WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2010; **10**:1193–1207
Published online 29 September 2008 in Wiley Online Library
(wileyonlinelibrary.com). DOI: 10.1002/wcm.678

Towards adaptive security for convergent wireless sensor networks in beyond 3G environments

Anelia Mitseva[1*,†], Efthimia Aivaloglou[2], Maria Marchitti[1], Neeli Rashmi Prasad[1*,†], Charalabos Skianis[2], Stefanos Gritzalis[2], Adrian Waller[3], Tim Baugé[3] and Sarah Pennington[3]

[1]*Networking and Security Section, Center for TeleInFrastruktur (CTIF), Aalborg University, Niels Jernes Vej 12, 9220 Aalborg East, Denmark*
[2]*Laboratory of Information and Communication Systems Security (Info-Sec-Lab), Department of Information and Communication Systems Engineering, University of the Aegean, Karlovasi, Samos, GR-83200, Greece*
[3]*Thales Research and Technology (UK) Ltd., Worton Drive, Worton Grange, Reading, RG2 0SB, U.K.*

Summary

The integration of wireless sensor networks with different network systems gives rise to many research challenges to ensure security, privacy and trust in the overall architecture. The main contribution of this paper is a generic security, privacy and trust framework providing context-aware adaptability, flexibility and scalability which allows customisation of wireless sensor networks to a diverse set of application spaces. Suitable protocols and mechanisms are identified, which when combined according to the framework form a complete toolbox solution which fits the architecture of Beyond 3G environments. Performance evaluation results demonstrate the feasibility and estimate the benefits of the security framework for a variety of scenarios. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: security management; adaptive framework; wireless sensor networks; context-aware; privacy; trust

1. Introduction

Sensor networks are set to become a truly ubiquitous technology that ambient intelligence applications will rely on for gaining context-awareness capability. Through capturing information via numerous sensors spread over sensing fields, Wireless Sensor Networks (WSNs) will allow for the provision of sophisticated, unobtrusive and context-aware applications related to different objects—individuals, equipment, buildings and services integrated with Beyond 3G (B3G) environments. It is envisioned that B3G networks will integrate technologies from broadcasting networks to wide area and metropolitan networks down to smaller networks like wireless local and personal area networks, all under the umbrella of a single, monolithic, IP-based core network [1]. B3G environments will provide a framework for adequate connectivity for

*Correspondence to: Anelia Mitseva and Neeli R. Prasad, Networking and Security Section, Center for TeleInfrastruktur (CTIF), Aalborg University, Denmark.
†E-mails: mitseva@es.aau.dk, mitseva@yahoo.com, np@es.aau.dk

Copyright © 2008 John Wiley & Sons, Ltd.

data delivery. On top of the connectivity, open architectures and platforms for service control and delivery will allow a wealth of communication services and applications to be offered to users and businesses [2]. The integration of ubiquitous WSNs in B3G mobile systems is the main objective of the e-SENSE project, aiming to contribute to the evolution and definition of the future Ambient Intelligent Mobile Systems beyond 3G by providing a toolbox approach [3]. Such a toolbox approach is necessary in order to satisfy the diverse requirements from different sensor network applications and scenarios.

The security and integrity of the data and the communications are essential requirements for the end applications and services to be reliable, while the protection of the privacy of the end users is essential for their adoption. Privacy concerns arise mainly because different types of sensor networks may be deployed for different purposes and will have different levels of trust. Hence, the diverse security, trust and privacy requirements of the applications, services and nodes impose the need for an adaptive, scalable and flexible security framework.

The main contribution of this paper is the proposal of a generic context-aware framework for security, privacy and trust services which maps a relevant level of each service to the application space's requirements. For the security services, existing protocols are identified based on their applicability. For the privacy services, the focus is on proposing a novel context-aware mechanism for controlled information disclosure, while for ensuring pseudonymity and anonymity, existing solutions are evaluated. For the trust establishment, a novel adaptive mechanism is proposed.

The principal distinctive aspect of B3G environments is the heterogeneity of the various access systems that will be combined into a common, flexible and seamless platform to complement each other in an optimum way for different service requirements [1]. This calls for flexible, scalable and adaptable solutions, and is the motivation for proposing the following core properties:

- *Flexibility and Scalability*—reconfigurable framework to provide the most suitable levels of security, trust and privacy functionality for different node architectures, hardware limitations, user requirements and application spaces. Essentially, different versions of the framework can be deployed for the network components, providing varying levels of security functionality.
- *Adaptability*—ensuring that the system works at the best of its capability, taking into account the trade-off among device constraints, change in context and different users' preferences. Essentially, the security protocols and primitives that are used for each communication after the network deployment are selected according to the context of the communication.

For example, the framework is *flexible* in order to allow for different versions of it to be deployed for a B3G gateway and a small sensor node, given that they have both different hardware limitations, and communication and security requirements. The framework is *adaptable* in order to allow for different protocols and primitives to be applied after deployment for the communications within the nodes of a body sensor network, and the communications between cluster heads and gateways.

The rest of the paper is organised as follows: Section 2 describes the application spaces, the integration of WSNs in the B3G environment and the security requirements and research challenges. An overview of the proposed adaptive security architecture is presented in Section 3 while Section 4 describes the components in more detail. The framework is applied in an example scenario in Section 5, and discussed and evaluated in Section 6. Related work is presented in Section 7. The paper is concluded in Section 8.

2. Setting the Scene: Wireless Sensor Networks in the B3G environment

2.1. Application Spaces

The application space that each sensor network application is designed for influences the services that are provided to the end users, the contexts and types of information to be captured, the types of sensor nodes that are utilised and essentially the security requirements and the sensitivity of the information collected and communicated. In order to cover a wide range of contexts and business cases, the application spaces under investigation here, are personal, community and industrial (given in Table I). In the following sections, the security framework will be presented from the point of view of a wireless hospital use case. The necessity for adaptive and context aware security management for WSNs used in medical scenarios has been described and analysed in Reference [4].

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

Table I. The services, the types of sensor networks and the measured phenomena.

Application space	Personal services	Community services	Industrial services
Theme	Lifestyle assistant	Wireless healthcare	Remote asset monitoring
Use cases	Mood based services Entertainment Nutrition	Wireless hospital Residential health monitoring Emergency coordination	Store of the future Food processing Tracking
Types of sensor networks	Body sensor network-type sensors represent the majority of sensors, indicating an emphasis on user context. Environmental-type sensors are used to capture physical phenomena in the user's surroundings	Body Sensor Network-type sensors represent the majority of sensors, indicating an emphasis on user context. Environmental-type sensors are used to capture information about the patient's close surrounding area	A combination of body sensor network and environmental sensors are used to acquire information about goods position, transportation conditions and environmental conditions
Phenomena	Related to the users	Within the vicinity of non-human entities	Environmental context
Information	Physiological, movement, location or social presence information		Condition and position of equipment and products

2.2. Integration of Wireless Sensor and B3G networks

The so called 'second generation wireless sensor networks' model merges hybrid hierarchical architectures comprising of various types of WSNs that are connected via gateways to a core network [5]. The sensor nodes form a network with a star or a mesh topology. The core network can be a B3G mobile communication system or a conventional wired backbone network. A WSN is comprised of nodes with different roles (source, sink and forwarding nodes) of different types (end nodes, clusterheads, coordinators and gateways), and with a diverse range of power, memory and computational capabilities. The gateways, for public or personal use, are responsible for the establishment of the required interconnections and, in order to be independent of the used B3G network access technology, they need to be equipped with appropriate network protocol conversion mechanisms.

For example, in a wireless hospital scenario where WSNs are deployed for remote monitoring of the patients' vital functions and the medical personnel's locations and stress levels, the boundaries of the B3G network can be set as the hospital terminals gathering data from the patients' body sensor networks and the handheld devices that the medical personnel are carrying. From a security point of view, access control is an important consideration related to the gateway functionality. The communication flows that are required for the various application spaces and need to be secured are both between sensor nodes of the same network and between sensor nodes and external entities through the gateways.

2.3. Security Requirements and Research Challenges

Depending on the application space and the role of each node in the network, the security requirements for the nodes and the information communicated are highly diverse. Diversity exists in the types and roles of sensor nodes utilised, their computational capabilities, their mobility model, the possibility of their regular maintenance and the type of information they collect. Some nodes may generate information whose correctness and freshness is crucial, thus requiring strong integrity protection, while others may generate information that has high confidentiality needs. This imposes the need for security, privacy and trust mechanisms which intelligently adapt to the context of each communication.

The general objective of this work is to define how lightweight security services will be provided within the overall network architecture, in a way that effectively covers the diverse security needs of the scenarios. The basic security issues that need to be addressed are data confidentiality and integrity, controlled disclosure, authentication and access control and management and establishment of trust relationships. The approach adopted for the design of the security framework aims to:

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

(1) Support the diverse security needs that are identified in the application spaces
(2) Support the diversity of the roles and capabilities of the nodes
(3) Explore and use the available context information to provide adaptability and flexibility in the system
(4) Cover the complete set of security requirements of the devices within the network.

To support the diversity in the types of nodes, networks and contexts, a flexible security architecture is defined in the next section, based on a modular approach for the design of the various protocol and control entities. To ensure the flexibility of the architecture, the appropriate protocol elements are selected and configured according to the role of the sensor nodes and the application requirements.

3. Adaptive Security Architecture—Integration Framework

3.1. Proposed Adaptive Security Framework

The proposed security framework is implemented by a cross layer Security Manager, positioned in the Management Subsystem of the e-SENSE protocol stack [3], depicted in Figure 1. The e-SENSE protocol stack architecture is decomposed into four logical subsystems, namely the Application Subsystem, hosting one or several sensor applications, the Middleware Subsystem, providing data transfer services for the transport of the application data packets, the Connectivity Subsystem, consisting of functions required for operating the physical layer, the medium access control and the network and transport layer, and the Management Subsystem, responsible for the configuration and initialisation of the stack. Each subsystem comprises various protocol and control entities, which offer a wide range of services and functions at service access points to other subsystems.

The security framework is designed as a cross-layer Security Manager, which defines flexible and context-aware services related to data security, privacy and trust at different levels of the protocol stack and related to different communication needs. A toolbox approach is followed for the Security Manager, with some of its components being optional for scaled-down versions of it.

The *Protocols and Mechanisms* component is the most fundamental, since it is the one required for all types of nodes in the network. It contains the security primitives necessary to implement several security protocols in a way that is transparent to the layers above it in the protocol stack. The adaptivity of the

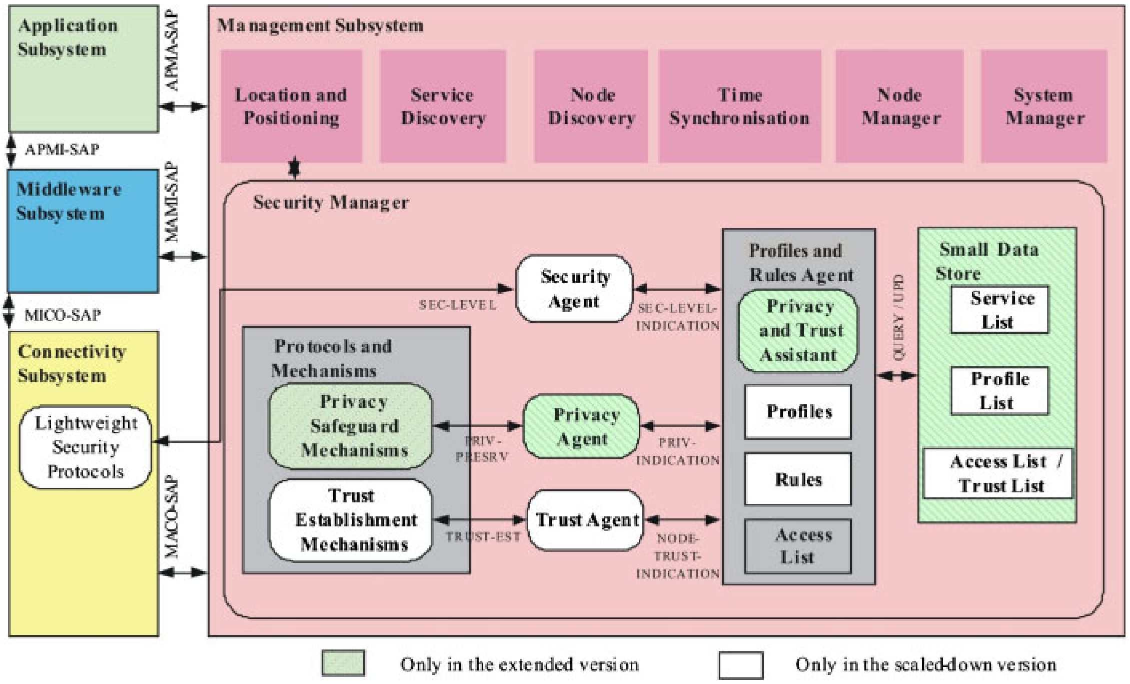


Fig. 1. Generic adaptive security framework within the e-SENSE protocol stack—scaled-down and extended versions.

Copyright © 2008 John Wiley & Sons, Ltd.

security mechanisms is ensured by the *Security Agent*, responsible for determining the most suitable security mechanisms and protocols for every message exchange. Decisions on the cooperation of nodes are based on their trust status, provided by the *Trust Agent*, while the *Trust Establishment Mechanisms* block is responsible for determining the trust status for unknown nodes. The *Privacy Agent* is responsible for determining if and in what form data should be disclosed, and for invoking the *Privacy Safeguard Mechanisms*, that interfere with the data by filtering it before any disclosure, by allowing or forbidding it, or by pseudonymising it. The *Privacy and Trust Assistant* is an application support component, existing only in user-related full-function nodes (for example a smart phone or PDA) and provides the interface between the user and the device for the configuration of data privacy policies and trust relationships.

The *Profiles and Rules Agent* interfaces with the Security, Privacy and Trust Agents for the exchange of security, privacy and trust definitions respectively. The Profiles and Rules Agent sends requests to the *Small Data Store* to get or modify (if required) the Security Level, Trust Level and profile information that are stored in the respective lists' entities. The context information that can lead to reconfigurations comes from S*ervice and Node Discovery*, *Location and Positioning* and the *Applications*.

Within the protocol stack implemented in any sensor node, cluster head or gateway, the Security Manager interfaces with various layers. The Security Agent interfaces with the connectivity layers for the configuration of the Protocols and Mechanisms component. The Trust Agent interfaces with the connectivity layers for the exchange of security protocol messages with peer nodes, and for the establishment of trust relationships. The Security Manager also offers its services to other layers of the protocol stack. Security requirements can come from the application layer; privacy policies and trust relationships could be obtained directly from the user with the help of the Privacy and Trust Assistant.

3.2. Ensuring Adaptability and Flexibility

Adaptability is supported by the proposed security framework in several ways. Firstly, with the help of the Security Agent, Security Levels are assigned for each communication (Table II), that determine the security mechanisms that are applied, according to its security needs. For example, in the wireless hospital use case where a BSN is attached to the patient's body and communicates data via a handheld device which acts as a gateway, the *Low* Security Level could be assigned when the patient is at home and the *High* level when he is in a public place. Secondly, adaptability is supported by the representation and establishment of various trust relationships between communicating parties by the Trust Agent. Finally, the Privacy Agent is responsible for determining if data should be disclosed, and if it should be provided anonymously according to the data sensitivity. Privacy level flags indicate how the user wants the data in question to be handled and revealed by the privacy agent.

Table II. Ensuring adaptability and flexibility.

Security levels	*Low*—provides non-privileged services and allows exchange of non-sensitive data *Medium*—provides limited protection, even if the data exchanged within the WSN is not necessarily sensitive *High*—provides privileged access to service and/or exchange of highly sensitive data
Trust status	*Unknown*—devices that enter the network and request access to some service for the first time *Untrusted*—devices that are not allowed to access the network for any reason even if they have previously been granted access *Trusted*—devices that have previously established a trust relationship and already share a trust key with the WSN
Privacy level flags	*Always give*—give data without asking the user for confirmation *Check with the profile agent*—check device profile for exception list and priority rules from rules manager before giving the data *Ask the user*—ask the user before handling sensitive data *Never give*—never disclose the sensitive data

Flexibility is ensured by enabling the role, capabilities and security needs of each node in the network to define the subset of Security Manager components which reside in the node. The extended version of the security framework applies to the coordinator and gateway nodes as well as to simple nodes without very harsh memory, battery and computational constraints (Figure 1). The scaled-down version does not include the Privacy Agent, the Privacy Safeguard Mechanism, the Privacy and Trust Assistant or the Small Data Store. As some fundamental information from the Data Store is necessary, the simpler and essential tables containing the minimum required policies, profiles and access list are stored in the Profiles and Rules Agent as a small Access Lists component. In the wireless hospital example, the extended version of the security framework resides in the handheld while the end sensor nodes from the BSN have the scaled-down version. The Security Manager residing in the handheld is responsible for defining the level of security and trust services for the communications with the BSN on one side and with external networks on the other. It also gives the end-user the possibility to set up rules for disclosing sensitive information to other networks and different requesting parties, and for the anonymisation of data. The scaled-down version residing in a sensor node from the BSN, because of the very limited power, memory and computational capabilities, only performs a specific security mechanism as requested by the Security Manager in the handheld device.

In addition to the components that might be omitted, others allow for lighter versions to be deployed, in order to provide only a subset of the services defined. The Protocols and Mechanisms component may support only a subset of the Security Levels. For highly constrained nodes with a strictly defined role, one Security Level may suffice for its communications with the cluster head. Moreover, the Trust Establishment Mechanisms are required for nodes that, during the network lifecycle and without reconfiguration, will need to communicate with nodes other than those they were initially configured to trust. Nodes might be equipped with a subset of the mechanisms defined, depending on their computational capabilities, their role in the network and their communication needs. In Figure 1, the two versions presented (scaled-down and full) are not strict regarding their components, since some components are customisable. Since the components are themselves customisable, this essentially enables many more than two versions to be deployed (i.e. additional intermediate versions).

4. Description of the Components

4.1. Security Agent

The Security Level is re-evaluated whenever there is a change in the network state, the device state, the surrounding context or when the user requests a level of data protection other than the current one. The Security Levels determine the mechanisms and protocols that are used to provide authentication, encryption, message freshness and integrity for each request. Table III includes a list of mechanisms that can be used for each Security Level. The list is indicative, since the mechanisms for each Security Level should be decided according to the criticality and the security needs of the scenario.

Table III. Indicative list of mechanisms that can be used for each security level.

Security level	Location/scenario	Type of service/data	Device requirement	Example protocols and mechanisms
Low	• Inside home environment • Wildlife monitoring	• Environment status • Acknowledgment • WSNs in industry or wildlife monitoring	• The lightest platform, tiny sensor device hardware constraint	• Authentication based on the identities claimed by nodes or use of symmetric network and group keys • Optional encryption • 0/32 bit integrity • Optional freshness
Medium	• Plant, office or shop monitoring • Inside known environment • Disaster situation • Vehicular scenario	• Location status • Object presence/moving object sensor • Application to robotics • Safety application for vehicles	• Medium capability platform, sensor hardware constraint	• Pairwise authentication using symmetric link keys and μTESLA for source authentication • 32/64 bit integrity • Relative freshness through message sequence numbers
High	• Inside public environment • High interference/adversary environment (e.g. airport) • Communication through public network	• Medical and health status • Sensitive and private data • Human centric application	• The highest capability platform, sensors with higher hardware capability	• Authentication through elliptic curve digital signatures • Asymmetric encryption • 64/128 bit integrity • Strong freshness through timestamps

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

The most appropriate current Security Level is determined as a function of the trade-off amongst the application/user requirements, policies, context, power and computational constraints. One approach for introducing flexibility in the encryption process in this framework is to use a combination of different parameters of RC5 as presented in Reference [6]. The assumption is that the shorter the key lengths are and the smaller the number of rounds is, the weaker the algorithm is. The three Security Levels are introduced as a combination of block length, different number of rounds and different key length.

For light-weight authentication and robustness against brute force attack in the strongest Security Level, Diffie-Hellman combined with Elliptic Curve Equations is considered [7,8]. For low levels of security, symmetric network and group keys could be used for authentication and integrity protection through 32/64 bit MACs. For medium levels of security, symmetric link keys are proposed for two-party authentication, together with μTESLA for authenticated broadcast through delayed key disclosure [9].

4.2. Trust Establishment

During the network lifecycle, some nodes will need to cooperate with nodes and networks that they are not pre-configured to trust. The trust establishment procedure assigns trust levels to unknown devices, for which no pre-deployment knowledge exists. It is an independent security service, performed by the Trust Agents of the communicating parties. The result of the procedure is the trust level assigned to the other node. The adaptive trust establishment process that is presented in Reference [10] is used by the Trust Agent, in order to support the diversity in the roles and the capabilities of the nodes in the deployments. The trust associations between any trust issuer i and any trust target j that it supports can be established:

(1) Prior to deployment through storing locally at each node information on its trust associations.
(2) As hierarchical trust relationships so that each node j is considered trusted by node i if it holds a valid certificate that i can verify using the stored public key of an offline trust managing authority that it has a trust association with. For generality, we take a view of a signed certificate from an offline trust managing authority as a recommendation with the highest trust value.
(3) By a cooperative procedure, where i asks for recommendations for j from nodes that it has a trust association with.
(4) Evaluated and made available by supervision nodes that perform behaviour-based trust evaluation [11,12], and i has a trust association with.

Once the Trust Agent receives a request for the trust value of a node, it determines the trust relationship with it by following Table IV, which describes the supported trust evidence for each type of trust

Table IV. Trust establishment evidence and evaluation [10] and privacy aspects and approaches.

Trust relationship between i, j	Evidence	Evaluation
Pre-established	Stored $T_{ij} \leq 1$, $R_{ij} \leq 1$	Not required
Hierarchical, trust managing authority x	Stored $T_{ix} \geq T_{\text{threshold}}$, Stored $R_{ix} \geq R_{\text{threshold}}$, Stored public key of x, Signed certificate of j	Validation of certificate $\Rightarrow T_{xj} = 1$ used as a recommendation
Distributed, set N_i of neighbouring nodes and supervision nodes	Stored $T_{ix} \geq T_{\text{threshold}}$, Stored $R_{ix} \geq R_{\text{threshold}}$, T_{xj}, $\forall x \in N_i$	Combination of recommendations
Privacy aspects and approaches		
Controlled information disclosure	• Policy-based • Role-based	
Node anonymity	• Pseudonym creation schemes • Group formation to increase the silence periods • Capability-based privacy-preserving scheme	
Controlled data access	• Hierarchical team-based access control • Secure multi-party access control	
Location anonymity	• Data cloaking • Mix-zones • Mix-contexts	

evaluation. If a trust association is not already established either before deployment or as a result of a previous trust establishment procedure, node i first attempts to establish a hierarchical and then a distributed trust relationship.

A trust association contains two metrics, namely the trust metric T_{ij} and the transition metric R_{ij}. Both of these metrics should have values above a certain threshold for i to accept recommendations from j for other nodes. The first is the trust value $T_{ij} \in [-1, 1]$, evaluated uniformly both for hierarchical and for cooperative trust establishment based on the recommendations from third parties.

The transition metric $R_{ij} \in [-1, 1]$ is the second part of a trust association, used to indicate a weight that node i will assign to future recommendations from node j. An example of the usability of a separate metric is that, during the initial configuration of a node in a cluster, it can be greater than zero only for the cluster head, so that i accepts recommendations only from it and not from the other nodes that it trusts. This metric is also used as the means to control trust evolution and spreading according to the level of distrust that each node should exhibit during its lifetime towards unknown parties.

There exist several choices for the functions used for the evaluation of T_{ij} and R_{ij}. Examples can be found in Reference [10]. This trust establishment scheme adapts to the needs of nodes that have strictly defined roles in the network or have limited computational capabilities through restraining the set of pre-established relationships that recommendations are accepted from. In the referred use case, a sensor node of a BSN that is pre-configured to trust only its cluster head c, without allowing it to provide recommendations through setting $R_{ic} \leq R_{\text{threshold}}$, will never establish trust relationships with other nodes.

4.3. Privacy Protection

Protecting the privacy of personal or corporate communicated data entails more than ensuring its confidentiality. Privacy protection itself has many aspects, for example information and location privacy, sender and receiver anonymity, unlinkability or prevention of sensitive data collection. Different privacy protection mechanisms are applied to different layers.

The approach taken in this work is to allow the privacy safeguard mechanisms to intervene by filtering the data before any disclosure (by allowing or forbidding it) as a first step, and after that, if necessary, to anonymise or pseudonymise it.

For controlled information disclosure the Privacy Agent evaluates the current context and the privacy policies to decide how to protect the sensitive data. The privacy flags are used to determine how particular pieces of sensitive data of varying granularity should be treated before disclosing (more details can be found in Reference [13]). In the referred to use case, protected user data could be medical status, medical history, contact information, etc., which the patient decides how to reveal to different requesting parties (e.g. doctor, nurse or administrator). Open issues which exist here are: the trade-off between perfect unlinkable anonymity and performance degradation; duration of pseudonyms; when is the best time for a pseudonym to be changed based on evaluation of (1) the most suitable context, (2) requirements coming from different application classes and (3) users themselves. Table IV provides an overview of some of the approaches under consideration for which more information can be found in Reference [14]. In the wireless hospital use case, a combination of these approaches (like in Reference [4]) can be applied to fully protect privacy.

5. Example Configuration

In the wireless hospital use case, the extended version of the security framework in Figure 1 will reside in the handheld, while the end sensor nodes from the BSN will have the scaled-down, lightweight version. The Privacy Agent, the Privacy Safeguard Mechanism, the Privacy and Trust Assistant and the Small Data Store will thus be omitted from the BSN nodes. Some components of the framework will require further configuration:

- The Protocols and Mechanisms component of the BSN nodes may not need to support the *High* Security Level. Especially if the BSN is intended to be used only within the controlled environment of a hospital, symmetric encryption for the communications between the BSN nodes and the handheld device might suffice.
- Based on pre-deployment knowledge of the network topology and the information flows, the alternative options for trust establishment of the Trust Establishment Mechanisms component will be restricted for the BSN nodes that will never during the network lifetime need to perform certificate validations or combinations of recommendations. In this scenario, it should be allowed only for the gateway

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

c to expand the trust relationships in the cluster. For this reason, for the BSN nodes only R_{ic} should be set above the threshold before deployment, and d_i should be set to zero. The initial trust associations of the gateway could allow it to have more flexibility.

During the network lifecycle, from all protocols and security primitives that are included in the framework, the BSN nodes shall only perform symmetric encryptions for the communications with the gateway, shall trust and accept recommendations for new BSN nodes only from the gateway, and shall perform no privacy protection operations.

From several experimental evaluations of the energy consumption of security protocols [15–17], it is known that symmetric cryptographic operations are considerably less costly than asymmetric operations, and lightweight symmetric cryptographic algorithms are considered acceptable for resource-constrained sensor nodes. The energy costs of symmetric cryptographic operations on Mica2 sensors, with a 7.3728 MHz ATmega128L microcontroller, 128 KB of program memory and 4 KB of data memory, were measured in Reference [16] and summarised in Table V. Similar evaluations for asymmetric operations show that elliptic curve cryptography is considerably less costly than traditional public key cryptography [7,15,17]. The energy costs of asymmetric cryptographic operations on Mica2dot sensors (Table V), with a 4 MHz ATmega128L 8-bit microcontroller, were measured in Reference [17].

These measurements are the main reason for suggesting symmetric cryptography for the first two and ECC for the third Security Level which, as shown in the example configuration, will only be used for the communication of devices like cluster heads or gateways. What the adaptivity property of the framework essentially ensures is the minimal use of resources through the selection of the optimal mechanisms and security primitives for each communication.

Table V. Energy cost for MICA2.

Impact of 29-bytes payload cipher (CBC mode) on CPU consumption on MICA2 [16]		
Algorithm	Time (ms)	Energy (μJ)
SkipJack	2,16	51,84
RC5	1,50	36,00
RC6	10,78	258,72
TEA	2,56	61,44
Energy cost of asymmetric computations on MICA2 [17]		
Algorithm	Signature (mJ)	Verification (mJ)
RSA-1024	304	11,9
ECDSA-160	22,82	45,09
RSA-2048	2302,7	53,7
ECDSA-224	61,54	121,98

6. Evaluation and Discussion

In this paper we have described an adaptive and flexible security framework for WSNs that allows for the provision of sophisticated, unobtrusive, context-aware applications and services. Memory, storage space and processing power can be severely limited on some nodes, and this has been addressed by allowing the framework's components to be simplified or even left out according to each individual node's capabilities. For example, the simplest nodes could implement policies as 'if-then-else' statements, whereas more capable nodes requiring sophisticated policy management can implement policy databases, and even expert systems. Battery lifetime can be an issue for some nodes, and this is particularly affected by communications overhead. This overhead will be increased by the need to send trust management messages, and perhaps to distribute policy updates. Such messages will be infrequent; however, future work will need to look at their impact and potential optimisation. Having said that, the adaptability that the framework provides may lead to significant savings in battery power. Without this adaptability, the standard security approach often provides the highest level at all times to protect data. In practice, several factors may affect the benefits from the security framework achieved. Some of the relevant factors for the lightweight security mechanisms could be:

- Processing versus communication—For the suggested method of varying the number of rounds and key size for RC5 encryption, this may have some effect on the computation cost but will have no effect on the data transmission costs. Another issue is that many scenarios require integrity more than encryption protection, and therefore in practice nodes may have to constantly apply integrity protection, but may sometimes not have to use encryption.
- Cost of other functionality on the node—The computation and data transmission costs of performing security are just some of the costs incurred by wireless sensor nodes.

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

- Overheads from security management—Frequent security level changes and trust evaluation operations incur communication overheads, while privacy safeguard mechanisms incur processing overheads. On the other hand, the security parameters may be communicated by piggy-backing on other messages, which will reduce some of the costs.
- Implementation cost—The complexity and cost for the configuration of the Security Manager components can be high for deployments with a large number of highly diverse nodes.
- Required lifetime of nodes and difficulty in replacement—Security Manager functionality may be preferred for nodes that cannot receive regular maintenance or cannot be replaced.
- Dynamicity of scenario—Mobile nodes need the extended Security Manager version in order to adapt within a dynamic environment, with the received benefits depending on the frequency of environment changes.

To investigate the influence of some of these factors and to validate the work, we have performed evaluation for a number of important points.

The benefits of the adaptability property on battery power consumption were quantified through a prototype implementation on sensor hardware (on Crossbow Mica2 motes—www.xbow.com). The aim of the performance evaluation was to quantify the difference in energy consumption between having and not having the ability to adapt the Security Level. A simplified version of the framework was deployed, with the security mechanisms being implemented using TinySec [18] and the Security Levels being represented by the TinySec transmit modes. *Low*, *Medium* and *High* security levels were characterised by no encryption or integrity protection, integrity protection only and both encryption and integrity protection respectively.

Figure 2 shows the variation in power consumption with the rate of changing the level of security in the adaptive security framework. The power consumed without the adaptive framework is also shown for comparison. The curves labelled 100%H, 100%M and 100%L show the power consumption per node with the security level fixed at *High*, *Medium* and *Low* respectively. The points labelled *50%L*, *40%M* and *10%H* represent the experimental values of the power consumption per node with the adaptable security framework switched on and with the respective proportions of time spent in each Security Level. The chart shows that in comparison to constantly using the *Medium* Security Level, benefits can be achieved by adapting the security behaviour, if the Security

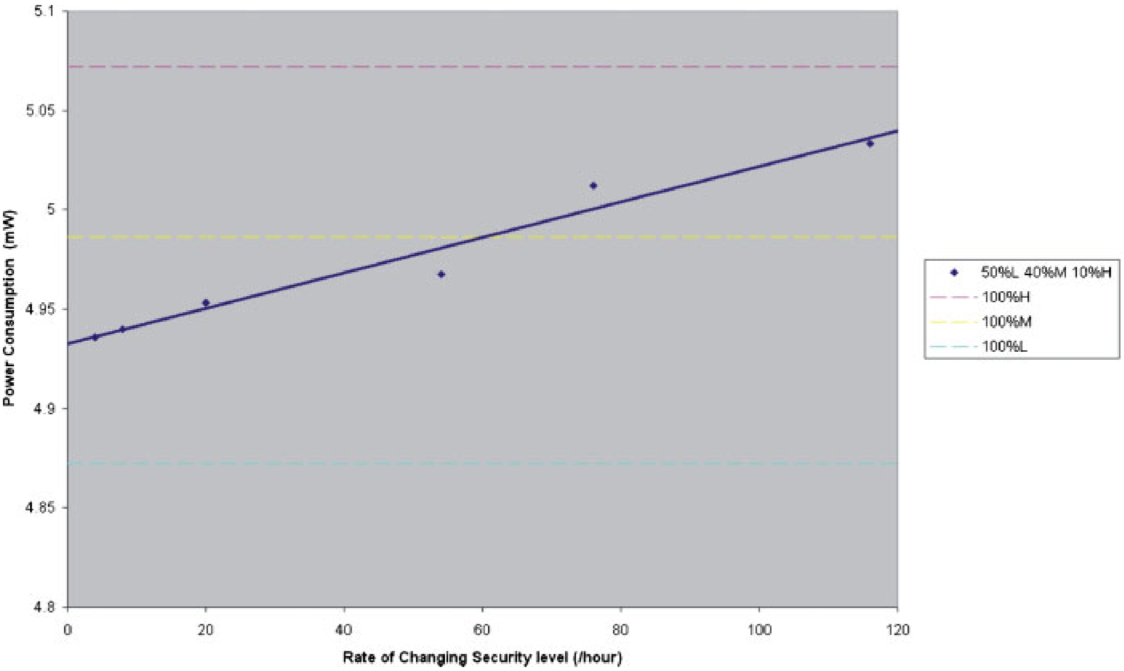


Fig. 2. Node power consumption with and without adaptable security.

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

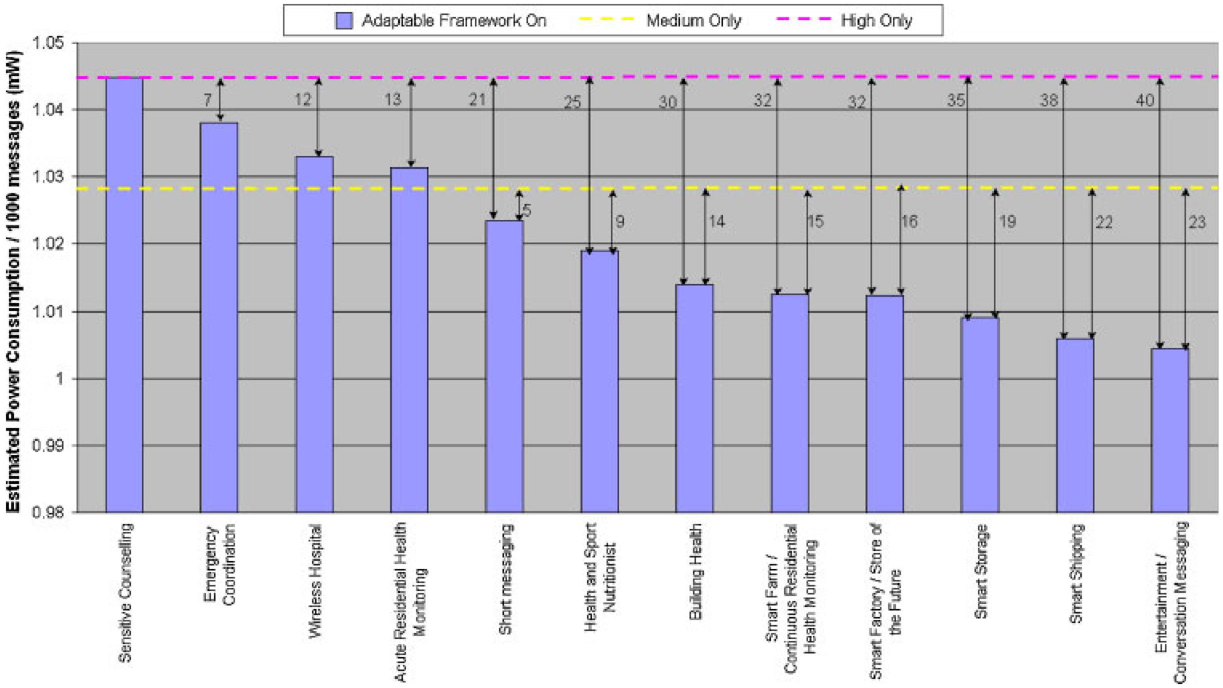


Fig. 3. Estimated power consumption for different scenarios.

Level changes less frequently than every minute. In a real setting, however, it is unlikely that the Security Level will be changed so frequently and so it is likely that the adaptive framework will provide a reduction in battery usage.

This test-bed scenario was also used to validate an analytical power consumption model, which was then used to estimate the benefits of the adaptability framework for other scenarios.

Figure 3 presents the power consumption per 1000 sensor data messages. The values shown do not include the power consumed in Security Level changes. The numbers indicate the number of configuration messages that can be sent per 1000 sensor data messages before the power consumed using the adaptive security framework exceeds that without the framework. The curves labelled *Medium Only* and *High Only* show the power consumption for fixed Security Levels of *Medium* and *High* respectively. For scenarios using only the *Medium* and *High* Security Levels—*Emergency Coordination*, *Wireless Hospital* and *Acute Residential Health Monitoring*, the reduction in power consumption achieved by the adaptable framework is limited. Using an adaptable framework provides the greatest power saving for scenarios that use the *Low* Security Level most of the time, such as the *Entertainment* scenario. The main conclusion drawn from this experimental evaluation is that the power savings from the adaptability property depend on the proportion of the total time spent in each Security Level during network operation, and the frequency of Security Level changes (also concluded in Reference [6]), i.e. to the number of configuration messages that are required.

The evaluation of the trust establishment process was performed through the identification of its resource consuming elements and the derivation of formulas for evaluating power consumption. The analysis showed that the energy, computation and communication requirements of the process depend entirely on the initial parameterisation of trust establishment components and can be optimised according to the node trust requirements and the pre-deployment knowledge of the network topology and the information flows.

For the evaluation of the privacy protection and context-awareness mechanisms, simulations were performed for varying the numbers of context attributes and applicable rules. The aim of the simulation was to estimate the effect of these two mechanisms on the response time, and the influence of the complexity and granularity of the context information on the time from placing a request for data until it is filtered. Figure 4 shows the results of the simulation performed

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

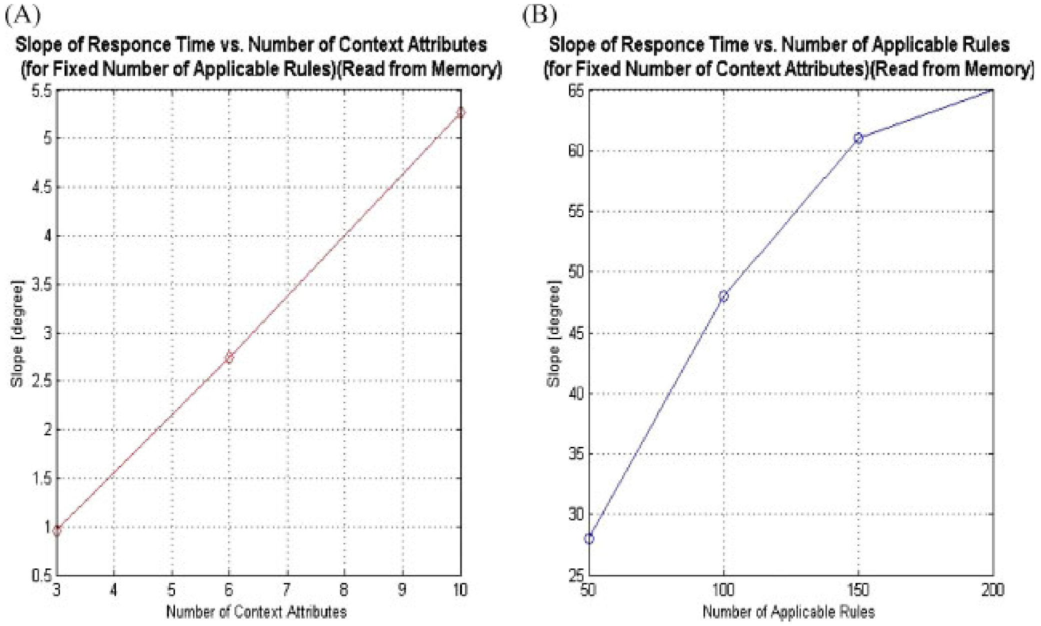


Fig. 4. Slope of response time versus number of context attributes (A) and versus number of applicable rules (B).

on a Pentium 4 laptop—2.4 GHz, 512 MB RAM, using Java in a Windows XP environment. The first diagram illustrates how the response time for different numbers of applicable rules depends on the semantic richness of the context while the second shows its dependence on the number of the applicable rules. The slope gives a view of how fast the increase of the response time is with respect to the increase of the number of context attributes or the number of applicable rules. The simulation showed that the response time and the memory requirements of the privacy protection solution can be optimised through selecting only vital rules and context attributes, and that a proactive approach for selection of valid rule subsets leads to smaller delays.

Overall, it was found that by only providing the security requirements that are strictly necessary according to the application needs, environmental context, etc., significant security processing and communications overhead can be saved. The additional processing that the framework entails will add some delays, but for WSN nodes this is unlikely to be significant as they are infrequent communicators rather than high bandwidth users. This could be more of an issue for gateways, as they are natural points of aggregation. Future work will investigate how much of an issue the power is in practice for gateways and whether any optimisations are possible.

While the work carried out suggests that there is potential in the proposed adaptive security framework, the saving in resources depends on the application. The measurements of the prototype implementation found that the power saving achieved by the adaptable security framework is dependent on the rate of changing the Security Level and the proportion of time spent in each Security Level. The adaptable security framework is mostly beneficial for scenarios that use the *Low* Security Level for a large proportion of the time and that change Security Level infrequently. Measurable savings were also obtained for scenarios that use authentication protection all the time with encryption being switched on and off. The work carried out does provide evidence that there is potential in this idea and that further in-depth validation may be worthwhile for certain scenarios.

Finally, the framework provides increased functionality for users, but at the potential cost of increased complexity for their interactions. The effects of this depend on how users need to interact with the system, and could be minimised with ‘user–centric’ design of interfaces and pre-defined configurations. In addition, the use of policies can be argued to simplify user interactions by allowing them to manage from a central point and concentrate on ‘what’ is needed rather than ‘how’ it is achieved. In other words, they are isolated from the complexities of implementations and can concentrate on what their requirements are.

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

7. Related Work

As per our best knowledge there are only a few published works on security and privacy frameworks for B3G aiming to provide complete solutions [19,20]. However, they do not offer flexibility, adaptability and context-awareness for security, privacy and trust services for WSNs. There are nevertheless works touching on only certain aspects related to security, privacy and trust in WSNs.

The security architecture for medium and large scale WSNs proposed in Reference [21] follows the probabilistic security paradigm for authentication and re-recognition, concealed data aggregation, key predistribution and secure distributed data storage in a toolbox of security-aware components.

Most solutions that have been proposed for privacy in sensor networks focus on the aspect of location privacy. Location brokers have been positioned either at a user terminal or at public devices, protecting the location of the user through data denial, anonymisation or delayed disclosure. Solutions exist at the network routing level to protect from mobile adversaries [22].

The trust establishment frameworks proposed for ad-hoc networks can be classified into two categories according to the scope, purpose and admissible type of evidence—certificate- and behaviour-based frameworks. However, very few of these frameworks are targeted for sensor networks, having acceptable resource requirements and supporting pre-established and stable trust relationships between clusters [11,12].

8. Conclusions

Overall, the proposed framework enables diverse applications and their associated security requirements to be supported in the heterogeneous network topologies that WSNs will need to integrate within real-world scenarios. The framework enables self-reliance and minimises the need for maintenance by providing for self-configuration of nodes according to their individual context and defined policy. In addition, the use of policies means that changes of requirements can be met rapidly without affecting implementations on the nodes (policies define 'what' is needed and not 'how' it is achieved, which is up to the nodes themselves). Performance evaluation results demonstrated the feasibility of the security framework and estimated its benefits for a number of scenarios.

Acknowledgement

The work presented in this paper was partially funded by the FP6 EU project 'e-SENSE, Capturing Ambient Intelligence for Mobile Communications though Wireless Sensor Networks', Contract Number: IST-4-027227-IP, www.ist-e-sense.org.

References

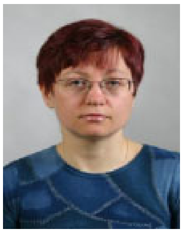
1. Kim YK, Prasad R. 4G Roadmap and Emerging Communication Technologies. Artech House Publishers, 2006; 292, ISBN 978-1-58053-931-9.
2. Knightson K, Morita N, Towle T. NGN architecture: generic principles, functional architecture, and implementation. *IEEE Communications Magazine* 2005; **10**: 49–56.
3. Presser GM, Shelby Z, Scotton P, Schott W, Chevillat P. e-SENSE reference model for sensor networks in B3G mobile communication systems, 15th IST Mobile and Wireless Communications Summit 2006, Myconos, Greece, June 2006, pp. 4–8.
4. Aivaloglou E, Mitseva A, Skianis C, Gritzalis S, Waller A, Prasad N. Scalable security management for wireless sensor networks for medical scenarios. In *Proceedings of the 10th International Symposium on Wireless Personal Multimedia Communications (WPMC 2007)*, Jaipur, India, December 2007; 1014–1018.
5. Verdone R, Corvino V, Orriss J. A hierarchical hybrid network model. In *Proceedings of IEE 3G&Beyond*, London, November 2005, pp. 7–9.
6. Rodrigues RS, David M, Loire D, Mitseva A, Prasad NR. Adaptive security management for body sensor networks in medical Scenario. In *Proceedings of the 9th International Symposium on Wireless Personal Multimedia Communications*, 2006, pp. 1037–1041.
7. Arazi B, Elhanany I, Arazi O, Qi H. Revisiting public-key cryptography for wireless sensor networks. *IEEE Computer* 2005; **38**: 103–105.
8. Wang Y, Ramamurthy B, Zou X. The performance of elliptic curve based group Diffie-Hellman protocols for secure group communication over ad hoc networks. In *Proceedings of the IEEE International Conference on Communications (ICC '06)*, 2006, pp. 2243–2248.
9. Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. SPINS: security protocols for sensor networks. *Wireless Networks* 2002; **8**: 521–534.
10. Aivaloglou E, Gritzalis S, Skianis C. Towards a flexible trust establishment framework for sensor networks. *Telecommunication Systems Modeling, Analysis, Design and Management* 2007; **35**(3–4): 207–213.
11. Aivaloglou E, Gritzalis S, Skianis C. Trust establishment in sensor networks: behavior-based, certificate-based, and a combinational approach. *International Journal of System of Systems Engineering (IJSSE)* 2008; **1**(1–2): 128–148.
12. Huang L, Li L, Tan Q. Behavior-based trust in wireless sensor networks. In *Proceedings of APWeb Workshops*, 2006, pp. 214–223.
13. Mitseva A, Imine M, Prasad NR. Context-aware privacy protection with profile management. In *Proceedings of the 4th International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots WMASH '06*, September 29, 2006, Los Angeles, USA in Conjunction with ACM MobiCOM 2006, pp. 53–62 (ACM Press).
14. Anonymity Bibliography http://www.freehaven.net/anonbib/topic.html

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

15. Wang Y, Ramamurthy B, Zou X. The performance of elliptic curve based group Diffie-Hellman protocols for secure group communication over ad hoc networks. In *Proceedings of the IEEE International Conference on Communications (ICC '06)*, 2006, pp. 2243–2248.
16. Guimaraes G, Souto E, Sadok D, Kelner J. Evaluation of security mechanisms in wireless sensor networks. In *Proceedings of Systems Communications '05*, 2005, pp. 428–433.
17. Wander A, Gura N, Eberle H, Gupta V, Shantz SC. Energy analysis of public-key cryptography for wireless sensor networks. In *Proceeding of the 3rd IEEE International Conference on Pervasive Computing and Communications*, 2005, pp. 324–328.
18. Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems*, ACM Press, 2004, pp. 162–175.
19. Fitzgerald W, Doolin K, Mahon F, *et al*. Daidalos Security Framework for Mobile Services. *Conference eChallenges e-2005*, Ljubljana, Slovenia, October 2005, pp. 19–21.
20. Prasad NR, Rugieri M. Adaptive security for low data rate networks. Special Issue on Security. *International journal on Wireless Personal Communications*. Kluwer Academic Publishers, 2004; **29**(3–4):323–350. ISSN 0929-6212.
21. Westhoff D, Girao J, Sarma A. Security solutions for wireless sensor networks. *NEC Technical Journal*, Vol.1, No.3/2006, www.ist-ubisecsens.org/publications/SecuritySolutionsWSN.pdf
22. Ozturk C, Zhang Y, Trappe W. Source-location privacy in energy-constrained sensor network routing. In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2004, pp. 88–93.

Authors' Biographies



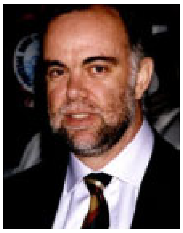
Anelia Mitseva received master's degree in Intelligent Multimedia from Aalborg University (Denmark) in 2001. She worked as Assistant Research Professor in Wireless Security and Sensor Networks Group, CTIF, Aalborg University. She has been heavily involved in a number of projects funded by the European Commission, performing management and research tasks. She is currently employed as a Project Manager with North Denmark EU-office. Her recent research interests are in the field of TeleHealthCare: wireless sensor networks, security, privacy and usability and user friendliness.

Efthimia Aivaloglou holds a Diploma in Information and Communication Systems Engineering from the University of the Aegean, Greece, and an M.Sc. in Advanced Computer Science from the University of Manchester, U.K. She is currently a Ph.D. candidate with the University of the Aegean working on the field of security, privacy and trust in wireless sensor networks.

Maria Marchitti obtained her master degree at the University of Cassino (Italy) in Telecommunication Engineering. She holds a master in Advanced Communication and Navigation Satellite Systems from the University of Rome Tor Vergata. Currently her main research field is mobility management in heterogeneous networks and security and privacy issues in wireless sensor networks.

Neeli Rashmi Prasad (Member IEEE) is Associate Professor and Head of Wireless Security and Sensor Networks Group, Center for TeleInFrastruktur, Aalborg University, Denmark. She has co-authored and co-edited two books on IEEE 802.11. Her research work is published in journals, international conferences and books.

Charalabos Skianis (Senior Member IEEE) is Assistant Professor at the University of the Aegean, Greece. His research work is published in journals, conferences and books. He is a member of editorial boards (e.g. IEEE Wireless Communications), guest editor, organiser of events and member of ComSoc TCs (e.g. Secretary for CSIM).



Stefanos Gritzalis is the Head of the Department of Information and Communication Systems Engineering, University of the Aegean, Greece and the Director of the Laboratory of Information and Communication Systems Security. His published scientific work includes more than 170 journal and international conference papers on Information and Communication Security Technologies topics.

Adrian Waller received a Ph.D. in Pure Mathematics (Royal Holloway, University of London) 1996. Adrian joined Thales Research & Technology (U.K.) in 1997. He is a Technical Consultant responsible for providing cryptography and information security expertise, and his current research interests include security for Wireless Sensor Networks as well as security and accreditation issues for adaptable and dynamic systems-of-systems. Adrian qualified as a CISSP in 2003 and is an Associate of the Institute of Information Security Professionals.

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm

Tim Baugé graduated from the Ecole Nationale Supérieure de Physique de Marseille (now Centrale Marseille) in 1997. He joined Thales Research & Technology (U.K.) in 1998, and is now an Assistant Chief Engineer with the Networks and Security group. His current research focuses on wireless sensor networks, with specific interest in their security, management, and integration into the Future Internet. He is a member of FEANI, CNISF and the IET.

Sarah Pennington graduated from Emmanuel College, University of Cambridge in 2007. She joined Thales Research & Technology (U.K.) as a Design Engineer in 2007. Her current research focuses on wireless sensor networks with an emphasis on security. Sarah is a member of the IET.

Copyright © 2008 John Wiley & Sons, Ltd.

DOI: 10.1002/wcm