Delphine Christin, Andreas Reinhardt, Salil S. Kanhere, Matthias Hollick:
Fine-grained Access Control Enabling Privacy Support in Wireless Sensor Networks. In: Reiner Kolla: Proceedings of the 9th GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze", p. 29-32, September 2010.

Fine-grained Access Control Enabling Privacy Support in Wireless Sensor Networks

Delphine Christin*, Andreas Reinhardt†, Salil S. Kanhere‡, Matthias Hollick*
* Secure Mobile Networking Lab, Technische Universität Darmstadt, Darmstadt, Germany
† Multimedia Communications Lab, Technische Universität Darmstadt, Darmstadt, Germany
‡ School of Computer Science and Engineering, University of New South Wales, Sydney, Australia
{delphine.christin, matthias.hollick}@seemoo.tu-darmstadt.de, areinhardt@kom.tu-darmstadt.de, salilk@cse.unsw.edu.au

***Abstract*—The deployment of wireless sensor networks may endanger the privacy of people monitored on purpose or unintentionally. To enhance the control of the surveilled people over their privacy, we propose to introduce a fine-grained access control scheme on monitored data. Towards this end, we design an architecture relying on granular access control and filtering of relevant information, which can be easily integrated with existing wireless sensor networks.**

I. Introduction and Motivations

Wireless sensor networks (WSNs) are deployed to cover a wide range of scenarios ranging from environmental monitoring [1] to medical applications [2]. However, some deployments raise privacy concerns. The threats to privacy are directly identifiable in people-centric scenarios. However, environment-centric scenarios may also threaten the privacy of persons located in the monitored environment, as their current activity could be extracted from sensor data. To ensure that the deployed WSNs are well-received in their communities, respecting privacy is a condition *sine qua non*. Within the scope of this paper, we propose to involve the concerned people in the privacy decisions by introducing a fine-grained access control. The monitored persons are able to select potential data retrievers and pair them with an appropriate degree of granularity applied to the sensor data. Our approach takes into account the privacy preferences of each concerned individual and also optimizes the data collection process. In fact, some individuals may select less restricted privacy settings than the default settings, if they estimate that revealing this information does not affect their privacy.

Our contributions are as follows: We examine related work in Section II. We then analyze representative privacy-sensitive WSN scenarios in Section III in order to identify privacy issues and data retrievers involved. We present in Section IV our concept and the related architecture introducing fine-grained access control in WSNs. Then, we evaluate the proposed approach and highlight the advantages and limitations in Section V. Finally, in Section VI we summarize our discussion and provide an outlook on prospective future work.

II. Related Work

Ensuring *data privacy* and *context privacy* [3] in WSNs has attracted the interest of many researchers. While *data privacy* focuses on the privacy protection of the collected data and queries submitted to the WSN, *context privacy* tackles the protection of location and timing information related to the traffic streams. Several approaches (e.g. [4] and [5]) that use intermediate processing, such as data aggregation, have been introduced to ensure *data privacy* protection on a node-to-node basis. Mechanisms based on variations of the K-anonymity principle [6] have been studied in [7] to guarantee privacy of queries in WSNs. Solutions to ensure location privacy of data sources and base stations have been proposed in [8] and [9], respectively. Random delays [10] may also be introduced to ensure temporal privacy. It can be observed that existing work mainly focuses on the privacy protection of the WSN and that fined-grained access control mechanisms are missing. The AlarmNet project [2] is close to our concept and presents a flexible access control scheme depending on the monitored patient's context and potential health emergencies. The privacy preferences of the patient may be enforced and additional access authorizations may be delivered in case of emergency. This approach clearly introduces some flexibility in comparison with traditional role-based access control [11]; however, the authorized people access the same set of data with the same granularity. Moreover, its applicability is restricted to health care applications, while our scheme may be integrated into a wider range of WSN applications involving monitored people. To the best of our knowledge, we are the first to envisage a fine-grained access control to support privacy in wireless sensor networks. Our aim is to optimize the trade-off between privacy guarantees and information required by the application to fulfill its duties.

III. Selected Privacy-sensitive WSN Deployments

From the multi-dimensional WSN design space [12], we select representative privacy-sensitive scenarios: People-centric and environment-centric scenarios. By monitoring human beings in multiple contexts and environments, people-centric applications raise obvious privacy concerns. In comparison with people-centric scenarios, people are not the core study subjects in environment-centric deployments. However, their privacy may also be threatened, as their activity and location may be monitored in the background. To illustrate both categories of scenarios, we restrict our selection to three representative examples of deployments: Assisted living, monitoring employees, and smart homes. For each example, we identify different

sensed parameters and potential data consumers.

A. People-centric Scenarios

1) Assisted living: Wireless sensor networks are deployed in elderly peoples' homes to monitor their physiological parameters and activities. The deployment consists generally of two subnetworks: A Body Area Network (BAN) and a fixed network, as presented in [2]. Wearable sensors measuring ECG, blood pressure and sugar level may be part of the BAN, while presence detection, temperature and humidity sensors may compose the fixed network. The collected data can interest different groups of people including doctors, nurses, family members and other residents. However, to protect the privacy of the monitored people, these data should not be delivered with the same degree of granularity. Doctors require the entire set of the physiological parameters with the finest degree of granularity to be able to establish a diagnosis as precise as possible, while family members are only able to find out whether the monitored person is at home or in his room. Room temperature information might be made available to all people interested.

2) Monitoring Employees: The employees' current activity can be monitored by sensor nodes deployed in offices and workplaces in order to determine whether they can be interrupted, as presented in [13]. For example, cameras and accelerometers can be used to determine the employees' context. However, sensitive information is gathered and should be carefully disclosed to potential data requestors. Different degrees of granularity are introduced to allow superiors, colleagues, friends or family members to find out the current state of interruptibility of the person of interest. For example, the responses of the system indicates that the person is busy or reveal his activity with a high degree of precision depending on the trust level between the monitored employee and the requesting person.

B. Environment-centric Scenario

1) Smart Homes: Temperature, humidity, brightness, and contact sensors can be disseminated within habitations to measure the ambient conditions and control the Heating, Ventilating and Air Conditioning (HVAC) systems in order to optimize their energy consumption. Different groups of people can exploit these measurements: The residents, the employees of the surveillance company and the firefighters. The residents can consult the sensor data to verify if the measured values correspond to their preferences or adjust them to their needs, while the surveillance company and the firefighters may consult the data to detect intrusions and fires respectively. Authorizing the access to the sensor data with the highest degree of granularity to the residents does not raise any privacy concerns. On the contrary, the privacy of the habitants may be endangered if the surveillance company and the firemen have access to these data and are able to extract the current activities of the residents. For example, if the light is on and the humidity degree increases in the bathroom, it can be easily deduced that somebody is taking a shower. To protect the privacy of the habitants, the sensor data should be delivered to the third parties with a coarser degree of granularity. However, the selected degree of granularity should be sufficient to allow them to detect abnormal events.

The examination of the previous scenarios has showed that distinct categories of people have interests in accessing the sensed data and demonstrated the necessity to introduce different degrees of granularity to ensure privacy. However, proposing a general mapping between categories of data consumers and degrees of granularity is made impossible by the personal nature of the privacy conception.

IV. Concept and Architecture

Based on the observations made in the previous section, we propose an approach to introduce fine-grained access controls supporting privacy in WSNs. We first introduce briefly our concept and we then provide a detailed description of the proposed architecture and the related components.

A. Concept Overview

Guaranteeing privacy in WSNs is a key factor to allow their acceptance by the public. In fact, without any privacy protection mechanism, their deployment may be refused or the monitored people may deactivate the sensing function. In this case, the sensor data collected by the application may be insufficient to deliver reliable results and fulfill its primary function. To avoid such pitfalls, we propose to optimize the trade-off between guaranteeing the protection of privacy and fulfilling the application needs by introducing a fine-grained access control mechanism. The concerned people are able to select the persons authorized to access their data and attribute them different privacy degrees depending on the nature of the data, their privacy preferences and their personal relationships. The mechanism of data delivery is not on a binary basis, available or unavailable, but becomes granular with multiple degrees. Consequently, more parties can benefit from the data without threatening the privacy of the monitored subjects.

B. Architecture

Our concept is based on a two-tier architecture including a WSN and a privacy-enhanced base station, as illustrated in Fig. 1. The base station supports interaction with the monitored persons, as well as potential data consumers.

1) Wireless Sensor Network: The WSN is composed of homogeneous or heterogeneous platforms. We assume that the sensor data are annotated with timestamps and that the base station can identify the type of sensor data. The data are transferred to the base station via traditional routing protocols adapted to characteristics of the deployment. The communication between the sensors and the base station is assumed to be adequately protected against external adversaries by well-established cryptographic techniques e.g. encryption and authentication. The integration of complex techniques using different encryption keys depending on the required level of privacy, such as presented in [14] may also be envisaged. Once the data reaches the base station, their characteristics

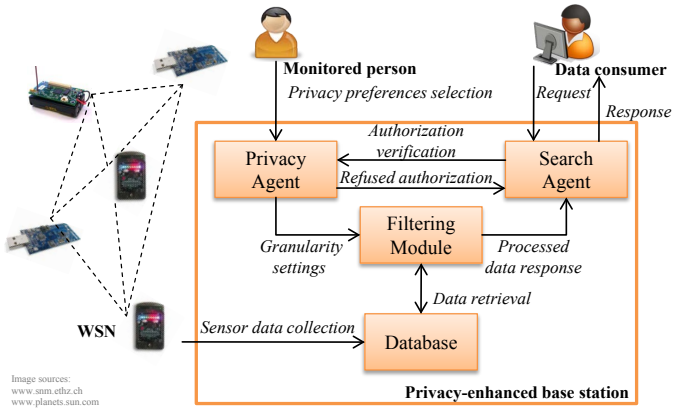

Fig. 1. Proposed Architecture

are extracted (e.g. timestamps, data type) and they are then stored in the database. The database is secured and protected against attackers by means of classical mechanisms.

2) Privacy-enhanced Base Station: It comprises four main components: A search agent, a privacy agent, a filtering module, and a database. The functionalities of these components are successively described in detail in the following paragraphs.

- *Search Agent*: Data consumers can login and search for data through a web interface. They can define different search parameters including e.g. type of data and collection time. These parameters are included into a data request and transmitted to the search agent. The search agent processes it and delegates the authorization verification to the privacy agent. If the data consumer is identified as unauthorized by the privacy agent, the search agent displays an "access denied" message. Otherwise the search agent displays the response provided by the system, once the full processing cycle is achieved.
- *Privacy Agent*: Each monitored person can define his/her privacy preferences through a dedicated interface. The privacy preferences include a list of authorized people mapped with a particular degree of granularity for each type of sensed data. The privacy agent stores, manages and maintains these privacy preferences. When a data request for accessing a particular data is received by the search agent, it forwards the same to the privacy agent. The privacy agent verifies the access authorization set by the concerned person(s). In case of diverging privacy settings between multiple monitored persons, the privacy agent selects the strictest preferences in order to ensure the maximal privacy guarantees for each person. For example, Alice and Bob are monitored in the same room and Alice authorized Carol to access her data with a high degree of granularity, while Bob did not mention Carol in his list of authorized people (or indicate a lower degree of granularity than Alice). Carol will thus not be authorized to access the requested data (or only with the lowest degree of granularity set by Bob). When the authorization is checked and the degree of granularity determined, the privacy agent transmits a data request including the corresponding data and granularity settings to the filtering component.
- *Filtering Module*: The filtering module is composed of different submodules. Each submodule supports a unique type of data and is able to extract different degrees of granularity from the sensor data. The amount and nature of the submodules is influenced by the WSN application and the deployed sensors. Moreover, the complexity of the processing depends on the nature of the sensor data. For example, extracting distinct degrees of granularity from temperature data requires simpler processing than from captured sounds. Once the filtering module receives the data request from the privacy agent, it retrieves the data from the database and conveys it to the dedicated submodule by indicating the desired degree of granularity. As soon as the processing is achieved, the resulting data are transmitted at the appropriate level of granularity to the search agent.

V. Evaluation and Discussion

To complete the presentation of our approach, we conduct a preliminary evaluation of our concept and highlight the key advantages and limitations. The discussions focus on two main dimensions: Technical and human aspects.

From a technical point of view, our approach can be integrated into a wide range of WSN applications without requiring major modifications of the WSN deployment. The protocols and mechanisms applied within the WSN remain unchanged. However, sensor registration or data annotations are required to identify the type of data sensed and to apply the correct processing in the filtering module. If no scheme to identify the data type is supported in the existing WSN, its introduction may cause additional overhead and complexity. The design and implementation of the base station would require some modifications in order to introduce the agents discussed in Section IV. The functionality of the privacy and search agent would not differ to a large extent from one application to another. Only the available types of sensor data have to be adapted in the selection of the privacy settings and the search process. Therefore, a generic design can be developed and easily reused by adapting the data types to the application requirements. Similarly, a library of submodules for the filtering module covering a large range of sensor data to process could be designed and implemented. By maintaining their structure modular and loosely coupled, such submodules could be integrated easily. Nonetheless, the dependencies of the architecture on the sensor data types limit the flexibility of the WSN. For each new sensor type introduced within the WSN, an additional submodule has to be added into the filtering module.

Considering the human dimension, our concept introduces a novel perspective for the monitored people by involving them in the privacy decisions. Instead of employing static and generic privacy protection mechanisms, the concerned people can tune the privacy settings (authorized parties and associated granular data) according to their preferences. In

comparison with existing work, our approach allows to take into account different privacy conceptions of individuals that cause potential conflicts between the concerned parties. Multiple monitored people may have conflicting privacy settings, as described in detail in Section IV.B. In this case, the strictest privacy settings among the conflicting settings are adopted to provide the maximal privacy protection. The privacy of the monitored people is therefore not jeopardized. Additionally, the selected privacy settings may be stricter than the minimal degree of granularity required by the application. Depending on the application scenario, the person can choose to modify her settings or leave the deployment, or the application enforces the privacy preferences in case of emergency. In the latter case, the notion of emergency should be clearly defined and the monitored people well-informed of such potential enforcements. Furthermore, we assume that each monitored person is able to define her privacy preferences. This assumption requires that the monitored people are known and identifiable. The applicability of our concept may therefore be limited in particular deployments, such as in public areas e.g. train stations, where people are entering and leaving the monitored location frequently. However, the crowd present in such locations protects to some extend the privacy of the monitored people, as personal data are difficult to extract.

VI. Conclusions and Outlook

In this paper, we have analyzed representative privacy-sensitive WSN scenarios and highlighted that privacy can be partially supported by allowing data access with different degrees of granularity depending on the nature of the relationships between the monitored people and the data consumers. We have then described our concept to introduce fine-grained access controls in WSNs and have proposed an architecture supporting the deployment of our approach in real scenarios. We have detailed the functionality of each component of the proposed architecture. Finally, we have conducted a preliminary evaluation of our concept to highlight the advantages and limitations of our approach by focusing on the technical and human perspectives.

In conclusion, our approach provides a generic solution adapted to a wide range of privacy-sensitive WSN scenarios demanding only limited adaptations to the application characteristics. By employing our concept within WSN deployments, the trade-off between privacy respect and application needs is optimized. Instead of disabling partially or completely the sensing capability of the deployment rendering the application inoperative to protect their privacy, the monitored people can finely define access authorizations including authorized parties and corresponding degrees of granularity. Moreover, the direct involvement of the monitored people in the privacy decisions and privacy setting selection may improve their acceptance of WSN deployment, as they have a direct influence on the mechanisms employed to protect their privacy.

A. Outlook

As future work, we plan to provide a proof-of-concept of our approach to complete the conducted conceptual evaluation. The implementation will include an extensive library of sub-modules for the previously defined filtering in order to provide off-the-shelf components that may be combined effortlessly in multiple combinations depending on the sensor data types. Additionally, we will pay particular attention to the design of interfaces used by the monitored people to select their privacy preferences. In fact, the selection process may rapidly become cumbersome for the user, if it includes the personalization of numerous parameters. Usability and simplicity will therefore be particularly considered.

In a second phase, we foresee to expand this approach to other platforms and build hybrid networks composed of traditional sensor platforms (e.g. Mica2, SunSPOT) and personal end devices (e.g mobile phones). Such mixed networks will benefit from the sensors embedded in the personal end devices providing mobility patterns, as well as convenient interfaces to support direct interactions between the monitored people and the network infrastructure.

Acknowledgment

This work was supported by CASED (www.cased.de).

References

[1] K.Martinez et al., "Glacsweb: A Sensor Network for Hostile Environments," in *Proc. of the Sensor and Ad Hoc Communications and Networks Conference (SECON)*, 2004.

[2] A. Wood et al., "Context-Aware Wireless Sensor Networks for Assisted-Living and Residential Monitoring," *IEEE Network*, 2008.

[3] N. Li et al., "Privacy Preservation in Wireless Sensor Networks: A State-of-the-art Survey," *Ad Hoc Networks*, vol. 7, no. 8, 2009.

[4] W. He et al., "PDA: Privacy-Preserving Data Aggregation in Wireless Sensor Networks," in *Proc. of the IEEE International Conference on Computer Communications (INFOCOM)*, 2007.

[5] W. Zhang et al., "GP^2S: Generic Privacy-Preservation Solutions for Approximate Aggregation of Sensor Data," in *Proc. of the IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2008.

[6] L. Sweeney, "k-anonymity: A Model for Protecting Privacy," *International Journal of Uncertainty Fuzziness and Knowledge Based Systems*, vol. 10, no. 5, 2002.

[7] B. Carbunar et al., "Query Privacy in Wireless Sensor Networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 2, 2010.

[8] P. Kamat et al., "Enhancing Source-Location Privacy in Sensor Network Routing," in *Proc. of the IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2005.

[9] J. Deng et al., "Decorrelating Wireless Sensor Network Traffic to Inhibit Traffic Analysis Attacks," *Pervasive and Mobile Computing*, vol. 2, no. 2, 2006.

[10] P. Kamat et al., "Temporal Privacy in Wireless Sensor Networks," in *Proc. of the International Conference on Distributed Computing Systems (ICDCS)*, 2007.

[11] D. Ferraiolo et al., *Role-based Access Control*. Artech House Publishers, 2003.

[12] K. Römer et al., "The Design Space of Wireless Sensor Networks," *IEEE Wireless Communications*, vol. 11, no. 6, 2004.

[13] A. Reinhardt et al., "Towards Seamless Binding of Context-aware Services to Ubiquitous Information Sources," in *Proc. of the International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)*, 2010.

[14] M. Shao et al., "pDCS: Security and Privacy Support for Data-Centric Sensor Networks," in *Proc. of the IEEE International Conference on Computer Communications (INFOCOM)*, 2007.