intractable problems. In the first scenario, there are usually a large number of solutions that have similar levels of error. The task is to choose one that maintains the maximal consistency in measured data and also contains a strong strength of the signature. Typical examples of this type of tasks are location discovery and tracking. In the second scenario, they add additional constraints during the model building of the physical world.

In the final scenario, they are dealing with NP-complete problems, and therefore it is impossible to find the provably optimal solution. Therefore, the goal is to find a high quality solution that also has convincing strength of the signature.

Probably the best way to explain the watermarking approach for sensor networks is to demonstrate its essential features using a simple, yet an illustrative example. For this purpose the authors demonstrate how a watermark can be embedded during the atomic trilateration process. Atomic trilateration is a widely used basic algorithmic block for location discovery that can be formulated on the example shown in Figure 14.1 in the following way.

**Problem:** There are four sensors: A, B, C, and D. Sensors A, B, and C know their locations in terms of x and y coordinates. The distances between themselves and node D are measured with a certain level of accuracy and are reported by A, B, and C.

**Goal:** The objective is to discover the location of sensor D in term of its x and y coordinates.

The problem can be stated as a system of three nonlinear equations that contain nine known values and two unknown variables as stated bellow.
**Known values**: $(A_x, A_y)$, $(B_x, B_y)$, $(C_x, C_y)$, $M_{AD}$, $M_{BD}$, $M_{CD}$ where $(A_x, A_y)$, $(B_x, B_y)$, $(C_x, C_y)$ are the x and y coordinates of sensor node A, B and C respectively. $M_{AD}$, $M_{BD}$, $M_{CD}$ are the measured distances from A to D, B to D and C to D respectively.
**Unknown variables:** $(D_x, D_y)$; that are components of the location of sensor node D that it suppose to conclude from the measured distances from all other three nodes to itself.

The key observation is that all distance measurements are noisy. Therefore, the equations can be solved in such a way that all of them are simultaneously satisfied. Instead, the goal is to assign the values to unknown variables in such a way that the solution to all the equations is maximally consistent. Maximal consistency, of course, can be defined in an infinite number of ways. For example, the following three measures are often advocated:

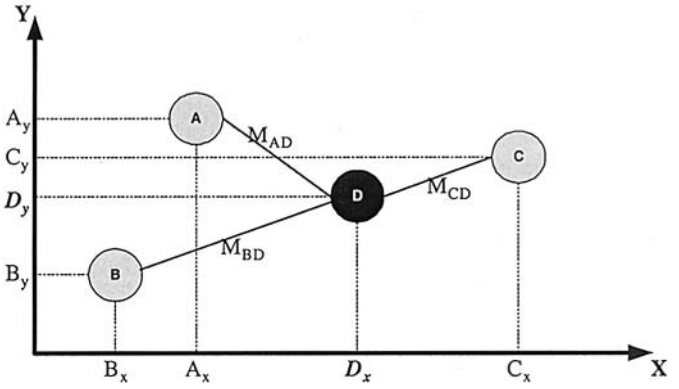


*Figure 14.1.* Atomic Trilateration.

$$L_1 = |M_{AD} - E_{AD}| + |M_{BD} - E_{BD}| + |M_{CD} - E_{CD}| \quad (14.1)$$

$$L_2 = \sqrt{(M_{AD} - E_{AD})^2 + (M_{BD} - E_{BD})^2 + (M_{CD} - E_{CD})^2} \quad (14.2)$$

$$L_\infty = max(|\frac{(M_{AD} - E_{AD})}{E_{AD}}|, |\frac{(M_{BD} - E_{BD})}{E_{BD}}|, |\frac{(M_{CD} - E_{CD})}{E_{CD}|}) \quad (14.3)$$

where

$$E_{AD} = \sqrt{(D_x - A_x)^2 + (D_y - A_y)^2} \quad (14.4)$$

$$E_{BD} = \sqrt{(D_x - B_x)^2 + (D_y - B_y)^2} \quad (14.5)$$

$$E_{CD} = \sqrt{(D_x - C_x)^2 + (D_y - C_y)^2} \quad (14.6)$$

The first measure, $L_1$, combines the errors in a linear way and asks for their simultaneous minimization. The second measure, $L_2$, is widely used and specifies the errors as linear combination of quadratic values. The intuition is that one will obtain a solution that will have not just a relatively low linear sum, but also will minimize, to some extent, the maximal error. The third measure $L_\infty$ aims to reduce the maximal error among all three measurements. $E_{AD}$, $E_{BD}$, $E_{CD}$ are the expected distances from A, B, C to D. Essentially, the goal is to minimize the differences between expected distances (E's) and measured distances (M's). The expected distances are written in terms of the location of node D. Thus, by minimizing the distances, the closest estimate of the real correct location of node D is determined. There are many ways to solve this small and simple system of equations. For example, one can use the conjugate gradient method or a multi-resolution grid to obtain the solution

according to the selected measure of quality. If they just solve the system of equations, they will have the requested location information, but will not have the proof that they conducted measurements and solve the system. However, if they impose additional constraints on the system of equations or on selected objective function, they will have both the high quality solution and the strong proof of the ownership.

One potential watermarking alternative process, where they modify the objective function, is illustrated using the following example. Suppose that "0001010011010001" is the binary string/signature that they want to embed. One option is to embed the signature by assigning weight factors to each term of the objective function according to the binary string. The binary string can be partitioned into sections (in this case, three sections), then converted to decimal numbers and used to assign weight factors. The process can be illustrated as in the following figure:

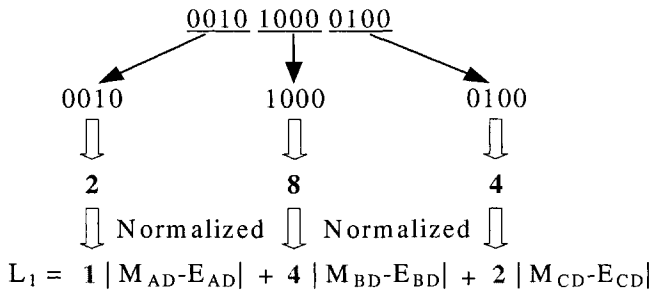


*Figure 14.2.* Embedding watermarks by assigning weight factors to the objective function during atomic trilateration.

### 14.3.3 GENERIC PROCEDURE

There exist numerous types of sensor networks and they can be used for many different purposes. Their goal is to watermark all data provided by a sensor network generically regardless of the type of data the network is collecting or what the purpose of the network is.

There exist two types of data being produced by a sensor network: raw sensor data and processed application data. The first type, sensor data, is the original data the sensor network captures or measures. It may or may not be what the user of the network desires. However, the second type, processed data, is the output of the network to the user. The distinction of these two types of data provides insight into where watermarking can take place: i) during the process of sensing data (original data capturing); ii) during the process of processing the original data. Therefore, they call these two processes watermarking in sensing data and watermarking in processing data.

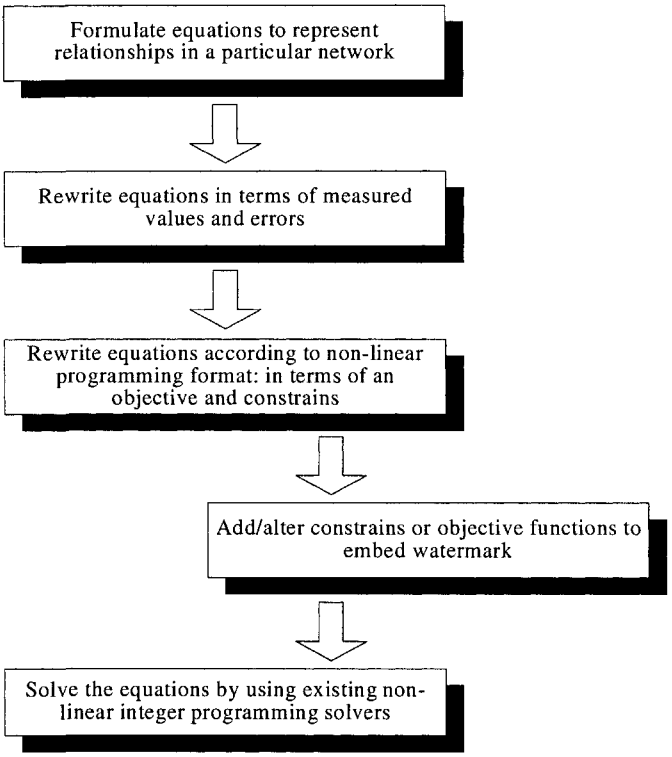


*Figure 14.3.* General procedure for embedding a watermark.

An important question to ask is how is the original raw data being processed in order to generate the processed application data? In this case, Feng and Potkonjak enquired the technique of non-linear programming. The general procedure can be summarized as Figure 14.3.

They first represent all the relationships that exist in the network using equations. Since everything is measured there always exists some degree of error. Realizing this, they replace the variables with the summation of a reasonable estimate and some error value. Their next goal is to minimize the errors in the equations, and achieve the closest possible estimates to the true values. This can be achieved by using effective non-linear programming solvers.

In order to illustrate this process, consider the example of navigation shown in Figure 14.4

**Problem:** A sensor node is moving over a period of time. At each point of time, atomic trilateration can be performed to determine its location.

**Goal:** The trajectory motion of a particular node over a period of time in terms of coordinates at each point of time.

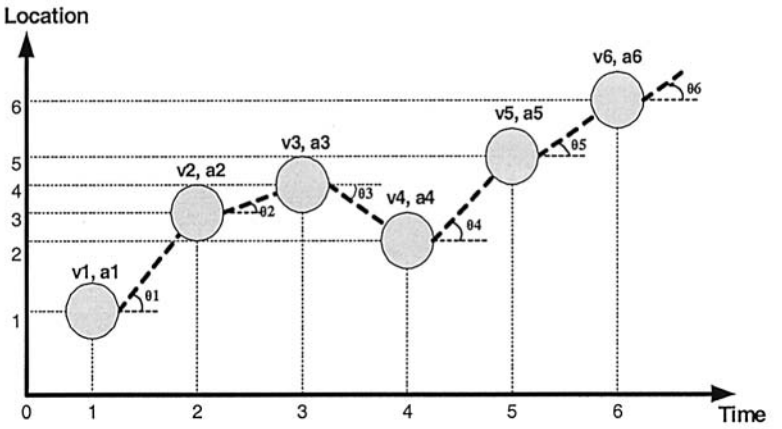


*Figure 14.4.* Trajectory process.

| Known (Measured) variables | | | |
|---|---|---|---|
| $V_{obj,0}$ | $V_{obj,1}$ | $V_{obj,2}$ | velocity |
| $a_{obj,0}$ | $a_{obj,1}$ | $a_{obj,2}$ | acceleration |
| | $\Delta$ t | | time interval |
| $d_{obj,a}$ | $d_{obj,c}$ | $d_{obj,d}$ | measured distance |
| $(x_a, y_a)$ | $(x_c, y_c)$ | $(x_d, y_d)$ | 3 known sensors |
| $d_{obj,f}$ | $d_{obj,g}$ | $d_{obj,h}$ | measured distance |
| $(x_f, y_f)$ | $(x_g, y_g)$ | $(x_h, y_h)$ | 3 known sensors |
| $d_{obj,I}$ | $d_{obj,j}$ | $d_{obj,k}$ | measured distance |
| $(x_i, y_i)$ | $(x_j, y_j)$ | $(x_k, y_k)$ | 3 known sensors |

| Unknown variables | |
|---|---|
| $(x_{obj,0}, y_{obj,0})$ | coordinates of object at time 0 |
| $(x_{obj,1}, y_{obj,1})$ | coordinates of object at time 1 |
| $(x_{obj,2}, y_{obj,2})$ | coordinates of object at time 2 |

*Table 14.1.* Known and unknown variable at time 2 for Figure .

Consider the case where the time is 2, they have the known and unknown variables which are shown in Table 14.1.

Now, this trajectory motion can be described by the following

$$d_{obj,a} = \sqrt{(x_a - x_{obj,0}) + (y_a - y_{obj,0})} \quad \text{9 equations}$$
$$d_{t_0 \to t_1} = (V_{obj,0})\Delta t + \frac{a_{obj,0}}{2}(\Delta t)^2 \quad \text{2 equations}$$
$$V_{obj,1} = V_{obj,0} + (a_{obj,0})\Delta t \quad \text{2 equations}$$
$$x_{obj,1} = (d_{t_0 \to t_1})cos(\alpha_{obj,0}) + x_{obj,0} \quad \text{4 equations}$$

$$y_{obj,1} = (d_{t_0 \to t_1}) sin(\alpha_{obj,0}) + y_{obj,0} \qquad \text{4 equations}$$

Feng et al. incorporate errors to each variable:

$$\begin{aligned}
\varepsilon_1 &\Leftrightarrow x_{obj,0} \\
\varepsilon_2 &\Leftrightarrow y_{obj,0} \\
\varepsilon_3 &\Leftrightarrow x_{obj,1} \\
\varepsilon_4 &\Leftrightarrow y_{obj,1} \\
\varepsilon_5 &\Leftrightarrow x_{obj,2} \\
\varepsilon_6 &\Leftrightarrow y_{obj,2}
\end{aligned}$$

Now, they can rewrite the system of equations in terms of objective function and constraints:

$$\text{OF: MIN}(|\varepsilon_1| + |\varepsilon_2| + |\varepsilon_3| + |\varepsilon_4| + |\varepsilon_5| + |\varepsilon_6|)$$

such that:

$$\begin{aligned}
d_{obj,a} &= \sqrt{(x_a - x_{obj,0}) + (y_a - y_{obj,0})} && \text{9 equations} \\
d_{t_0 \to t_1} &= (V_{obj,0})\Delta t + \tfrac{a_{obj,0}}{2}(\Delta t) && \text{2 equations} \\
V_{obj,1} &= V_{obj,0} + (a_{obj,0})\Delta t && \text{2 equations} \\
x_{obj,1} &= (d_{t_0 \to t_1}) cos(\alpha_{obj,0}) + x_{obj,0} && \text{4 equations} \\
y_{obj,1} &= (d_{t_0 \to t_1}) sin(\alpha_{obj,0}) + y_{obj,0} && \text{4 equations} \\
x_{obj,0} &= Ex_{obj,0} + \varepsilon_1 \\
y_{obj,0} &= Ey_{obj,0} + \varepsilon_2 \\
x_{obj,1} &= Ex_{obj,1} + \varepsilon_3 \\
y_{obj,1} &= Ey_{obj,1} + \varepsilon_4 \\
x_{obj,2} &= Ex_{obj,2} + \varepsilon_5 \\
y_{obj,2} &= Ey_{obj,2} + \varepsilon_6
\end{aligned}$$

There are a number of methods that can be used to solve problems posed as non-linear programming problem in the form of objective function and constraint. The most popular options includes feasible direction, active set, gradient projection, penalty, barrier, augmented lagrangians, cutting plane, direct, and quasi-Newton methods. The standard nonlinear programming references include [26].

The watermarking procedure is a self-contained block that is embedded in the overall multi-model sensor fusion process, as shown in Figure 14.3. The watermarking procedure can be conducted in many ways. For example, one can augment or alter the objective function with new components that correspond to the signature. Or one can superimpose additional constraints that correspond to a pseudorandom binary string that correspond to the signature. The advantage of the former technique is that it usually provides rather low overhead in terms of the solution quality. The advantage of the later technique is that it usually provides exceptionally strong proof of the authorship. In all

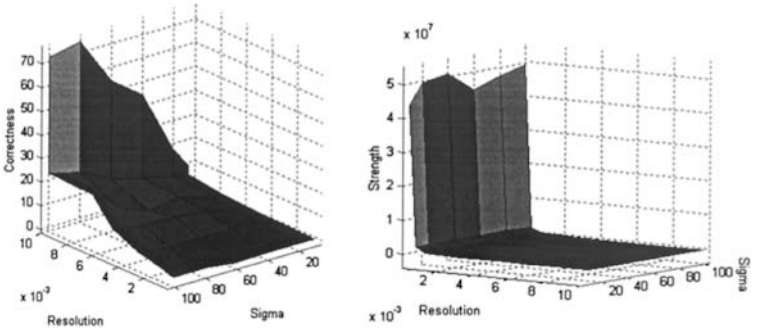


*Figure 14.5.* Correctness & Strength of authorship of the watermarking scheme given various Resolution and Sigma.

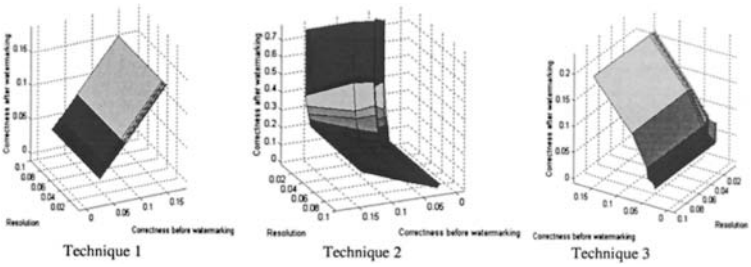


*Figure 14.6.* Comparison of correctness based on changes on resolution: before vs. after embedding watermarks.

cases, exact mapping of the pseudorandom string onto the constraints or objective function can be conducted in many ways. Three specific instances are presented in their sxperimental results.

The objective is to demonstrate the effectiveness of the approach on very small example (where it is most difficult to hide information) by statistically analyzing the relationships between correctness, strength of authorship, measurement errors, and resolution used for measurements and computations in terms of bits. Correctness is defined as the normalized difference in errors from the optimal solution between the watermarked solution and the solution obtained without watermarked. Strength of authorship is defined as 1 out of the all possible solutions that have at least the same quality as the watermarked solution.

The simulation process was conducted in the following way. They first generated the coordinates of three points according to the uniform distribution on the interval [0.0, 1.0]. For comparison and evaluation purposes later on, they also generate the coordinates of the point that they are trying to determine its location. After that, they calculated the exact distances between the forth point

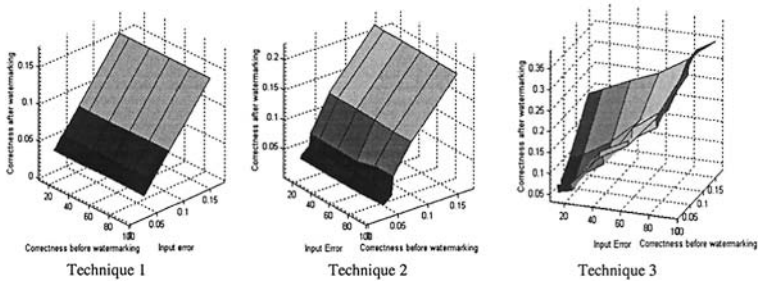


*Figure 14.7.* Comparison of correctness based on changes on sigma: before vs. after embedding watermarks.

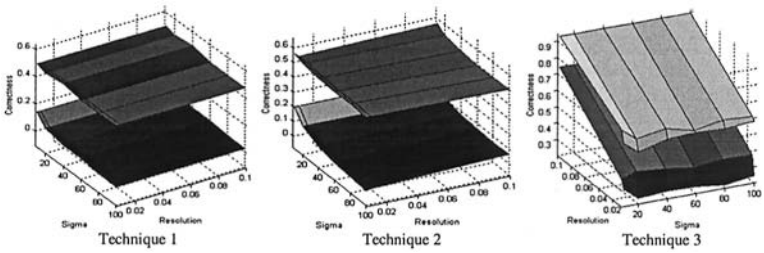


*Figure 14.8.* Comparison of correctness: 2-D vs.3-D.

and the three beacon points. Furthermore, they add a small error value to the correct distances in order to simulate the estimated/measured distances. These small changes are randomly generated according to the Gaussian distribution (0, 1).

They consider three specific watermarking schemes. The first one just alters the least significant bit according to the signature. It is well known that this technique is not adequate for watermarking. They used it solely to provide basis for comparison for two other techniques. The second technique alters the components of the objective function according to the user's signature. The final technique, finds among all solutions that differ at most k% (they used value k = 5 in their experiments) on terms of estimated error from the non-watermarked solution, one that has the smallest Hamming distance from the signature stream.

From Figures 14.5-14.9, it is easy to see that two last techniques perform well, in particular when they consider 3D trilateration. The following series of figures show the comparisons of embedding signature in 2-D vs. 3-D by applying three different watermarking techniques. As they can observe from the figures, spreading the signature into more places (i.e. embedding watermarks in 3-D) produces a more accurate and stronger solution.

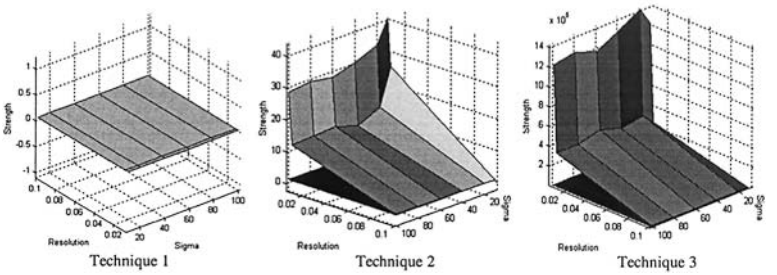


*Figure 14.9.* Comparison of strength of authorship: 2-D vs. 3-D

## 14.4 FUTURE DIRECTIONS

In this section, we briefly discuss the research directions that we perceive as the most challenging and most promising. We classify these directions in eight broad categories: (*i*) individual nodes, (*ii*) network infrastructure, (*iii*) sensor data and information, (*iv*) applications at the semantic level, (*v*) denial of service techniques, (*vi*) mobility, (*vii*) actuators, and (*viii*) theoretical foundations.

As we previously mentioned, wireless sensor networks are highly susceptible to security attacks due to their deployment, their hardware, and their resource constraints. Due to these factors, we can expect that fault inducing attacks and power consumption attacks will be conducted much more often on sensor network nodes. In addition, we expect that sensor and actuator related attacks will attract a significant amount of attention. As of now, no work has been done to address these security issues.

Similarly to the case of individual nodes, wireless sensor network infrastructures are potentially more susceptible to attacks than traditional networks. The operational state of the nodes are also conceptually very different because many nodes will often go into sleep mode and many nodes will be rarely active. Although significant progress has already been made on securing basic network protocols, it is clear that we need additional work to produce techniques for protecting canonical tasks in wireless senor networks such as routing, broadcast, multicast, and data aggregation. It will also be important to develop techniques which ensure that at least some nodes in each geographic area are operational. From the system point of view, we expect to see the development of firewalls specifically designed for the needs of WSN. For example, nodes in the network could be grouped in clusters and access to each cluster will be available through only a single node. Low power requirements may insist that nodes interchangeably serve as the firewall clusterhead.

WSN are designed and deployed because of sensors and therefore the primary objects of protection should be the sensor data and information. Very

little work has been reported on these topics. A number of security and privacy issues need to be addressed including how to ensure the integrity of sensor data, how to provide mechanisms for authentication and access control, and how to efficiently, in terms of energy and storage, measure the usage of each sensor node by each user query.

In a sense, conceptually the most novel techniques will be developed for securing applications at the semantic level.We expect that most users will be most concerned with the privacy of their actions and information about their physiological state and the environment that surrounds them. Therefore, there is an urgent need to develop techniques that ensure privacy of subject and objects in sensor networks. One potential starting point for these efforts could be work done by the database community [1, 13, 35].

Recently, with the proliferation of the Internet, denial of service (DoS) techniques have gathered a great deal of attention [11, 38]. A number of static and dynamic defense mechanisms have been proposed. Due to the unique nature of WSN, we expect that denial of service attacks will be very popular. In addition, node sensitivity to energy consumption will further facilitate the effectiveness of denial of service attacks. One way to better learn about the most dangerous attacks is the development of controlled Honeypots of WSN that would register the exact sequence of steps taken by attackers and therefore eventually facility the development of better defense techniques [33]. Also we expect that a number of intrusion detection techniques for WSN will be soon developed.

Numerous WSN will be mobile, and as we already stated, mobility makes security and privacy significantly more difficult from one point of view and possibly easier from another point of view. Research in mobile WSN has just started and there is a need to develop tractable yet realistic mobility models. Note that in some mobile scenarios, restrictions on the size and power of the energy supply will not be as strict as in tradition wireless networks. Furthermore, note that mobility itself impacts essentially all network infrastructure tasks such as routing and data aggregation as well as how data is collected and processed.

Lastly, actuators will close the loop between the physical and information world. They have the potential to greatly improve the quality of individual life and industrial and economic processes. However, it is apparent that once the control of actuators is compromised, an attacker will be positioned to induce not just intellectual but also direct physical harm and damage. To the best of our knowledge, security of an actuator is a topic which still needs to be addressed. We expect that authentication and control techniques based on secret sharing will play an important role. Finally, in addition to outlining a great number of security techniques for sensor networks their exists a clear need to develop a sound theoretical foundation of the field. This is particularly true with emerging misinformation and privacy research.

## 14.5 CONCLUSION

In this Chapter we discussed security issues in wireless sensor networks at the network layer, specifically mobility assisted security. Additionally, we survey a watermarking technique for digital right management of data and information from sensor networks. Furthermore, we summarize some of most promising pending research directions related to security and privacy in sensor networks.

## REFERENCES

[1] R. Agrawal and R. Srikant. Pricacy-preserving data minimg In *International Conference on Management of Data*, pages 429–450, 2000.

[2] D. Boneh and J. Shaw. Collusion-secure fingerprinting for digital data In *Advances in Cryptology*, pages 452–465, 1995.

[3] J. T. Brassil, S. Low, and N. F. Maxemchuk. Copyright protection for the electronic distribution of text documents In *Proceedings of the IEEE*, volume 87, pages 1181–1196, 1999.

[4] P.T. Breuer and K.C. Lano. Creating specifications from code: Reverse engineering techniques *Journal of Software Maintenance: Research and Practice*, 3:145–162, 1991.

[5] C. Thomborson C. Collberg and. Watermarking, tamper-proofing, and obfuscation - tools for software protection *Transactions on Software Engineering*, 28(2):735–746, 2002.

[6] A.E. Caldwell, H. Choi, A.B. Kahng, S. Mantik, M. Potkonjak, G. Qu, and J.L. Wong. Effective iterative techniques for fingerprinting design IP In *Design Automation Conference*, pages 843–848, 1999.

[7] L.J. Camp. Drm: doesn't really mean digital copyright management In *ACM Computer and Communications Security*, pages 78–87, 2002.

[8] S. Capkun, L. Buttyan, and J. Hubaux. Self-organized public-key management for mobile ad hoc networks In *ACM International Workshop on Wireless Security*, pages 52–64, 2002.

[9] S. Capkun, J.P. Hubaux, and L. Buttyan. Mobility helps security in ad hoc networks In *ACM Symposium on Mobile Ad Hoc Networking and Computing*, pages 46–56, 2003.

[10] R. Chapman and T. Durrani. Ip protection of dsp algorithms for system on chip implementation *IEEE Transactions on Signal Processing*, 48(3):854–861, 2000.

[11] S. Cheung and K. N. Levitt. Protecting routing infrastructures from denial of service using cooperative intrusion detection In *New Security Paradigms Workshop*, pages 94–106, 1997.

[12] I. Cox, J. Killian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for images In *IEEE Int. Conf. on Image Processing*, pages 243–246, 1996.

[13] D. Dobkin, A. Jones, and R. Lipton. Secure databases: Protection against user influence *Transactions on Database Systems*, 4(1):97–106, 1979.

[14] J. Feng and M. Potkonjak. Real-time watermarking techniques for sensor networks In *SPIE Security and Watermarking of Multimedia Contents*, pages 391–402, 2003.

[15] C. Fornaro and A. Sanna. Public key watermarking for authentication of csg models *Computer Aided Design*, 32(12):727–735, 2000.

[16] J. Fridrich, M. Goljan, and A.C. Baldoza. New fragile authentication watermark for images In *International Conference on Image Processing*, pages 446–449, 2000.

[17] F. Hartung and M. Kutter. Multimedia watermarking techniques In *Proceedings of the IEEE*, volume 87, pages 1079–1107, 1987.

[18] Y.-C. Hu, D. B. Johnson, and A. Perrig. Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks In *IEEE Workshop on Mobile Computing Systems and Applications*, pages 3–13, 2002.

[19] H. Huang and S. F.x Wu. An approach to certificate path discovery in mobile ad hoc networks In *ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2003.

[20] A. B. Kahng, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe. Robust IP watermarking methodologies for physical design In *Design Automation Conference*, pages 782–787, 1998.

[21] D. Kirovski, Y.-Y. Hwang, M. Potkonjak, and J. Cong. Intellectual property protection by watermarking combinational logic synthesis solutions In *International Conference on Computer-Aided Design*, pages 194–198, 1998.

[22] D. Kirovski, D. Liu, J. L. Wong, and M. Potkonjak. Forensic engineering techniques for VLSI CAD tools In *Design Automation Conference*, pages 581–586, 2000.

[23] D. Kirovski and H.S. Malvar. Robust spread-spectrum watermarking In *International Conference on Acoustics, Speech, and Signal Processing*, pages 1345–1348, 2001.

[24] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks In *IEEE International Conference on Network Protocols*, pages 251–260, 2001.

[25] J. Lach, W.H. Mangione-Smith, and M. Potkonjak. Robust FPGA intellectual property protection through multiple small watermarks In *Design Automation Conference*, pages 831–836, 1999.

[26] D. Luenberger. *Linear and Nonlinear Programming*. Addison Wesley, 1984.

[27] J.G. Markoulidakis, G. L. Lyberopoulos, D. F. Tsirkas, and E. D. Sykas. Mobility modeling in third-generation mobile telecommunication systems In *IEEE Personal Communications*, pages 41–56, 1997.

[28] R. Ohbuchi, H. Masuda, and M. Aono. Watermarking three-dimensional polygonal models In *ACM International Multimedia Conference*, pages 261–272, 1997.

[29] J. Palsberg, S. Krishnaswamy, M. Kwon, D. Ma, Q. Shao, and Y. Zhang. Experience with software watermarking In *Annual Computer Security Applications Conference*, pages 308–316, 2000.

[30] P. Papadimitratos and Z.J. Haas. Securing mobile ad hoc networks In *Handbook of Ad Hoc Wireless Networks*. CRC Press, 2002.

[31] G. Qu. Publicaly detectable techniques for the protection of virtual components In *Design Automation Conference*, pages 474–479, 2001.

[32] J. Scourias and T. Kunz. An activity-based mobility model and location management simulation framework *Workshop on Modeling and Simulation of Wireless and Mobile Systems*, pages 61–68, 1999.

[33] L. Spitzner. *Honeypots: Tracking Hackers*. Addison-Wesley., 2002.

[34] M. Wagner. Robust watermarking of polygonal meshes In *Geometric Modeling and Processing*, pages 201–208, 2000.

[35] S. Warner. Randomized response: A survey technique for eliminating evasice answer bias *Am. Stat. Assoc*, 60(309):62–69, 1965.

[36] R. Wolfgang and E. Delp. A watermark for digital images In *International Conference on Images Processing*, pages 219–222, 1996.

[37] R. Wolfgang, C.I. Podilchuk, and E. Delp. Perceptual watermarks for digital images and video In *International Conference on Security and Watermarking of Multimedia Contents*, volume 3657, pages 40–51, 1996.

[38] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks *Computer*, 35(10):54–62, 2002.