Privacy and Security in Environmental Monitoring Systems

Sabrina De Capitani di Vimercati, Giovanni Livraga, Vincenzo Piuri, Fabio Scotti
Dipartimento di Informatica, Università degli Studi di Milano
Via Bramante 56 – Crema, Italy
email: *firstname.lastname*@unimi.it

***Abstract*—There is today an increasing interest in environmental monitoring for a variety of specific applications, with great impact especially on natural resource management and preservation, economy, and people's life and health. Typical uses encompass, for example, Earth observation, meteorology, natural resource monitoring, agricultural and forest monitoring, pollution control, natural disaster observation and prediction, and critical infrastructure monitoring. While on one hand these systems play an important role in our society, on the other hand their adoption can raise a number of security and privacy concerns, representing a possible obstacle for the development of future environmental applications. In this paper, we analyze the security and privacy issues characterizing both the environmental monitoring infrastructures and the data collected and processed by them. We also provide an overview of possible countermeasures for diminishing the effects of these issues.**

I. Introduction

Environmental monitoring systems allow the study of physical phenomena and the design of prediction and reaction mechanisms to dangerous situations. In its general form, a monitoring system is composed by a certain number of sensors designed to measure different physical quantities, one or more processing nodes, and a communication network. The sensors provide in output analogical signals, which are conditioned and converted into the digital domain. The digital signals are transmitted to the processing devices, which aggregate the obtained data to understand the measured phenomenon. In our society, these systems are becoming more and more important since they have a fundamental role for detecting new environmental issues and for providing evidences that can help in prioritizing the environmental policies. Monitoring systems are also useful to better understand the relationships between environment, economical activities, and individuals' daily life and health. There is then great interest in monitoring the environment to associate possible effects with observed phenomena and predict critical or dangerous situations. For instance, today we know that there is a direct link between the exposure to PM10 and PM2,5 and different pathologies of vascular systems. Besides, natural disaster detection, observation and, eventually, prediction can be based on monitoring the geographical areas of interest. Monitoring of critical infrastructure, such as railways, highways, gas pipelines, and electric energy distribution networks represents another sector in which these systems are becoming highly significant.

In the last years, environmental monitoring systems have been subject to fundamental changes due to the rapid advancements of the technology as well as the development of a global information infrastructure, such as the Internet, allowing an easy and rapid diffusion of the information worldwide. As an example, the advances in spectral and spatial resolutions, new satellite technologies, and the progress in communication technologies have improved the level of detail of satellite Earth observations, thus making available high resolution spatial and spectral data. Although such technological developments have the positive effect of expanding the application fields where environmental data can be successfully used, there is also a negative effect related to the increase of possible misuses of environmental data and systems. As a matter of fact, seemingly innocuous environmental information can lead to privacy concerns. For instance, ambient environmental monitoring data could be used to identify small geographic areas. Property owners identified in the vicinity of a hazardous waste site or other pollution sources could experience decreased property values or increased insurance costs.

In this paper, we aim at providing a comprehensive analysis of the main security and privacy issues that can arise when collecting, processing, and sharing environmental data. After a description of the architectures and data collected by environmental monitoring systems (Section II), we analyze their security and privacy issues (Section III), which involve both the infrastructure of the environmental monitoring systems and the data collected and disseminated, and describe possible countermeasures for mitigating them (Section IV). The paper represents therefore a first step towards the development of security and privacy-aware solutions easily integrable with environmental monitoring systems.

II. Environmental monitoring systems and data

Before describing the security and privacy issues that can arise in the context of environmental monitoring systems, it is fundamental to clarify the architectures that characterize them, and the environmental data that can be typically collected and possibly released to the public.

A. System architectures

According to the overall architecture of the system used for data acquisition and measurement processing, environmental monitoring systems can be classified as: *centralized*, *distributed*, and *remote sensing* systems [7]. Centralized systems

are composed of a single processor or controller, a limited number of sensors and a simple output presentation interface. Data are collected by sensors and transmitted to the processing unit that performs all data analysis and feature extractions required by the application, and stores all relevant information as specified by the application itself. Distributed systems are composed of a high number of sensing nodes, which often can be added or removed, and can exploit distributed computing and storing abilities. Sensing nodes contain a limited number of sensors, a processing unit, and a network communication channel. These nodes collect data, may perform local processing, and route data and information towards processing nodes in the distributed structure. Some nodes have interfaces to deliver results of their elaborations, and storage devices to save acquired sensor data and processed information. Sensing nodes can be either deployed in a fixed position, or mobile on board of robots to explore the environment. Remote sensing systems are based on signals and images acquired by sensors installed on artificial satellites or aircrafts and are typically used for vast geographical phenomena.

Many environmental monitoring systems have a distributed architecture, since it allows for limiting costs and impact on the environment (small and inexpensive sensors, shorter and cheaper sensor connections, small low-cost processing units for real-time operations, and possibly wireless transmission for limited interconnection costs). Besides, self-configuration and self-calibration capabilities can be introduced for easier deployment. This network topology has often higher power requirements since sensing nodes continuously transmit data. Moreover, adjacent nodes may measure redundant or highly correlated data. Scalability may also become difficult due to computational and bandwidth issues.

To overcome these communication, energy, and scalability problems, hierarchical sensor networks can be considered, which are usually composed of three-levels: *local* nodes (sensors), *intermediate* nodes (local aggregation centers), and a *central processing* node. Some nodes can also coordinate a reduced number of sensors (cluster) by performing synchronization and data fusion [28] (Figure 1). Computation is distributed in the hierarchical structure to create abstract views of the environment at different abstraction levels and to compact the information by extracting the relevant knowledge as locally as possible. Local processing should be performed carefully to avoid possible erroneous interpretations of the corresponding data at higher levels. Appropriate data aggregation techniques must be adopted to achieve a global understanding of the measured phenomena, while avoiding data loss and redundant transmissions [12].

Communication is a critical aspect in sensor networks. As in the conventional architectures, it can be wired. The use of cables to power sensors and transmit the data can however create difficulties that can be overcome with the adoption of Wireless Sensor Networks (WSN) [5]. In these architectures, geographical position of nodes may not be a-priori known: GPS or GIS systems are used to trace the positions of the data collected from sensors.

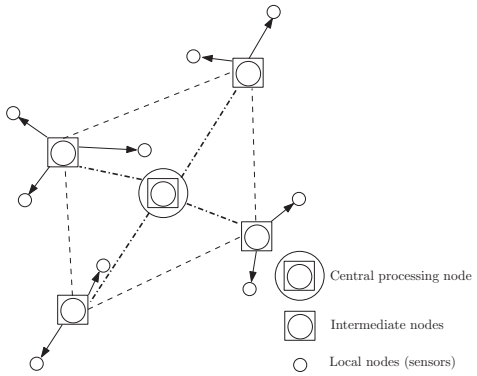

Fig. 1. Hierarchical sensor network.

Sensing can be performed by using sensors for the specific quantities to be measured, placed locally in the point in which the measure has to be taken. However, in some environments direct local sensing may be difficult or even impossible due to costs or environmental/operating conditions. To overcome this problem, for some quantities indirect measures can be taken by observing the point of interest from some distance. Visual Sensor Networks (VSN) are an example of this approach: their nodes are equipped with image-capturing devices and use image-based monitoring techniques. VSNs require however more complex devices, a greater memory usage, a higher bandwidth, and also nodes with more power consumption. Hierarchical sensor network architectures, composed of heterogeneous nodes, can be used to reduce the costs and the computational load [24].

Remote sensing system can capture several types of quantities at a significant distance (e.g., via aircrafts or artificial satellites). Such systems can be passive or active. In the first case, the sensors only detect quantities naturally produced by the object, such as the radiations of the reflected sunlight emitted by the objects. Many passive sensors can be used according to the chosen wavelength and signal dimension (e.g., radiometers, multispectral and hyperspectral imaging). On the contrary, active systems send a signal to the object to be monitored and measure the reflected pulse (e.g., RADAR, LIDAR, laser altimeters). Remote sensing techniques can be merged with terrestrial sensor networks to integrate local data with large-scale observations to enhance the observation quality, for example by co-registration [6].

Environmental monitoring systems can be classified also according to their geographical extension in *large-scale*, *regional*, and *localized* systems [22]. Large-scale environmental monitoring systems are used for observing very large areas, spanning often over several countries or even the whole globe. Typical large-scale systems are those used for meteorological monitoring, and the monitoring of seismic activity and hostile environments (e.g., [2], [3]). Regional monitoring systems cover a more limited geographical area, at the level of a single region of a country, or of a single city. Application examples are represented by water or air quality, land sliding, forest wildfires, and manufacturing plant monitoring (e.g., [20]–

[22]). Localized networks focus on a very limited area, often using small nodes and wireless transmission techniques. Examples of this kind of network are used for the monitoring of the quality of the water and of the groundwater in very localized points (e.g., [1]).

Environmental monitoring systems are also characterized by the type of functionalities performed [22]. In *mono-function* systems the measured quantities are directed to provide knowledge for a single application. In *multiple-function* systems, data are collected (possibly in subsets of different types from different locations) and used by different applications, even for different global purposes.

More complex measurement systems, called *heterogeneous sensor networks* [22], may be created by integrating subsystems of the above types, especially when applications use systems already deployed in the environment of interest or when quantities must be measured in an heterogeneous setting.

B. Environmental data

Different data types are used in environmental monitoring systems, depending on the applicative context. In fact, the used sensors can measure data related to different physical quantities: movement, speed, acceleration, force, pressure, humidity, radiation, luminosity, chemical concentration, as well as audio, video, and so on. Usually, the acquired data consist in monodimensional or multidimensional signals (images/frame sequences).

The data used by large-scale environmental monitoring systems are inherent to the physical quantities chosen to measure a single phenomenon. In these systems, the capture and aggregation of the data are done at a high frequency, to perform a continuous monitoring of the phenomenon. In most cases, the geographical positions of the measuring nodes are fixed, known a-priori and released publicly. For instance, the system described in [23] was composed of 192 measurement stations with fixed and known positions, and performed a continuous monitoring of air temperature, humidity, precipitations, solar radiations, wind speed and direction, and atmospheric pressure. The system described in [2] was composed of more than 150 measurement stations with fixed and known positions, and measured data from seismographs.

In the case of regional or localized environmental monitoring networks with multiple functions, nowadays nodes may not have fixed or known a-priori positions, can be equipped with GPS devices, use wireless transmission techniques, and be powered using batteries. For this reason, the data transmission frequency is often smaller than the one used in large-scale environmental monitoring systems. For instance, the system described in [4] performed the continuous monitoring of the waves along the coasts of Louisiana and the Mexican gulf, measuring the wave height, their period, the direction of propagation, the water level, and the direction and speed of the currents. Different kinds of nodes with wireless transmission capabilities can be used (e.g., [21], [25], [29]).

At high level, the lifecycle of environmental data can be divided in three macro-steps: *collection*, *storage*, and *publication*. Data are collected from the environment and stored at the sensor and/or processing nodes. The format of the stored data depends on the specific purpose for which such data have been collected. Authorized parties can access the environmental data for analysis or other purposes. The environmental data (or a subset of them) can then be made publicly or semipublicly available. The publication of the data is typically in the form of macrodata (i.e., tables reporting aggregated information about an environmental phenomenon) or microdata (i.e., records reporting data related to specific physical measurements) [15].

In the remainder of this paper, we illustrate some security and privacy risks that may arise in the different steps of their lifecycle. To fix ideas and make the following discussion clear, we refer our examples to a scenario charaterized by a localized network in the city of San Francisco, which is under the control of the local municipality. The system is distributed and the sensor nodes are organized according to a centralized configuration. The collected data are stored at processing node $\mathcal{PN}$. *Alice* is an adversary that tries to violate the monitoring system and to discover sensitive information. We also consider a fictitious factory $\mathcal{A}$, which improperly releases pollutants and production rejects in the environment.

III. Security and privacy in environmental monitoring

Security risks are related to the threats that can undermine the confidentiality, integrity, and availability of the data during any stage of their lifecycle, and of the system in its entirety (e.g., system architecture and communication infrastructure). Privacy risks are related to the threats that can allow an adversary to use the environmental data for inferring sensitive information, which is not intended for disclosure and should be kept private. Security and privacy risks are often correlated, and an adversary can exploit a security violation for breaching data privacy. For instance, *Alice* might violate the physical security of processing node $\mathcal{PN}$ (security violation) to access private information related to the pollutant levels in the air of San Francisco, and infer pathologies of the citizens of a given area of the city (privacy violation). Note that in the following discussion, we neither consider the classical security problems related to failures of the system and/or applications due to errors, nor the reliability and dependability aspects of the system, as our goal is to focus on the less-known security and privacy issues.

A. Security risks

They are related to all threats that can: *i)* damage the system infrastructure; *ii)* violate communication channels among the system components; *iii)* allow unauthorized parties to intrude into the system for malicious purposes.

- *Damages to the system infrastructure*. This category of security risks includes attacks aimed at physically damaging the monitoring system or at violating the confidentiality, integrity, and availability of the collected data. These attacks can have an effect on each of the three steps of the environmental data's lifecycle. For instance,

suppose that the local municipality of San Francisco analyzes the collected environmental data to determine the safest location where a new children playground can be build, and suppose that *Alice* maliciously damages the sensor nodes close to factory $\mathcal{A}$. Clearly, the collection of the environmental data is compromised since this sensor nodes is not available (data availability violation). An analysis on the (partial) environmental data available to the local municipality can erroneously identify an area close to factory $\mathcal{A}$ as the safest area where building the new playground. In this case children will be exposed to pollutants and production rejects. The same risks apply when all sensor nodes are working properly but the processing node stops to work, since the analysis of the environmental data is compromised as it cannot be based on the latest measurements of the sensor nodes. Similar problems can happen when an adversary attacks the databases where environmental data are stored (storage step), or the systems where they are published (publication step). In all these cases, data confidentiality, integrity, and availability can be compromised.

- *Violation of the communication channels*. An adversary may violate the communication channels in the sensor network. In particular, the adversary might only monitor the communication channels (passive adversary) or also attempt to delete or modify data transmitted on such channels (active adversary). In addition to these "classical" attacks (which can violate the confidentiality and integrity of the data), an adversary can also monitor the accesses performed on the data by the authorized parties, thus discovering some sensitive information about them. For instance, the fact that an authorized party accesses data related to the concentration of particulates discloses the fact that the party is interested in discovering the polluted areas. If the party is a building constructor, this may imply that the party is interested in building a new apartment complex, and therefore the adversary can speculate on the costs of the lands. Effective protection of data access also requires the protection of access patterns: an adversary should not be able to see whether two accesses performed by two different parties aimed at the same data. For instance, *Alice* should not be able to see if two competitors are interested in performing similar analysis on the environmental data. If so, *Alice* would be able to sell this knowledge to one of the two competitors.
- *Unauthorized access*. Environmental data should be available only to the authorized parties. Clearly, access restrictions apply only when data are not publicly released since in this case (publication step) data are available to everybody without further restrictions. Unauthorized accesses can possibly involve the sensor nodes or the database where environmental data are stored after their collection and analysis. In the first case, an adversary can be interested in accessing raw data to update them or to inject false data so that tampered data are sent to the processing node. For instance, *Alice* can be interested in manipulating the measurements performed by the sensor nodes close to factory $\mathcal{A}$ to reduce the concentration of a specific harmful substance. In the second case, an adversary is clearly interested in accessing environmental data after their collection, normalization, and analysis. Such data can also be stored together with other datasets and therefore the adversary can discover correlations and dependencies among these different datasets. In these cases, both data confidentiality and integrity are at risk.

B. Privacy risks

They are related to all threats that can allow an adversary to (directly or indirectly) infer sensitive information from the collected environmental data. These inferences can involve individuals, the environmental area on which data have been collected, and also areas close to or correlated with it. For instance, the dissemination of studies on the presence of polluting substances in geographical areas or workplaces can be correlated with the medical history of the patients living in that areas. As another example, the knowledge that some geographical areas are polluted with harmful substances can also affect individuals who live in other areas if, for instance, they own properties in the polluted areas. In fact, the value of such properties could decrease due to such knowledge. Privacy risks can occur when environmental data are made publicly available (publication step) or when they are (properly or improperly) accessed, and can be a consequence of data correlations and associations, of observations of data evolutions and unusual data, and of the knowledge of users' locations.

- *Data correlation and association*. The correlations existing among different phenomena can be successfully exploited for inferring sensitive information. As an example, consider a life and sickness insurance company in San Francisco. Suppose that an external source releases a study about the relationship between pollutants and rare diseases. By analyzing environmental data collected by the local municipality, and comparing them with this study, the insurance company can decide to increase the risk associated with citizens living in polluted areas of San Francisco and re-compute their insurance policies. In addition to correlation, also the association of environmental data with other data coming from different sources can be exploited for inferring sensitive information. For instance, suppose that *Alice* can access a collection of data recording the medical histories of a community of patients. *Alice* might then link such data with airborne pollution studies (by exploiting city and county zones that are used to identify population exposed to specific airborne pollutants), and violate patients' privacy.
- *Data evolutions*. Sensor nodes can perform several measurements of quantities of interest over time (e.g., a measuring station can continuously record the noise level in a given area of a city). While a high number of samples allows a more meaningful analysis of a given phenomenon, such repeated measurements can be exploited for inferring sensitive information. For instance,

suppose that *Alice* wants to discover the timetable of the freight trains traversing the railroad passing in San Francisco, which is kept secret by the local train company. Suppose also that the environmental monitoring of the local municipality includes the measurements of the noise pollution in the city. Having access to the measurements collected close to the railway, *Alice* can notice peaks in the noise levels and correlate this information with the public timetables of passenger trains, thus re-constructing the freight trains timetable.

- *Unusual data*. Inferences can also be drawn when the collected environmental data deviate from what is expected or is considered as normal. For instance, suppose that the environmental monitoring of San Francisco shows a high level of radioactivity. If the neighbor cities do not show such a high level of radioactivity, it may highlight the presence of a location storing radioactive material. Otherwise, if the same level of radioactivity is observed also in other cities, the radioactivity in San Francisco can be due to some peculiarities of the soil.
- *Users' locations*. Mobile phones (or smartphones) are nowadays portable computers that everyone uses and carries with her all times. In the near future, we can imagine that our phones will be equipped with new sensors and new applications specifically targeted to the environmental monitoring (e.g., the PEIR project). This implies that environmental monitoring will be directly performed by users, who will collect data related to the locations they visit. Such data have to be tagged with the location in which they have been captured. An adversary able to track the movements of a user can violate her privacy since the adversary can discover user's frequent addresses (e.g., home and workplace), usual movements (e.g., from home to work) and habits, and, accordingly, infer sensitive information about the user. For instance, suppose that *Alice* gains access to the movements of her colleague *Bob*. *Alice* can discover that *Bob* visits every day a clinic for cardiovascular diseases, meaning that *Bob*, or one of his relatives or close friends, suffers form a cardiovascular disease.

IV. Countermeasures

We now describe possible countermeasures that can be adopted to avoid or mitigate the security and privacy risks described in the previous section.

A. Counteracting security risks

The security risks related to the system architecture can be prevented by the hardening of the physical security of the whole system architecture and by adopting intrusion detection systems [27]. Fault-tolerance solutions can also be helpful when an adversary turns out to be successful and some parts of the system report damages. For instance, a simple solution for ensuring the availability of the data stored in the processing node consists in replicating the data on several machines, possibly located in different sites. The classical attacks on the communication channels can indeed be prevented by encrypting the traffic. However, this approach is not always applicable, since data measurements can be performed by sensor nodes with limited computational capabilities. In this case, smarter lightweight solutions are needed (e.g., [11]). Specific techniques have to be adopted for protecting the access patterns in line with the techniques developed in the database field (e.g., [18]). The idea is to change the physical location (blocks of the hard disk) where data are stored at each access. To prevent unauthorized access to the system, an access control mechanism is needed. Since in the considered scenario the identity of the users accessing the data may not always be known in advance, traditional identity-based access control techniques (e.g., [19]) might not be applicable. To overcome this problem, attribute-based access control might represent a viable solution (e.g., [9]). In this case, rather than considering users' identities, the authorizations stating who can access what data are defined by taking into consideration properties (e.g., age, nationality, occupation) of the authorized parties. For instance, suppose that the local municipality of San Francisco aims at giving access to the collected environmental data only to U.S. citizens. To this aim, the access control policy might grant access to users showing that they hold a U.S. passport, regardless of their identity.

B. Counteracting privacy risks

To protect environmental data from inferences it is needed to adopt techniques such that: *i)* the analysis that an adversary can perform on them are limited; *ii)* correlations, associations, and dependencies among data coming from different sources are obfuscated. Intuitively, storing data in encrypted form can represent a possible solution to guarantee the protection of environmental data from inferences. Since however different users can be entitled to access different portions of the data, data encryption should be combined with access control, thus enforcing selective encryption (e.g., [16]). With this strategy, the key with which data are encrypted is regulated by the authorizations holding on the data. In particular, selective encryption ensures that each user can compute all and only the keys of the resources that she can access. When encryption results too heavy or when the encryption of the whole data is an overdue, alternative solutions can be adopted. For instance, there can exist situations in which what is sensitive is the data association, rather than specific data values. For instance, while the release of the list of air pollutants in the area of San Francisco or of the list of places equipped with a sensor might not be considered harmful, the association between the position of a sensor and the measured pollutants concentration can be considered sensitive. In such cases, the privacy of sensitive information can be protected by adopting solutions based on the vertical fragmentation of the data (e.g., [14], [17]). The intuition here is that when the joint visibility of some pieces of information is sensitive, such pieces of information can be split in different portions not joinable. For instance, suppose that the collected environmental data include information about: *i)* the concentration of a pollutant

in an area; *ii)* the area; and *iii)* the owner of the properties within the area. To protect the identities of those individuals who own polluted properties, it is sufficient to split the data in two fragments: one fragment includes the concentration of the pollutant and the corresponding area (with the information about the owners of properties possibly encrypted) and the other fragment includes the information about the owners.

When environmental data are publicly released, the possible countermeasures for their protection depend on the format of the data themselves (see Section II). In case of macrodata, it is possible to protect the data before tabulations (producing a sanitized version of the data collection so that the information reported in a macrodata table cannot be exploited for inferring sensitive information), or after tabulation (finding and protecting those cells that can reveal sensitive information) [15]. For instance, consider a macrodata table reporting the concentration of a pollutant during the day and night for each county of a given region. The cells of the microdata table that contain a high value can be considered sensitive since they indicate that the person living in the high polluted counties may have a high probability of suffering from specific illnesses. The content of these cells need therefore to be suppressed. In case of microdata, privacy can be preserved adapting techniques that, for example, generalize the data (e.g., k-anonymity [26]) while however preserving data truthfulness. Goal of these techniques is to protect either the identities, or the sensitive information of the individuals to whom data refer. For instance, consider the release of an environmental microdata table reporting, for each citizen of San Francisco, the air pollutants concentration measured by her closest sensor in the city. Publishing a k-anonymous version of this table ensures that, broadly speaking, the identity of each respondent can be indistinguishably related to no less than $k-1$ other individuals.

Inferences exploiting observations of users' positions and movements can be counteracted adopting techniques developed for protecting location data. For instance, the privacy of users can be protected by hiding the link between their identity and their sensitive information (e.g., [10]), by degrading the accuracy of the location measurement (e.g., [8]), or by releasing a path shared by multiple users so to make them indistinguishable (e.g., [13]).

V. Conclusions

This paper presented an overview of the main security and privacy issues in environmental monitoring systems. Our work can help in understanding such issues and in designing novel environmental systems and applications that guarantee a privacy-aware collection, management, and dissemination of environmental data.

Acknowledgments

This work was supported by the Italian Ministry of Research within the PRIN 2008 project "PEPPER" (2008SY2PH4), and by the Università degli Studi di Milano within the "UNIMI per il Futuro - 5 per Mille" projects "PREVIOUS" and "Adaptive Systems for Environmental Monitoring".

References

[1] [Online]. Available: http://www.kingcounty.gov/environment/dnrp.aspx
[2] "Global Seismographic Network." [Online]. Available: http://www.iris.edu/hq/programs/gsn
[3] "NSF Polar Programs UV Monitoring Network." [Online]. Available: http://uv.biospherical.com/
[4] "WAVCIS Wave-Current-Surge Information System for Coastal Louisiana." [Online]. Available: http://www.wavcis.lsu.edu
[5] "ZigBee Allianz." [Online]. Available: http://www.zigbee.org
[6] D. Aksoy and A. Aksoy, "Satellite-linked sensor networks for planetary scale monitoring," in *Proc. of VTC 2004*, Los Angeles, CA, USA, 2004.
[7] F. Amigoni, A. Brandolini, V. Caglioti, V. Di Lecce, A. Guerriero, M. Lazzaroni, F. Lombardi, R. Ottoboni, E. Pasero, V. Piuri, O. Scotti, and D. Somenzi, "Agencies for perception in environmental monitoring," *IEEE TIM*, vol. 55, no. 4, pp. 1038–1050, 2006.
[8] C. Ardagna, M. Cremonini, , S. De Capitani di Vimercati, and P. Samarati, "An obfuscation-based approach for protecting location privacy," *IEEE TDSC*, vol. 8, no. 1, pp. 13–27, 2011.
[9] C. Ardagna, M. Cremonini, S. De Capitani di Vimercati, and P. Samarati, "A privacy-aware access control system," *JCS*, vol. 16, no. 4, 2008.
[10] C. Bettini, S. Jajodia, P. Samarati, and X. S. Wang, Eds., *Privacy in Location-Based Applications: Introduction, Research Issues and Applications*. LNCS 5599, Springer, 2009.
[11] C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregation of encrypted data in wireless sensor networks," *ACM TOSN*, vol. 5, no. 3, pp. 1–36, 2009.
[12] C. Y. Chong and S. P. Kumar, "Sensor networks: Evolution, opportunities and challenges," in *Proc. of the IEEE*, vol. 91, no. 8, 2003.
[13] C.-Y. Chow and M. Mokbel, "Trajectory privacy in location-based services and data publication," *SIGKDD Expl.*, vol. 13, no. 1, 2011.
[14] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Combining fragmentation and encryption to protect privacy in data storage," *ACM TISSEC*, vol. 13, no. 3, 2010.
[15] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati, "Microdata protection," in *Secure Data Management in Decentralized Systems*, T. Yu and S. Jajodia, Eds. Springer-Verlag, 2007.
[16] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Encryption policies for regulating access to outsourced data," *ACM TODS*, vol. 35, no. 2, pp. 1–46, 2010.
[17] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Fragments and loose associations: Respecting privacy in data publishing," *PVLDB*, vol. 3, no. 1, pp. 1370–1381, 2010.
[18] S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, G. Pelosi, and P. Samarati, "Efficient and private access to outsourced data," in *Proc. of ICDCS 2011*, Minneapolis, MN, USA, 2011.
[19] S. De Capitani di Vimercati and P. Samarati, "Access control in federated systems," in *Proc. of NSPW*, Lake Arrowhead, CA, USA, September 1996.
[20] A. Genovese, R. Donida Labati, V. Piuri, and F. Scotti, "Virtual environment for synthetic smoke clouds generation," in *Proc. of VECIMS 2011*, Ottawa, Canada, 2011.
[21] A. Genovese, R. Donida Labati, V. Piuri, and F. Scotti, "Wildfire smoke detection using computational intelligence techniques," in *Proc. of CIMSA 2011*, Ottawa, Canada, 2011.
[22] J. K. Hart and K. Martinez, "Environmental sensor networks: A revolution in the earth system science?" *Earth Science Reviews*, vol. 78, no. 3-4, pp. 177–191, 2006.
[23] G. Hoogenboom, "The Georgia automated environmental monitoring network," *Southeastern Climate Review*, vol. 4, no. 1, pp. 12–18, 1993.
[24] P. Kulkarni, D. Ganesan, P. Shenoy, and Q. Lu, "SensEye: A multitier camera sensor network," in *Proc. of Multimedia 2005*, Singapore, 2005.
[25] Q. Li, Q. Hao, and K. Zhang, "Smart wireless video sensor network for fire alarm," in *Proc. of WiCOM 2010*, Chengdu, China, 2010.
[26] P. Samarati, "Protecting respondents' identities in microdata release," *IEEE TKDE*, vol. 13, no. 6, pp. 1010–1027, 2001.
[27] W. Stallings, *Network Security Essentials: Applications and Standards*, 4th ed. Upper Saddle River, NJ, USA: Prentice Hall Press, 2010.
[28] M. Tubaishat and S. Madria, "Sensor networks: an overview," *IEEE Potentials*, vol. 22, no. 2, pp. 20–23, 2003.
[29] G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees, and M. Welsh, "Monitoring volcanic eruptions with a wireless sensor network," in *Proc. of EWSN 2005*, Istanbul, Turkey, 2005.