SECURITY AND COMMUNICATION NETWORKS
*Security Comm. Networks* 2015; **8:**2016–2036
Published online 23 December 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1151

RESEARCH ARTICLE

# Embedded Systems Security: A Survey of EU Research Efforts

Charalampos Manifavas[1], Konstantinos Fysarakis[2], Alexandros Papanikolaou[2]* and Ioannis Papaefstathiou[2]

[1] Department of Informatics Engineering, Technological Educational Institute of Crete, Heraklion, Greece
[2] Department of Electronic & Computer Engineering, Technical University of Crete, Chania, Greece

## ABSTRACT

Embedded systems security is a recurring theme in current research efforts, brought in the limelight by the wide adoption of ubiquitous devices. Significant funding has been allocated to various European projects on this subject area, in order to investigate and overcome the various security challenges. This paper provides an overview of recent EU research efforts pertaining to embedded systems security, where several prominent security issues and the respective proposed approaches are presented. Surveying relatively recent EU research projects, the authors identify 20 such projects that focus on embedded systems security aspects. The investigated technologies are categorised using a layered approach, to facilitate the presentation of the results; the categories comprise the node, network, and middleware and overlay layers, as well as architectures, frameworks and formal validation of the security of embedded systems. From this survey, certain patterns emerge regarding the issues investigated and the technologies researchers focus on, in order to address the said issues. Finally, the existing open issues are summarised, and directions for future research are given. Copyright © 2014 John Wiley & Sons, Ltd.

**KEYWORDS**
embedded systems; security; resource-constrained devices; sensor networks

***Correspondence**
Alexandros Papanikolaou, Department of Electronic & Computer Engineering, Technical University of Crete, 73132 Chania, Crete, Greece.
E-mail: alxpapanikolaou@gmail.com

Received 14 May 2014; Revised 15 September 2014; Accepted 26 September 2014

## 1. INTRODUCTION

Embedded devices have nowadays an important role in a variety of systems, such as critical infrastructures, enhanced reality, the Internet of Things (IoT) and e-health applications. However, their resource-constrained nature and their deployment in dynamic, heterogeneous networks, which are commonly exposed to various attacks, even physical in nature, only exacerbate their security, privacy and dependability issues [1].

The wide adoption of embedded systems for various application scenarios makes it imperative to face the aforementioned security issues, regardless of the layer these may be found in; thus, the focus of current research on these issues is evident and justified. This survey paper has been conducted within the scope of such a project, nSHIELD [2], an EU-funded research project focusing on embedded systems security. The work presented here aims at providing an overview of the said past and running projects in order to identify emerging trends, state-of-the-art technologies being used or developed, opportunities for composing or expanding past work and, generally, highlight open issues that need to be addressed in the future. The resource-constrained nature of such devices makes tackling the various security-related issues a rather challenging task, as in many cases, it is not possible to apply conventional, well-established methods and techniques. In addition, this survey partly demonstrates the broader areas of embedded systems security that researchers chose to focus on, given the latest technological advancements (nationally funded projects have not been taken into account).

Out of a large number of projects initially gathered, a smaller subset of the most recent ones was selected to be included in this work, based on their relevance to security and dependability aspects of embedded systems design, as well as their availability of public deliverables and publications lists. Research in these projects has been

**Table I.** Selected EU-funded projects related to embedded systems security.

| | Acronym | Project Title | Start Date End Date | Cost (EUR) | Call |
|---|---|---|---|---|---|
| 1 | AETHER | Self-adaptive embedded technologies for pervasive computing architectures | 01/01/2006 31/12/2008 | 5.92M | FP6 |
| 2 | AWISSENET | Ad hoc PAN and wireless sensor secure network | 01/01/2008 28/02/2010 | 3.10M | FP7 |
| 3 | CESAR | Cost-efficient methods and processes for safety relevant embedded systems | 01/03/2009 01/03/2012 | 33.5M | ARTEMIS JU |
| 4 | CHAT | Control of heterogeneous automation systems: Technologies for scalability, reconfigurability and security | 01/09/2008 31/08/2011 | 3.58M | FP7 |
| 5 | EVITA | E-safety vehicle intrusion protected applications | 01/07/2008 31/12/2011 | 5.89M | FP7 |
| 6 | GINSENG | Performance control in wireless sensor networks | 01/09/2008 29/02/2012 | 4.66M | FP7 |
| 7 | HYDRA | Networked Embedded System middleware for heterogeneous physical devices in a distributed architecture | 01/07/2006 30/06/2010 | 12.75M | FP6 |
| 8 | MADNESS | Methods for predictAble Design of heterogeNeous Embedded System with adaptivity and reliability Support | 01/01/2010 31/12/2012 | 2.92M | FP7 |
| 9 | MORE | Network-centric Middleware for group communications and resource sharing across heterogeneous embedded systems | 01/06/2006 31/05/2009 | 2.75M | FP6 |
| 10 | OVERSEE | Open VEhiculaR SEcurE platform | 01/01/2010 30/06/2012 | 3.91M | FP7 |
| 11 | PRESERVE | Preparing Secure Vehicle-to-X Communication Systems | 01/01/2011 31/12/2014 | 5.44M | FP7 |
| 12 | pSHIELD | Pilot Embedded Systems Architecture for Multi-layer Dependable Solutions | 01/06/2010 31/12/2011 | 5.40M | ARTEMIS JU |
| 13 | SecFutur | Design of Secure and energy-efficient embedded systems for Future internet applications | 01/05/2010 30/04/2013 | 4.20M | FP7 |
| 14 | SEPIA | Secure, Embedded Platform with advanced Process Isolation and Anonymity Capabilities | 01/06/2010 31/05/2013 | 3.26M | FP7 |
| 15 | SMEPP | Secure Middleware for embedded peer to Peer Systems | 15/09/2006 14/09/2009 | 4.46M | FP6 |
| 16 | TECOM | Trusted Embedded Computing | 01/01/2008 31/03/2011 | 9.02M | FP7 |
| 17 | TERESA | Trusted computing Engineering for Resource constrained Embedded Systems Applications | 01/11/2009 31/10/2012 | 3.79M | FP7 |
| 18 | UbiSec&Sens | Ubiquitous sensing and security in the European homeland | 01/01/2006 31/12/2008 | 2.91M | FP6 |
| 19 | UNIQUE | Foundations for Forgery-Resistant Security Hardware | 01/09/2009 29/02/2012 | 4.22M | FP7 |
| 20 | WSAN4CIP | Wireless sensor networks for the protection of critical infrastructures | 01/01/2009 31/12/2011 | 4.02M | FP7 |

conducted using EU resources; hence, they have a budget within the funding limits imposed by the EU itself and have undergone a similar review process in terms of novelty, application and quality requirements. In addition, they all try to achieve the common goal of attaining a uniform technological level among all EU state-members. Details on the EU-funded projects related to embedded systems security that were selected for the purposes of this paper are presented in Table I.

The ubiquitous nature of embedded systems is evident in Table II, which features the various application areas pertaining to each project. It should be noted that the application table was produced based on how the researchers themselves identify the application areas of the technologies they present, as this emerges from the project deliverables and publications. It goes without saying that many of the identified technologies could belong to other application areas as well, either with or without additional modifications.

In terms of the layers that were used to classify identified literature work, the lowest one is the node, which involves the hardware and firmware technologies. The network layer includes various protocols, authentication schemes and other security-related mechanisms. Middleware layer mainly refers to low-level software that operates on top of the device's operating system but, in most cases,

**Table II.** Application areas overview.

| Acronym | Aerospace | Automotive | Railway | Smart home and smart buildings | Smart metering | e-Health | Industry 4.0 and agriculture | Mobile devices | Critical infrastructure and environmental monitoring |
|---|---|---|---|---|---|---|---|---|---|
| AETHER | | X | | X | | X | X | | X |
| AWISSENET | | X | | | | | | | X |
| CESAR | X | X | X | | | | X | | |
| CHAT | X | | | | | | | | |
| EVITA | | X | | | | | | | |
| GINSENG | | | | | | | X | | |
| HYDRA | | | | X | X | X | X | | |
| MADNESS | | | | | | | X | | |
| MORE | | | | | | X | | | X |
| OVERSEE | | X | X | | | | | | |
| PRESERVE | | X | | | | | | X | |
| pSHIELD | | | X | | | | | | |
| SecFutur | | | | X | X | | | | X |
| SEPIA | | | | | | | | X | |
| SMEPP | | | | X | | | | X | X |
| TECOM | | X | | | | X | X | X | |
| TERESA | | X | X | X | X | | X | | |
| UbiSec&Sens | | X | | | | | X | | X |
| UNIQUE | | | | | X | | | | X |
| WSAN4CIP | | | | | | | X | | X |

below any other applications (namely, overlay). Finally, the architectures and formalisation classification comprises various frameworks and other holistic approaches to the security of embedded systems, including solutions that consider their formal validation.

The paper is organised as follows: Sections 2–4 give an overview of the research efforts in some recent EU-funded projects related to embedded systems security, following a layered approach. In particular, Section 2 presents the various technologies related to embedded systems' nodes. Section 3 deals with the network-related technologies. Section 4 presents the approaches followed for the middleware and overlay layers. Section 5 focuses on architectures and frameworks, as well as on the formal validation of the security of embedded systems. Issues that future research could deal with are presented in Section 6, and finally, the paper concludes in Section 7.

## 2. NODE TECHNOLOGIES

The heterogeneous nature of the field is evident from the literature review. In terms of hardware used, it was confirmed that there is a variety of platforms being utilised, with equally varied capabilities, such as the low-power TelosB, IRIS and MICAz platforms from Crossbow Technology [3], the more capable Verdex Pro XL6P COM from Gumstix [4] and the FOX LX board from Acme Systems [5]. In some cases, even more powerful devices are being used, such as the Freescale i.MX51 [6] and the Xilinx Spartan-6 [7] Field Programmable Gate Array family. The latter, along with low-power x86-based platforms, are also typically used in the development of future vehicular applications. Equally varied are the software security solutions being utilised and developed, featuring different operating environments, protocols and cryptographic primitives.

Given the often unattended nature of deployed embedded systems, sometimes within hostile environments, the aspect of physical security cannot be ignored. Gaining physical access to a device enables the launch of various side-channel attacks, such as simple/differential power analysis and differential fault attacks, which could potentially expose security-related information (cryptographic algorithms used, length of keys, etc.), thus jeopardising the security of both the device itself and the network it belongs to as a whole. What is more, the inherent limitations of embedded systems devices, in terms of processing power, memory, storage and energy, require suitable cryptographic techniques that take those constraints into consideration. Such lightweight cryptographic mechanisms can facilitate secure communication without becoming a burden, resource-wise, on the device itself. Alternatively, virtualisation techniques can be used to fortify ESs security, and specialised hardware modules can be employed to speed up various cryptographic functions.

This section is dedicated to presenting technologies aiming at protecting the embedded system's physical secu-

**Table III.** Node technologies overview (projects that did not focus on these aspects have been left unchecked).

| Acronym | Purpose-built hardware and features | Virtualisation | Lightweight crypto | Side-channel security issues | Trusted Platform Modules |
|---|---|---|---|---|---|
| AETHER | X | X | | | |
| AWISSENET | X | | X | | |
| CESAR | | | | | |
| CHAT | | | | | |
| EVITA | | | | | |
| GINSENG | | | | | |
| HYDRA | | | | | |
| MADNESS | | | | | |
| MORE | | | | | |
| OVERSEE | | | | | |
| PRESERVE | | | | | |
| pSHIELD | | | | | |
| SecFutur | | | | | X |
| SEPIA | X | X | | X | X |
| SMEPP | | | X | | |
| TECOM | | X | | | X |
| TERESA | | | | | |
| UbiSec&Sens | | | X | X | |
| UNIQUE | X | | | | |
| WSAN4CIP | | | | X | |

rity, a variety of lightweight cryptography schemes and other techniques for enhancing a node's physical security that take into consideration the various resource constraints. An overview of the node-related technologies identified can be found in Table III.

## 2.1. Hardware-related security modules

### 2.1.1. Tamper-resistant modules.

A significant area of security research related to Wireless Sensor Networks (WSN) aims at utilising Trusted Platform Module (TPM) hardware and adapting it to the specific needs of resource-constrained applications. Such a TPM-related subject is that of the implementation of the Direct Anonymous Attestation (DAA) scheme specified by the Trusted Computing Group. In [8], a detailed report on the implementation of the aforementioned functionality is provided, as well as suggestions for improvements. The presented experimental results indicate that especially the rogue detection part of the DAA protocol can be very time consuming and the overhead is very evident on resource-constrained devices, increasing linearly with the size of the black lists of rogue TPMs. Moreover, problems with the mechanisms and protocols used to report compromised TPMs are identified. On the subject of TPMs, research has also focused on the security extensions of mobile platforms for hosting Mobile Trusted Module (MTM) functionality. Two different reconfigurable MTM architectures are presented in [9]; the first one is based on a software implementation of the MTM running on the same physical processor as the applications using that MTM, and the second is based on JavaCards providing the MTM functionality via the Java runtime environment, each with its own set of isolation mechanisms between the MTM and its users. The techniques utilise security features commonly found on mobile devices, that is, Secure Elements and ARM TrustZone [10], proposing respective techniques for dynamic loading of TPM commands, aiming to alleviate the performance and memory issues arising from the security facilities of mobile platforms. In [11], the server side of Trusted Computing functionality is examined, presenting a design based on the Nizza Architecture [12] but minimising the trusted computing base and aiming to provide anonymous and trustworthy service for users, even counteracting certain insider attacks which, with the proposed scheme cannot go undetected.

An approach for protecting agents by utilising tamper-resistant cryptographic hardware is presented in [13]. The proposed agent migration protocol (Secure Migration Library) is based on the use of Trusted Computing technology that attempts to protect the agent from malicious hosts. A weakness of this system is the key management system that requires further improvement. In particular, because the available key storage in the TPM is very limited, the key to be used is loaded into memory when required and is offloaded as soon as it is no longer useful, thus triggering many key transactions. Issues such as the use of key caching and the best possible management of cached keys remain topics that future research could deal with.

It should be evident from the previous discussion that TPMs are an important tool for building secure embedded system platforms; still, it must be noted that they should not be considered fail-proof. In [14], an active hardware

attack on TPMs is detailed, which may not allow access to protected data (e.g. cryptographic keys), but circumvents the chain of trust assumed to be provided by the trusted platform. So, the module itself might be tamper resistant, but the communication channels are often vulnerable, and this is something that must be taken into consideration at the design phase.

Regarding defence against more invasive attacks, a clock frequency watch dog, implemented using a digital standard CMOS library, is presented in [15]. The proposed scheme is able to prevent clock speed manipulations, thus preventing side-channel attacks on cryptographic hardware devices. The cost in terms of both additional area and energy requirements is low and is therefore suitable for being applied to low-cost devices, such as wireless sensor nodes.

#### 2.1.2. Hardware acceleration.

Another approach to WSN node security is based on the use of low-cost, low-energy consumption Complex Programmable Logic Devices (CPLDs), which are programmable logic devices having a complexity between that of Programmable Logic Arrays and that of Field Programmable Gate Arrays, sharing architectural features with both. A WSN platform, which embeds a CPLD in a standard WSN node, is presented in [16]. As real-world experiments show, this CPLD-equipped platform can increase the performance of a standard WSN node by a factor of 1220 to 3000 when executing certain algorithms and also reduce power consumption, with a reported reduction of up to 98%. This concept is further expanded in [17], where various networking and security protocols are implemented on the aforementioned platform and real-world performance is compared to existing schemes. In [18], RESENSE is presented, a complete node platform integrating this technique on popular WSN nodes (MICAz and IRIS from Crossbow Technology) running the TinyOS operating system.

#### 2.1.3. Physically unclonable functions.

The use of Physically Unclonable Functions (PUFs) is a method for protecting devices against attacks on their keys [19]. These functions extract secrets from physical characteristics of integrated circuits (ICs), which can be used, among others, for storing keys securely. The keys are therefore "hidden" into the various hardware parts, instead of being stored into the device's memory. In this way, even by using very advanced tools for attacking hardware, any such attempts for side-channel attacks will be unsuccessful in retrieving any useful information. For an additional layer of security, Logically Reconfigurable PUFs that have the ability of changing their challenge/response behaviour in a random manner can be used [20]. Hence, a potential attacker will also have to deal with a continually-changing behaviour. PUFs can be used in any embedded system comprising ICs, even in the very resource-constrained RFID tags, especially when the latter are used for high-security applications, such as passports.

Combining PUFs and Public PUFs (PPUFs) with Fuzzy Extractors, it is possible to substitute dedicated hardware security modules, as demonstrated in [21,22], where these technologies are investigated in the context of pseudonymous communication in vehicular networks. There are various open issues in the said field, as these anonymisation techniques are not really effective when every vehicle knows the PPUF characteristics and alternatives should be investigated (e.g. using lists of the PPUF characteristics themselves as pseudonyms). Moreover, using PPUFs in challenge–response and authentication mechanisms in general could be further investigated.

#### 2.1.4. Channel characteristics exploitation.

A similar concept of exploiting physical characteristics in order to derive cryptographic keys is the method presented in [23]. No dedicated hardware is being used in this case; instead, an adaptive quantisation algorithm is proposed, able to generate sufficiently long keys by exploiting the radio channel randomness between two communicating parties. In multipath radio environments, due to the scatters effects, the waveforms travel differently from one location to another. Hence, a potential eavesdropper is incapable of obtaining similar channel measurements and therefore cannot extract the secret key from the communicated data.

### 2.2. Virtualisation

Virtualisation is a feature that, as research has shown, adds to the overall security of the system, in various ways. Firstly, it seems to be a remedy for facing the severe security challenges that mobile devices have, given that they are usually targeting a completely open setup [24]. In addition, efficient virtual machines have successfully been implemented in micro-kernel-based systems, thus enabling the reuse of arbitrary operating systems [25]. The overhead imposed on the kernel growth was rather marginal, and the overall performance was found to be similar to other virtual machine implementations. An analysis on how and to which degree recent x86 virtualisation extensions can influence the response times of a real-time operating system that hosts virtual machines was performed in [26]. In [27], it was shown that a thin and rather simple virtualisation layer can add to the overall system's security, as it provides fewer options for attack to a potential adversary. What is more, this approach was found to exhibit significantly better performance, compared to contemporary full virtualisation environments. Finally, regarding the way virtual machines should be implemented, it is claimed in [28] that their construction should follow the principle of incremental complexity growth. Namely, additional functionality should not be included in the trusted computing base of a component if the benefits it offers are less than the drawbacks (e.g. due to larger risk for introduced bugs and errors). Such an approach can be efficiently implemented,


DOI: 10.1002/sec

and it was possible to achieve high throughput and good real-time performance. The utilisation of Trusted Platform Modules and virtualisation techniques is an emerging pattern in relevant EU projects. A combination of the said technologies is presented in [29], intending to provide a reference design for a Trusted Computing-based, lightweight, virtualisation framework specifically aimed at cloud computing scenarios, an increasingly important area of applications. The proposed architecture exploits both the ARM TrustZone and the TPM DAA technologies. Lightweight containers are supervised by a relevant supervisor application. In the proposed scheme, lightweight containers ($\mu$compartments) are built on top of the Linux kernel, with each isolation container enclosing the code and data required for the compartment to operate. Each compartment is monitored and managed by a per-compartment supervisor application, responsible for constructing the security policies, enforcing them and finally destructing its compartment.

## 2.3. Lightweight cryptography

An overview of the literature pertaining to time and energy overhead various cryptographic primitives impose on popular types of wireless sensor nodes is presented in [30]. A number of symmetric and public-key algorithms, hash functions and cryptographic primitives in general are mentioned as well as their lightweight counterparts, where available. It is worth pointing out that the node lifetime data presented in the literature usually refer to the overhead imposed by the security-related functionality alone and, in a real-life scenario, values would be significantly lower because of additional functions running on the same node.

In the literature, whenever strong encryption is required on rather resource-constrained devices, elliptic-curve cryptography (ECC) is always a strong candidate. In [31], the finite fields $F_p$, $F_{2^d}$ and $F_{p^d}$ are being investigated for suitability for performing ECC on the ATmega128 microcontroller, and it turns out that binary fields are most preferable when efficient implementations are required.

An interesting security scheme for WSN that provides transparent security is proposed in [32]. This scheme is effectively a lightweight CBC-X mode cipher that is able to provide encryption/decryption and authentication, combined as a one-pass operation. Consequently, it exhibits significant energy gains of about 50–60%, compared to TinySec [33]. Furthermore, the proposed scheme has no ciphertext expansion for the transmitted data payload, thus significantly reducing the communication overhead. Although a block cipher is used, ciphertext expansion is avoided by having padding rules making use of a Data Stealing technique and a MAC Stealing technique, thus allowing for zero redundant padding bytes.

A strong, compact and efficient block cipher, Data Encryption Standard Lightweight extension (DESL), based on the DES cipher design is proposed in [34]. Instead of using eight S-boxes as in DES, it uses a single S-box repeated eight times, thus considerably reducing chip size requirements. Furthermore, a lightweight implementation of DESL is also proposed, which requires almost half the chip size and 86% less clock cycles compared to the best AES implementations targeted for RFID applications, therefore rendering DESL a strong candidate for ultra low-cost encryption applications.

An optimised implementation of a modular multiplication is presented in [35]. The proposed algorithm was tested on an 8-bit microcontroller (AVR), using a 160-bit standard compliant elliptic curve (namely, secp160r1). Given that the majority of the processing time for ECC is spent on modular multiplication, related schemes such as EC ElGamal or ECDSA would greatly benefit from it, as well as their applications in the field of resource-constrained devices (such as WSNs).

Hardware-specific optimisations have also played an important role in lightweight cryptography research efforts. The authors in [36] present an area-efficient implementation of AES (requires 0.33 $mm^2$ in a 0.25 $\mu$m technology), featuring good performance and low-power consumption. These goals were achieved by optimising both the individual functional blocks of AES and the overall architecture.

## 2.4. Miscellaneous node topics

The authors in [37] propose a scheme for implementing security on extremely low-cost sensors that run with minimal resources regarding computational power, energy consumption and memory size. The sensors are initially loaded with firmware suitable for providing asymmetric cryptography during the one-time bootstrapping phase. Then, through a dynamic code update, it is replaced by other security protocols that are required for the operation of the WSN, effectively offering hybrid security functionality. Their proof-of-concept implementation makes use of the FlexCup plug-in for TinyOS.

The practicality of group signature schemes on mobile devices is examined in [38], where the authors constructed a Java framework that allows for an in-depth evaluation of three such schemes (out of a total of seven defined in the upcoming ISO20008-2 standard). Performance evaluation took place on a laptop bearing an Intel i7 CPU, as well as on three recent Android-based smartphones, so as to gather up-to-date results. The conducted tests were aiming at determining the required signing time, as this is considered very important in the investigated scenarios. Initial results ranged from 304.2 to 4752.7 ms, among the three smartphones, for various algorithms and key lengths. However, when pre-computation was employed, the times dropped significantly and fell within the range of 0.71–631.11 ms, respectively. Verification times were significantly longer for the mobile devices (245.6–9735.5 ms), nevertheless still within acceptable limits for real-world implementations.

# 3. NETWORK TECHNOLOGIES

The resource-constrained and often heterogeneous and distributed nature of embedded systems imposes restrictions and introduces issues at the network layer as well. It is quite common that certain applications of embedded systems require the integrity of the provided service. If web services are being used, it is important to be able to ensure the validity of each participating node, thus ensuring that the system has not been compromised and their communicated data (e.g. measurements) is trustworthy. This is the objective that the various attestation techniques try to achieve. One other issue that needs to be taken care of is the secure transmission of the obtained data to their destination. Examples for meeting this requirement are the implementation of secure routing or secure data aggregation techniques. Detection of potentially malicious nodes in a network is another important issue that may be achieved with the deployment of a suitable intrusion detection system (IDS). Such systems usually look for abnormalities in the overall system behaviour and raise alerts accordingly. Once again, all these additional security mechanisms should not burden the overall system's performance to an extent where the system is effectively rendered useless; therefore, suitable lightweight techniques must be employed.

This section is dedicated to presenting technologies related to node attestation and authentication techniques, secure routing and secure data aggregation, and various intrusion detection schemes. Table IV features an overview of the network technologies identified and their related projects.

## 3.1. Node attestation and authentication

The interoperability with existing infrastructures and the Internet is a major challenge, which must be tackled in a definitive way if we are to realise what is often referred to as the IoT. A very valuable tool in this area is the combination of the IEEE 802.15.4 standard with 6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks, [39]), which, expectedly, introduces new security challenges and opportunities. An example of the security challenges introduced by using these new technologies can be found in [40], where an off-the-shelf T-Mote Sky wireless sensor is transformed into an 802.15.4 packet sniffer. Analysis is then trivial using open source software like Wireshark. Of course, this technique is a valuable tool in the hands of researchers developing protocols but can also be exploited by malicious users to eavesdrop on a network or even launch active attacks (e.g. packet injection). The authors in [41] propose new compression mechanisms for 6LoWPAN security headers, along with cryptographic mechanisms typically used with the IP security architecture, allowing the establishment of end-to-end secure channels between internet hosts and sensor nodes. The proposed mechanisms also allow for fine-grained control over the energy consumed on security-related tasks on the nodes, while the proposed model was evaluated in [42], with AES-CCM and SHA1 as the cryptographic primitives of choice.

The security and constraints stemming from the limited resources of sensor nodes have been investigated in EU projects extensively. Such an EU-funded attempt at trying to tackle these issues is presented in [43], giving an

**Table IV.** Network technologies overview (projects that did not focus on these aspects have been left unchecked).

| Acronym | 6LoWPAN and 802.15.4 | Privacy and anonymity | NFC and RFID | Secure routing and secure services protocols | Intrusion and malicious node detection | Secure aggregation |
|---|---|---|---|---|---|---|
| AETHER | | | | X | | |
| AWISSENET | X | | X | X | X | |
| CESAR | | | | | | |
| CHAT | | | | | X | |
| EVITA | | | | | | |
| GINSENG | X | | | | | |
| HYDRA | | | | | | |
| MADNESS | | | | | | |
| MORE | | | | | | |
| OVERSEE | | | | | | |
| PRESERVE | | X | | X | X | X |
| pSHIELD | | | | | X | |
| SecFutur | | | | X | X | |
| SEPIA | | X | X | | | |
| SMEPP | | | | | | |
| TECOM | | | | | | |
| TERESA | | | | | | |
| UbiSec&Sens | | | X | | | X |
| UNIQUE | | X | X | | | |
| WSAN4CIP | | | | | | X |


DOI: 10.1002/sec

overview of the topic, including security and operational requirements, sensor and network constraints as well as the objectives of this specific project. Another overview, more focused on smart-home applications, can be found in [44], where, among others, key privacy and security issues are identified.

### 3.2. Privacy and anonymity

Anonymous Authentication and Anonymity schemes in general are another key area of current research, because privacy is essential in many applications (e.g. social, medical) and anonymising access to resources and services is a common technique to safeguard users' privacy. An analysis of how trusted computing technologies can be used for anonymous authentication, and how they can be integrated into common security frameworks (e.g. Java Crypto Architecture) can be found in [45]. This work is based on the DAA scheme for providing anonymity over secure communications channels (i.e. anonymous TLS client authentication), but using alternative, more lightweight, schemes than those defined in the TPM v1.2 specification. Another interesting aspect of this work is the discrepancies reported between various TPM manufacturers (e.g. Infineon, Atmel, Winbond, Intel, ST Micro), TPM emulators and the original specification.

Another anonymous authentication scheme based on an optimised version of DAA and aimed at resource-constrained mobile devices is presented in [46]. Functionality includes secure devices authentication, credential revocation and anonymity and untraceability of the said devices against service providers. The proof-of-concept implementation was deployed on an ARM11-equipped development platform (exploiting the ARM TrustZone feature, using an elliptic curves and pairings scheme, while integration with the OpenSSL security framework was also demonstrated).

Further work on Trusted Computing Group anonymity schemes (i.e. PrivacyCA and DAA) is attempted in [47]. The goal is to overcome the need for a trusted third party, which is evident in the aforementioned standard schemes, while maintaining compatibility with the TPM v1.2 specification. The proposed anonymisation scheme for trusted platforms overcomes the need for a trusted third party while relying on the TPM's DAA functionality so that no TPM modifications are required.

Regarding anonymous authentication, a DAA protocol utilising Near Field Communication-equipped (NFC, [48]) mobile devices and RFID is proposed in [49], expanding on the now relatively popular Secure Element scheme presented in [50]. Experimental results are also presented, using off-the-shelf mobile devices.

The scheme proposed in [51] offers anonymous authentication for RFID, with the use of additional devices, the *anonymisers*. The latter interact with the RFID tags, and any communication with external devices (e.g. RFID tag readers) is performed through the anonymisers that mask certain information, thus ensuring the tags' anonymity and unlinkability. What is more, the anonymisers operate as some sort of proxies to the RFID tags, by undertaking the task of performing the required public-key cryptographic operations that the tags are unable to do so, due to their very resource-constrained nature.

As smartphones are already ubiquitous, some researchers focus on taking advantage of the features of modern smartphones in smart vehicle applications, as this alleviates some of the requirements from the vehicle platform itself (in terms of processing power, presence of Global Positioning System (GPS) functionality etc.). In [52], the privacy issues of such an application, namely, the use of smartphones for data acquisition of Intelligent Transportation Systems (ITS). The authors propose the extension of an existing architecture with anonymous authentication, allowing for privacy-aware traffic and location sample collection and protecting users' privacy even in cases of compromised ITS servers.

Wireless communication in Vehicular Ad hoc Networks (VANETs) is typically protected by digital certificates. As such certificates and related identifiers must not be usable to track vehicles, short-term pseudonymous certificates are applied and regularly changed in order to protect the driver's privacy. The authors in [53,54] introduce and implement a distributed PKI architecture for vehicular networks, utilising pseudonymous certificates for privacy-preserving vehicular applications complying with related standards. Using tickets as cryptographic tokens, the proposed scheme offers authentication, authorisation and accountability, while maintaining the vehicle's privacy (e.g. guaranteeing that consecutive pseudonym requests cannot be correlated).

Nevertheless, there are certain incidents (e.g. traffic accidents) where it should be possible to identify the actual user via the certificate issuer. Hence, resolution of pseudonym identifiers is needed. The authors in [55] propose a generic pseudonym resolution protocol to be used by network infrastructure entities under such critical predefined conditions. The proposed protocol, CoPRA, does not increase pseudonym certificate size and imposes no additional overhead nor delay in the certificate acquisition phase. Moreover, it allows for validation of the situation that warrants the pseudonym resolution, prior to providing any information regarding the users' identity.

Privacy concerns pertaining to future smart vehicles are not restricted to VANET-related issues. The expected wide deployment of electric vehicles and charging infrastructures will require the use of protocols to control authentication, authorization and billing of vehicle owners. The ISO/IEC 15118 [56] standard defines the vehicle to charging station communication interface, also including the necessary security mechanisms. Still, it does not cater for the privacy protection of service users, making it trivial to, for example, let charging station operators track the location of a specific user. Therefore, authors in [57] propose POPCORN, a modular extension to the protocol defined in the aforementioned standard, which includes various privacy enhancing technologies like anonymous credentials.

A proof-of-concept implementation is also presented to demonstrate the feasibility and investigate the performance of the proposed scheme.

### 3.3. Secure routing

Secure routing protocols constitute another critical research area of networking technologies. In [58], an overview of security issues and current trends in trusted routing for ad hoc networks is provided, evaluating their applicability in WSNs. Various trust-management enhanced routing protocols and trusted routing frameworks are investigated, focusing on their applicability on resource-constrained environments. A secure routing protocol better suited to such environments is proposed in [59], namely, Ambient Trust Sensor Routing (ATSR) and its performance and effectiveness are evaluated. In ATSR, the geographical location of nodes along with other parameters (e.g. their remaining energy, for better load balancing and lifetime extension) is considered. Moreover, the protocol features a distributed trust model, based on both direct and indirect trust data, to detect malicious nodes.

The authors in [60,61] also proposed a mobile ad hoc network routing protocol based on the Better Approach To Mobile Ad hoc Networking protocol [62] that utilises concepts from the domain of trusted computing. Device attestation is integrated on the protocol itself, thus routing and data transmissions can be restricted to trustworthy devices only. A Trusted PlatfModule (TPM) serves as root-of-trust on each device, and hence, any devices that have been identified as being malicious can automatically be recognised by all network nodes, thus leading to their exclusion from the trusted network. Additional issues need to be looked into, such as interoperability with other network standards, interaction with other networks (homogeneous or not) and the maintenance of a trustworthy connection over another layer-2 protocol.

The interactions between secure routing protocols and the Service Discovery functionality on WSN networks where the nodes are used as service providers are investigated in [63]. Simulation results presented in the aforementioned work indicate that in some situations, there is an efficiency gain if routing protocols allow the higher layers to override the routing decisions, which might, for example, try to avoid using an untrusted node that the service discovery layer wants to use.

### 3.4. Intrusion and malicious node detection

The IDS are a key tool in safeguarding distributed ES networks. A dynamic and distributed IDS scheme is presented in [64] and further expanded in [65], where nodes act as local monitors of their neighbours and, in combination with data received from other monitors, are able to detect malicious entities. Simulations are used to prove the effectiveness of the proposed methods, with applications focusing mostly on smart vehicles. Defensive techniques for sensor networks based on the nodes' locations are surveyed in [66], assuming every node is capable of detecting its own location. Furthermore, concepts of robust statistics (i.e. robust regression) are proposed, aiming to localise a node in the presence of malicious beacons. To facilitate the analysis and understanding of IDS data, various advanced methods have been investigated in EU-funded products, including neural network-based techniques for the visualisation of the said data, as presented in [67].

Awareness of nearby vehicles and their location is a basic foundation of electronic safety application in VANETs. However, the ad hoc nature of the vehicular networks makes them vulnerable to malicious nodes. Moreover, it is realistic to assume that in some cases, there will be no pre-established trust relationships between vehicles. Researchers in [68] try to address these challenges by proposing a fully distributed cooperative solution, namely, a lightweight protocol, which relies only on information exchange among neighbouring entities, enabling the effective identification of adversarial nodes.

A central evaluation scheme is proposed in [69], where malicious peers are detected and excluded from the VANET using misbehaviour detection systems. These systems use trust and reputation information provided in misbehaviour reports submitted by vehicles as well as roadside units. As simulations indicate, the presented system is significantly effective against ghost/malicious vehicles broadcasting faked position and other information, which is one of the most critical attacks on VANETs. It should be noted that the proposed scheme is not fully distributed and vehicles rely on a central authority, namely, the Misbehaviour Evaluation Authority, to detect attackers.

Even in cases where a PKI scheme is established, insider attackers, that is, malicious entities possessing legitimate key material, must be considered as well. Authors in [70] propose the exploitation of redundant information dissemination for consistency checks and evaluate dissemination protocols using three graph-based metrics they introduce.

### 3.5. Secure aggregation

Information aggregation techniques are a useful tool, especially in mobile ad hoc networks (MANETs), to facilitate information dissemination and to reduce bandwidth requirements. In the context of VANETs, which are considered a sub-category of MANETs, the vehicles must communicate to exchange information for various enhanced services (safety, efficiency, traffic, entertainment etc.). Aggregation techniques can be used so that vehicles exchange high quality summaries of the said information, instead of exchanging each individual message. Still, it is essential to utilise secure aggregation schemes, as the information exchanged between vehicles can be used for important decisions (e.g. traffic management, fleet control or road safety). Authors in [71] present such a


DOI: 10.1002/sec

dynamic and secure aggregation scheme for VANETs, which prevents insider attacks from influencing the aggregation results. Furthermore, its security mechanisms can be applied to existing aggregation schemes to produce dependable aggregates.

When it comes to WSNs, maximising the sensors' battery life is, naturally, of great importance. For this reason, *in-network aggregation* protocols have been proposed, where the required function(s) on the measurements is/are computed as data traverse the network [72]. One problem in such a scheme is that a corrupted sensor providing incorrect measurements cannot be distinguished from a sensor under attack, where the attacker has either modified the environmental conditions or obtained the sensor's cryptographic secrets, in order to inject false measurements into the data sink. A novel secure data aggregation protocol is presented in [73] that is able to provide security, privacy and integrity for sensor networks, using inexpensive cryptographic tools. The main idea of the proposed A Balls and Bins Approach protocol is to define several *bins* for different *sensing intervals* and to demand each sensor to provide its sensed value adding one *ball* in the appropriate *bin*.

The aforementioned problem of deliberately-introduced corrupt data in an in-network aggregation protocol may be countered by exploiting the statistical properties found in the communicated data [74,75]. In particular, the naturally existing correlation between the readings produced by different sensors are taken into consideration to increase the resilience of data aggregation, without any special assumption on the distribution of the sensor readings, or the attacker's strategy.

Should the scheme involve the election of aggregator nodes, the authors in [76] discuss the requirements that need to be fulfilled, in order to have a non-manipulable aggregator node election protocol. Moreover, they provide a comparative review of three Secure Aggregator Node Election protocols, based on a particular threat model.

A similar private aggregator node election protocol, where the election is performed in an anonymous manner, was proposed in [77]. The objective of this protocol was to make it difficult for an adversary to identify aggregator nodes in the network and then physically compromise them. The protocol was deployed alongside with a private data aggregation protocol and a private query protocol that masked the data flows to and from the aggregator nodes, thus maintaining their privacy. An enhanced version of the protocol that is able to detect any misbehaviour within the network was also proposed, such as the one introduced by an attacker who injects false reports. Nevertheless, further research is required for the system to be able to identify the misbehaving node.

### 3.6. Miscellaneous network topics

Because of the very limited memory of certain types of devices (e.g. Harvard-based architecture devices, such as Mica motes), it was believed that these devices were immune to buffer overflow attacks that inject code into the stack and then execute it. Nevertheless, the authors in [78] demonstrated the feasibility of a remote code injection attack for Mica sensors, where the injected code is permanent, thus enabling the attacker to gain full control of the target sensor, persistently across reboots. What is more, they show how this attack can be transformed into a worm, namely, how to make the injected code self-replicating and therefore able to propagate through the WSN, with the potential of eventually forming a sensor botnet. The employed techniques for this attack involve return-oriented programming and fake stack injection. It only suffices for the attacker to corrupt one network node and use its keys to propagate the malware to its neighbours. Packet authentication and cryptographic techniques in general can make such code injection attacks more difficult; nevertheless, they cannot completely prevent them.

A security service protocol for MANETs, able to negotiate the security settings for the communications, is presented in [79], a feature that is particularly useful in heterogeneous networks, both in terms of hardware and of services provided. This negotiation protocol aims at selecting the cheapest services that consume the least possible amount of energy, while offering the highest possible security level among nodes with different security requirements. In addition, runtime negotiation of services is supported, thus making it suitable for cases where self-adaptivity is involved. Nevertheless, the protocol is not yet complete, and additional work is required on the message exchange for key management and errors.

The trustworthiness of messages received by peers is especially important in the context of e-vehicle safety-related applications (e.g. local danger warnings), as critical decisions often need to be made on those messages, decisions directly affecting passenger safety. To increase the trustworthiness in the said messages, a consensus mechanism can be used, that is, the same warning needs to be received at least $x$ times from peers before it is considered legitimate. Researchers in [80] investigate this threshold and its effect on the decision delay, including the possibility of malicious peers launching information forgery attacks.

## 4. MIDDLEWARE AND OVERLAY TECHNOLOGIES

Moving to higher layers, namely middleware and overlay, researchers have to tackle additional challenges as system complexity increases. On the other hand, operating from a higher level allows the utilisation of more advanced features, like the secure and efficient resource management (by aggregating information from the lower layers) and mechanisms to facilitate the interoperability and management of heterogeneous ES networks. It is, therefore, of no surprise that middleware and overlay technologies are a common area of research and development efforts for

**Table V.** Middleware and overlay technologies overview (projects that did not focus on these aspects have been left unchecked).

| Acronym | Secure middleware | Services and overlay applications | Reconfigurability and fault tolerance |
|---|---|---|---|
| AETHER | | | X |
| AWISSENET | | | |
| CESAR | | | |
| CHAT | | | X |
| EVITA | | | |
| GINSENG | X | | X |
| HYDRA | X | | |
| MADNESS | | | X |
| MORE | X | X | |
| OVERSEE | | | |
| PRESERVE | | | |
| pSHIELD | X | | |
| SecFutur | | | |
| SEPIA | X | X | |
| SMEPP | X | | X |
| TECOM | X | | |
| TERESA | | | X |
| UbiSec&Sens | X | | X |
| UNIQUE | | | |
| WSAN4CIP | | | |

many of the projects investigated, aiming to exploit the aforementioned tools in order to design secure embedded systems and related services.

This section is dedicated to presenting various types of middleware, such as trusted, service-oriented, context-aware, reconfigurable and fault-tolerant. Table V presents the middleware and overlay technologies, which were identified in this work.

## 4.1. Trusted middleware

Trusted Software is another important area of middleware layer research and Reiter *et al.* [81] propose a Trusted Software Stack (which acts as an interface between applications and a TPM) to be integrated into existing security framework, facilitating the adaptation to Trusted Computing technology. The prototype developed and proposed uses the .NET programming environment, taking advantage of the environment's fault-detection functionality (e.g. regarding buffer overflows), portability and developer base.

## 4.2. Service-oriented middleware

The main features of a secure, service-oriented middleware for embedded peer-to-peer systems, in order to face the various security challenges of the IoT, are presented in [82]. The notion of groups is used, as peers offer services inside groups and the discovery of these services is also performed within the group. Services can be state-less or state-full, and the latter ones may be session-less or session-full. The offered API allows for abstract peer and group management, as well as for events and message handling, features that facilitate application development within this environment. The presented service model and component-based middleware satisfies necessary principles such as security, heterogeneity, interoperability and scalability. The model was validated with two very different applications, including applications of WSN for monitoring radiation in nuclear power plants and for health-care in a mobile environment.

The deployment and orchestration of web services on heterogeneous embedded systems is another emerging research area and a task often assigned to the middleware layer, following the standardisation of the Devices Profile for Web Services (DPWS, [83]) open framework and research already conducted in the SIRENA project [84] and its follow-ups, SODA [85] and SOCRADES [86]. Some pervasive applications often require remote management and monitoring while maintaining interoperability, and the Web Services standard offers a solid basis for that. It is therefore justifiable that the runtime of the middleware developed for the MORE project [87] was based on the aforementioned DPWS specifications, as detailed in [88]. The DPWS4J [89] Java-based stack was extended and, to further facilitate development, the middleware is managed via the OSGi [90] modular service platform environment running on a Java Virtual Machine. Further enhancements were also introduced, enabling small footprint service orchestration in a DPWS-compliant environment [91]. The whole concept was validated on Gumstix Verdex XL6P embedded platforms.

### 4.3. Context-aware middleware

An extensive overview of context-aware middleware is presented in [92], categorising their properties and use. An ontology-based approach has been followed in [93], using the Web Ontology Language and Semantic Web Rule Language in order to develop monitoring and diagnosis rules. In this way, any malfunctions can be detected and self-healing procedures can be invoked, in an effective, extensible and scalable way, as it was proved by the experimental results.

Enriching the relations between the different systems' parts with semantic information, as well as exploiting contextual process data, can yield useful information, which can be fed into the various control and decision-making algorithms [94,95]. Utilising the aforementioned concepts to enhance user profiling and trust sharing and to offer content and context-awareness for cloud-based services is also examined in [96]. The proposed model is based on a representation of the cloud service through semantic integration and ontologies for user profiles, trust, context and content. Web Ontology Language restrictions are specified to guarantee access to trust-based context data.

### 4.4. Reconfigurable and fault-tolerant middleware

The aspect of reconfigurability and its repercussions on security are considered from a higher-level perspective in [97]. A security architecture is proposed, which, based on a middleware layer, offers secure reconfiguration and communication (i.e. SecComm component framework) with fine-grained application-specific policy enforcement, authenticated downloading from a remote source (i.e. ALoader component framework) as well as a re-keying service for key distribution and revocation (i.e. re-keying component framework).

The scheme presented in [98] is a configurable and adaptive middleware that aims at reducing the complexity of the realisation of an appropriate security level for a given WSN application. It consists of a modular middleware architecture, which separates core functionality needed for adaptability support from pure security functionalities and also introduces the concept of a middleware compiler. A suitable configuration tool compiles a security architecture at development time and the architecture allows for dynamic exchange of security modules at run time. An initial set of security modules is configured before the deployment of the application; the application programmer then has to specify the security functionality that is required by the application, such as secrecy and authentication, as well as some additional information regarding the hardware platform of the sensors (processor type, memory size, etc.). Based on this information, the appropriate security modules are selected. In cases where either the application needs have changed or an update is required for facing a newly-detected vulnerability, security modules can be exchanged after deployment. Such functionality is particularly useful for long-living applications.

Middleware can also be used in Kahn Process Networks implemented on a Network on Chip. In [99], a methodology for identifying requirements and implementing fault tolerance and adaptivity is presented. The overhead in terms of computational time and total data traffic can be lower than 10%, depending on the chosen bound of the connectors and the tokens' size being transferred at the application level. Because embedded systems exhibit a significant number of soft errors, their correction imposes equally significant hardware and real-time overhead. For improving embedded systems' dependability, the authors of [100] proposed an approach that exploits application knowledge to classify errors according to their relevance and the impact of their correction to the system. Avoiding to correct every single error (effectively delaying the error-correcting process) caused a reduction in the imposed correction overhead, thus making it easier to meet mandatory deadlines in cases where real-time behaviour is an absolute requirement.

Fault monitoring and fault-tolerant control for constrained sensor nodes is also examined in the GINSENG project [101,102], wherein a multi-layered, middleware-based architecture is proposed. The scheme involves multiple agents implementing distributed artificial intelligence techniques for robust control over the wireless sensor nodes and also details the communication and coordination mechanisms involved.

In [103], a middleware called MWSAN that provides high-level services for Wireless Sensor and Actor Networks (WSANs) is proposed, where the nodes are not only able to sense environmental data, but can also react by affecting the environment. It follows the component-oriented paradigm, and it leaves it up to the developers to configure it according to the actor and sensor resources, by taking into consideration issues such as the network configuration, the quality of service and coordination among actors. Because actor nodes are usually more powerful than sensor nodes, the middleware features high configurability to match the diversity of requirements between these two types of nodes. For instance, the middleware for sensors does not include the various actor-related components, thus leading to a much smaller memory footprint. What is more, provision has been made for enabling the definition of real-time characteristics, in order to offer improved temporal behaviour, such as cases of priority schemas where the highest priority events are executed first.

### 4.5. Overlay applications

Facilitating seamless online payments is another key issue researchers try to address. Such services often raise privacy concerns, and location-based services even more so. Privacy-preserving payment schemes are one of the main themes examined in the SEPIA project. Application scenarios involve end-users being equipped with mobile

devices featuring ARM processors and TrustZone support [104], like NFC-equipped smartphones. An application of the aforementioned privacy-preserving mechanism on NFC-enabled smartphones is presented in [105]. The proposed method is based on selective disclosure protocols, and experimental results on a standard JavaCard indicate that a key of up to 1024 bits may be feasible. Utilisation of the ARM TrustZone features would be beneficial to the security and overall performance of the model, as would further support for lightweight cryptography (e.g. ECC) on the JavaCard.

Cloud-related scenarios are an associated theme where, for instance, privacy issues arise from the application of the split processing mode on mobile transactions. In such schemes, lightweight tasks are executed on end-user devices (e.g. smartphones, tablets), whereas more demanding tasks are offloaded to the Cloud. The proposed payment scheme utilises ARM's TrustZone and Intel's Trusted Execution Technology, assuming the said support is present on both the client and the cloud provider platforms and allows the end-user to take advantage of the cloud resources while the cloud provider is unable to track users' activity patterns [106]. Moreover, the authors in [107,108] propose a node join protocol, which, via remote-attestation, does not allow nodes with unknown configurations to join the cloud network, thus alleviating concerns for control over data and code execution on such networks. Proof-of-concept implementations are presented for the Android operating system, both on Intel and on ARM-based platforms. Presented work assumes every node hosts a TPM, which, in the case of the ARM platform, requires an add-on module to be installed. With the add-on module in place, the ARM prototype's security qualities were similar to those of the x86-based platform.

## 5. ARCHITECTURES AND FORMALISATION

Embedded systems are usually the building blocks of a greater and more complex systems, created for a given purpose. A careful design of such architectures, as well as of their provided services, would certainly have a positive effect on any security-related issues, by minimising unforeseen flaws and deficiencies. What is more, formalising the process of designing and building embedded systems would, in most cases, lead to an easier integration of the final system, while maintaining high levels of security and dependability.

In this section, such proposed frameworks and architectures are presented for different application areas: safety-critical applications, security and dependability applications, and smart vehicle applications. Table VI gives an overview of the attempts related to architecture and formalisation, along with the respective projects.

Some approaches in current research focus on providing fully featured frameworks and/or formalising the process of designing and developing secure and dependable embedded systems, especially in applications where safety is critical. In [109], the two distinct domains of embedded systems and security are considered, and an appropriate view of a final system model is provided, aiming to support cooperation between the two domains, while leaving them independent from each other. The proposed scheme is intended for on-demand provision of communication services in crisis-related situations, where different actors could be involved, also bearing heterogeneous client devices. The model consists of two components: The System Security Interface that abstracts the system design model for communicating security needs and resource availability and the Security Building Block that abstracts the implementation for a security mechanism.

In [110], a process metamodel is introduced, which takes safety lifecycle requirements into consideration for secure software engineering (e.g. validation). This concept is explored further in [111], where a process metamodel, the Repository-Centric Process Metamodel (RCPM) is described. RCPM includes safety lifecycle concepts at its core and includes software tools for creating the required models, as well as a case study based on a railway application. Moreover, the authors in [112] present a model-based framework, which focuses on formalising and managing fault-tolerance and redundancy concepts and which uses composable UML components to construct fault-tolerant infrastructures. A test case of a fault-tolerant GPS is evaluated using the aforementioned system. A similar model-based technique is used in [113] aiming to encode security and dependability (S&D) patterns, while introducing artefacts for the formal validation of these patterns.

**Table VI.** Architecture and formalisation efforts overview (projects that did not focus on these aspects have been left unchecked).

| Acronym | Architectures | Formalisation |
|---|---|---|
| AETHER | | |
| AWISSENET | | |
| CESAR | X | X |
| CHAT | | |
| EVITA | X | X |
| GINSENG | | |
| HYDRA | | |
| MADNESS | | |
| MORE | | |
| OVERSEE | | X |
| PRESERVE | X | |
| pSHIELD | | |
| SecFutur | X | |
| SEPIA | | |
| SMEPP | | |
| TECOM | | |
| TERESA | X | |
| UbiSec&Sens | | |
| UNIQUE | | |
| WSAN4CIP | | |

Therefore, the fulfilment of S&D requirements identified at higher abstraction levels can be validated via the proposed process. The concept of S&D formalisation is further explored in [114], where the authors focus on the systematic reuse of S&D patterns in embedded systems where S&D are major concerns. To facilitate, automate and enforce fulfilment of S&D requirements, Jouvray *et al.* [115] define a trust-aware platform-independent architecture, the TECOM architecture, as it was the outcome of the research project bearing the same name. An attempt to encode S&D patterns utilising meta-modelling techniques can also be found in [116], while the said work also includes an implementation of those patterns using a profiled UML and adapted to resource-constrained embedded systems. The goal is to help application developers integrate the application building blocks they typically use with S&D building blocks. Furthermore, the authors in [117] apply modelling techniques on reconfigurable systems; namely, distributed real-time embedded systems. The approach presented is called RCA4RTES, and published work includes the case study of a GPS, where the dynamic reconfigurations of the system are described by state machines.

With the widespread use of embedded systems leading to the IoT, smart vehicles are another emerging and significant application. The potential new features and services available to vehicle occupants are, of course, numerous. Still, S&D is essential in this scenario, and any compromise to the safety of vehicle occupants and other road users would not be acceptable. For example, over-the-air updates that extend functionality through the offered services could be exploited by an attacker for installing malicious firmware during an over-the-air diagnosis and firmware update procedure. The authors in [118] introduce the Open VEhiculaR SEcurE platform, which aims to provide a standardised vehicular infrastructure with a protected runtime environment and on-board access and communication points. The proposed platform allows the integration of multiple Engine Control Units into one hardware node, offering temporal and spatial isolation, a secure interface for connecting to external networks (e.g. the Internet), and also the required interfaces and open APIs to allow the secure download and execution of OEM and third party applications, much like the functionality offered by smartphones and their application "markets" [119,120]. Part of the research in the field is more engineering-oriented in nature. The authors in [121] present such an approach, as developed on project CESAR. Functional safety and tool-chain integration are the main challenges, which researchers try to address by developing a reference technology platform. The work presented in [122] extends the safety-oriented environment AVATAR (a SysML modelling language framework) [123] with security constructs and verification techniques, to formally secure safety-critical automotive applications.

A capability-based, object-oriented software architecture is presented in [124]. Featuring a micro-kernel interface and enforceable security policies along with virtualisation provisions, it aims to improve security and provide isolation between multiple untrusted software components.

The authors in [125] propose Privacy-by-Design, that is, a systematic approach of integrating privacy requirements onto the design and implementation of a system. Using ontologies, a formal method is introduced, which allows the evaluation of the system in terms of the realisation of those pre-defined privacy requirements. The application of this method on the development of ITS applications is demonstrated in [126].

## 6. OPEN ISSUES AND FUTURE WORK

The increased complexity and interconnection of the current systems' components, as well as the varying and often undefined security levels of the networks they consist of, demand different approaches in the way the requirements are stated, in addition to the way these systems are designed. An integrated approach is required, where the components' security level is properly and systematically assessed, thus enabling the correct evaluation of the architecture's overall security level. In order for this to occur, reliable and useful metrics need to be defined, also applicable to legacy and therefore potentially insecure systems.

Furthermore, lightweight alternatives or improvements to existing cryptographic primitives and key distribution mechanisms could be looked into. Even though plenty of mechanisms and techniques that would typically be deployed to secure other types of computing devices (e.g. for access control, cryptography, network routing etc.) already exist, they are not always applicable or have limited efficacy in the context of embedded systems.

The development of comprehensive cryptographic tools focused on embedded systems and featuring lightweight primitives could be a very important development, including utilisation of TPM functionality and virtualisation features, where available. Similarly, extending and improving the interoperability of existing, standardised, cryptographic mechanisms (e.g. IPsec) with new types of networks (e.g. 6LoWPAN deployments) would be desirable.

Wearable systems introduce more challenges, like developing the means to securely and seamlessly collect, store and transmit various data, some of which might be private sensitive in nature (thus having to consider regulatory compliance issues that arise when dealing with such data). Access to location-based services is commonly required in such applications, as well as various vehicular and smartphone-related smart services, which again raises various privacy concerns. This mandates the development of efficient anonymising schemes, which must allow the user to access the said services, while prohibiting the service provider from uniquely identifying the specific user and her location among the rest of the users.

Future research is also expected to focus on revising the traditional role of middleware (namely, facilitating inter-

action and compositions via discovery and orchestration). By upgrading middleware technologies and transforming them into recommendation engines, able to dynamically and adaptively detect patterns and predict potential service interactions, embedded systems will better reflect the new crowdsourcing, social and generally human-related applications. These changes though are bound to introduce novel security and privacy issues that will have to be addressed.

The concepts of self-reconfiguration (e.g. in order to adapt to changes in the security levels, network, application/user requirements or location) and self-recovery (e.g. in fault conditions) could be investigated further. This can be achieved via on-the-fly hardware and/or software changes and can even be used to enhance the robustness of embedded systems against side-channel attacks (by controlling electromagnetic emissions etc.).

Moreover, there is a room for improvement on the formalisation, definition and application of S&D concepts. It is important to be able to formalise S&D requirements and product lifecycle in general, accurately modelling the processes from research and development until the end product. In this way, it will enable the validation of the end product whether it meets all S&D and the other requirements defined at earlier stages.

As future work in the context of the survey presented in this paper, it would be interesting to examine each of the sections (e.g. node) and their identified technologies separately and with respect to the current state of the art for each of the identified technologies of the section. Such a comparison would facilitate the evaluation of the results of EU-funded research efforts in a global context and help draw useful conclusions about the quality of the projects' output and the return on European investments in the said research topics.

## 7. CONCLUSIONS

A survey was performed on EU-funded research projects related to embedded systems security, a very active topic with many completed and ongoing projects, which have received significant funding. From this survey, certain patterns have emerged regarding the issues investigated and the technologies researchers focus on, in order to address the said issues. As the application areas of secure embedded systems evolve, handling sensitive private data and assuming critical roles, their requirements change accordingly, and certain security issues become more pressing. This is expected to continue as the focus now shifts to vehicular and other safety-related applications, automated payment schemes, smart-metering and Industry 4.0 applications, most of which are also expected to provide services interoperable with traditional networks and the Internet, in order to realise the IoT. Various open security issues exist in all of the aforementioned areas of application; issues that future research will have to deal with and hopefully resolve.

## ACKNOWLEDGEMENTS

This work has been supported by the Greek General Secretariat for Research and Technology (GSRT), under the ARTEMIS JU research programme nSHIELD (new embedded Systems arcHItecturE for multi-Layer Dependable solutions) project. Call: ARTEMIS-2010-1, Grant Agreement No. 269317.

## REFERENCES

1. Fysarakis K, Hatzivasilis G, Rantos K, Papanikolaou A, Manifavas C. Embedded systems security challenges, *Measurable Security for Embedded Computing and Communication Systems (MeSeCCS 2014), within the International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2014)*, Lisbon, Portugal, January 2014; 255–266.
2. new embedded Systems arcHItecturE for multi-Layer Dependable solutions (nSHIELD). (Available from: http://www.newshield.eu) n.d. Accessed 15/09/2014.
3. Crossbow Technology. (Available from: http://www.moog-crossbow.com) n.d. Accessed 15/09/2014.
4. Gumstix. (Available from: https://www.gumstix.com) n.d. Accessed 15/09/2014.
5. Acme Systems. FOX LX. (Available from: http://www.acmesystems.it/FOXLX) n.d. Accessed 15/09/2014.
6. Freescale. i.MX51 processors. (Available from: http://www.freescale.com/webapp/sps/site/taxonomy.jsp?code=IMX51_FAMILY) n.d. Accessed 15/09/2014.
7. Xilinx. Spartan-6 FPGA Family. (Available from: http://www.xilinx.com/products/silicon-devices/fpga/spartan-6/index.htm) n.d. Accessed 15/09/2014.
8. Dietrich K, Winter J, Luzhnica G, Podesser S. Implementation aspects of anonymous credential systems for mobile trusted platforms, *12th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security (CMS '11)*, Ghent, Belgium, October 2011; 45–58. SEPIA.
9. Dietrich K, Winter J. Towards customizable, application specific mobile trusted modules, *5th ACM Workshop on Scalable Trusted Computing (STC '10)*, ACM New York, NY, USA, October 2010; 31–40. SEPIA.
10. ARM Security Technology. Building a secure system using TrustZone technology, 2008. (Available from: http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf). Accessed 15/09/2014.

11. Böttcher A, Kauer B, Härtig H. Trusted computing serving an anonymity service. In *1st International Conference on Trusted Computing and Trust in Information Technologies: Trusted Computing (Trust '08) – Challenges and Applications*. Springer Berlin: Heidelberg, March 2008; 143–154. TECOM.
12. Hartig H, Hohmuth M, Feske N, Helmuth C, Lackorzynski A, Mehnert F, Peter M. The Nizza secure-system architecture, *International Conference on Collaborative Computing: Networking, Applications and Worksharing*, San Jose, CA, USA, 2005; 10.
13. Muñoz A, Maña A, Antón P. In the track of the agent protection: a solution based on cryptographic hardware. In *Computer Network Security*, vol. 6258, Kotenko I, Skormin V (eds), LNCS. Springer Berlin: Heidelberg, 2010; 284–297. SecFutur.
14. Winter J, Dietrich K. A hijacker's guide to the LPC bus. In *Public Key Infrastructures, Services and Applications*, vol. 7163, Petkova-Nikova S, Pashalidis A, Pernul G (eds), LNCS. Springer Berlin: Heidelberg, 2012; 176–193. SEPIA.
15. Vater F, Peter S, Langendörfer P. Combinatorial logic circuitry as means to protect low cost devices against side channel attacks. In *Information Security Theory and PracticesSmart Cards, Mobile and Ubiquitous Computing Systems*, vol. 4462, Sauveron D., Markantonakis K., Bilas A, Quisquater JJ (eds), LCNS. Springer Berlin: Heidelberg, 2007; 244–253. UbiSec&Sens.
16. Christou P, Kyriakoulakos K, Sotiriadis E, Papadopoulos K, Mplemenos GG, Papaefstathiou I. Low-power security modules optimized for WSNs, *16th International Workshop on Systems, Signals and Image Processing (IWSSIP)*, Chalkida, Greece, June 2009; 1–4. AWISSENET.
17. Mplemenos GG, Christou P, Papaefstathiou I. Using reconfigurable hardware devices in WSNs for accelerating and reducing the power consumption of header processing tasks, *IEEE Advanced Network and Telecommunication Systems (ANTS '09)*, New Delhi, India, December 2009; 1–3. AWISSENET.
18. Mplemenos GG, Papadopoulos K, Brokalakis A, Chrysos G, Sotiriades E, Papaefstathiou I. RESENSE: reconfigurable WSN nodes. In *The Second Wireless Sensing Showcase (WiSiG Showcase '09)*. National Physical Laboratory: London, UK, 2009. AWISSENET.
19. Simons P, van der Sluis E, van der Leest V. Buskeeper PUFs, a promising alternative to D flip-flop PUFs, *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST '12)*, San Francisco, CA, USA, June 2012; 7–12. UNIQUE.
20. Katzenbeisser S, Koçabas Ü, Leest V, Sadeghi AR, Schrijen GJ, Schröder H, Wachsmann C. Recyclable PUFs: logically reconfigurable PUFs. In *Cryptographic hardware and embedded systems (ches '11)*, vol. 6917, Preneel B, Takagi T (eds), LNCS. Springer Berlin: Heidelberg, 2011; 374–389. UNIQUE.
21. Petit J, Bosch C, Feiri M, Kargl F. On the potential of PUF for pseudonym generation in vehicular networks, *IEEE Vehicular Networking Conference (VNC)*, Seoul, South Korea, November 2012; 94–100. PRESERVE.
22. Feiri M, Petit J, Kargl F. Efficient and secure storage of private keys for pseudonymous vehicular communication, *First Workshop on Security, Privacy and Dependability for Cybervehicles (CyCar '13) at 20th ACM Conference on Computer and Communications Security (CCS '13)*, ACM, New York, NY, USA, November 2013; 9–18. PRESERVE.
23. Ben Hamida ST, Pierrot JB, Castelluccia C. An adaptive quantization algorithm for secret key generation using radio channel measurements, *3rd International Conference on New Technologies, Mobility and Security (NTMS '09)*, Cairo, Egypt, December 2010; 1–5. WSAN4CIP.
24. Brakensiek J, Dröge A, Botteck M, Härtig H, Lackorzynski A. Virtualization as an enabler for security in mobile devices, *1st Workshop on Isolation and Integration in Embedded Systems (IIES '08)*, ACM New York, NY, USA, April 2008; 17–22. TECOM.
25. Peter M, Schild H, Lackorzynski A, Warg A. Virtual machines jailed – virtualization in systems with small trusted computing bases, *1st Eurosys Workshop on Virtualization Technology for Dependable Systems (VDTS '09)*, ACM New York, NY, USA, March 2009; 18–23. TECOM.
26. Schild H, Lackorzynski A, Warg A. Faithful virtualization on a real-time operating system, *Eleventh Real-Time Linux Workshop*, Dresden, Germany, 2009; 237–243. TECOM.
27. Steinberg U, Kauer B. NOVA: a microhypervisor-based secure virtualization architecture, *5th European Conference on Computer Systems (EuroSyS '10)*, ACM New York, NY, USA, 2010; 209–222. TECOM.
28. Liebergeld S, Peter M, Lackorzynski A. Towards modular security-conscious virtual machines, *Twelfth Real-Time Linux Workshop*, Nairobi, Kenya, October 2010. TECOM https://www.osadl.org/RTLWS-Submitted-Papers.rtlws12-submitted-papers.0.html.
29. Dietrich K, Winter J. Towards a trustworthy, lightweight cloud computing framework for embedded systems, *4th International Conference on Trust*

*and Trustworthy Computing (TRUST '11)*, Pittsburgh, PA, USA, June 2011; 16–32. SEPIA.

30. Trakadas P, Zahariadis T, Leligou HC, Voliotis S. Analyzing energy and time overhead of security mechanisms in wireless sensor networks, *15th International Conference on Systems, Signals and Image Processing (IWSSIP '08)*, Bratislava, Slovak Republic, June 2008; 137–140. AWISSENET.
31. Kargl A, Pyka S, Seuschek H. Fast arithmetic on ATmega128 for elliptic curve cryptographyIACR Cryptology ePrint Archive, 2008, SMEPP.
32. Li S, Li T, Wang X, Zhou J, Chen K. Efficient link layer security scheme for wireless sensor networks. *Journal of Information and Computational Science* June 2007; **4**(2): 553–567, SMEPP.
33. Karlof C, Sastry N, Wagner D. TinySec: a link layer security architecture for wireless sensor networks, *2nd International Conference on Embedded Networked Sensor Systems (SenSyS '04)*, ACM New York, NY, USA, November 2004; 162–175.
34. Poschmann A, Leander G, Schramm K, Paar C. New lightweight crypto algorithms for RFID, *IEEE International Symposium on Circuits and Systems (ISCAS '07)*, New Orleans, Louisana, USA, May 2007; 1843–1846. UbiSec&Sens.
35. Uhsadel L, Poschmann A, Paar C. Enabling full-size public-key algorithms on 8-bit sensor nodes. In *Security and Privacy in Ad-hoc and Sensor Networks*, vol. 4572, Stajano F, Meadows C, Capkun S, TM (eds), LNCS. Springer Berlin: Heidelberg, 2007; 73–86. UbiSec&Sens.
36. Vater F, Langendörfer P. An area efficient realisation of AES for wireless devices. *it – Information Technology* 2007; **49** (3): 188–193, UbiSec&Sens.
37. Poschmann A, Westhoff D, Weimerskirch A. Dynamic code update for the efficient usage of security components in WSNs, *Communication in Distributed Systems (KIVS), ITG-GI Conference*, Bern, Switzerland, February 2007; 1–11. UbiSec&Sens.
38. Potzmader K, Winter J, Hein D, Hanser C, Teu P, Chen L. Group signatures on mobile devices: practical experiences. In *Trust and Trustworthy Computing*, vol. 7904, Huth M, Asokan N, Čapkun S, Flechais I, Coles-Kemp L (eds), LNCS. Springer Berlin: Heidelberg, June 2013; 47–64. SEPIA.
39. Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 packets over IEEE 802.15.4 networksRFC 4944, 2007.
40. Poettner WB, Wolf L. IEEE 802.15.4 packet analysis with Wireshark and off-the-shelf, *Poster presented at the 7th International Conference on Networked Sensing Systems (INSS'10)*, Kassel, Germany, 2010. GINSENG.
41. Granjal J, Monteiro E, Sá Silva J. Enabling network-layer security on IPv6 wireless sensor networks, *IEEE Global Telecommunications Conference (GLOBECOM '10)*, Miami, FL, USA, 2010; 1–6. GINSENG.
42. Granjal J, Monteiro E, Sá Silva J. A secure interconnection model for IPv6 enabled wireless sensor networks, *IFIP Wireless Days (WD '10)*, Venice, Italy, 2010; 1–6. GINSENG.
43. Trakadas P, Zahariadis T, Leligou HC, Voliotis S, Papadopoulos K. AWISSENET: setting up a secure wireless sensor network, *50th International Symposium ELMAR 2008, Focused on Mobile Multimedia*, Zadar, Croatia, September 2008; 519–523. AWISSENET.
44. Papadopoulos K, Zahariadis T, Leligou HC, Voliotis S. Sensor networks security issues in augmented home environment, *12th IEEE International Symposium on Consumer Electronics (ISCE '08)*, Vilamoura, Portugal, April 2008; 519–523. AWISSENET.
45. Dietrich K. Anonymous client authentication for transport layer security. In *Communications and Multimedia Security*, vol. 6109, LNCS. Springer Berlin: Heidelberg, May 2010; 268–280.
46. Wachsmann C, Chen L, Dietrich K, Löhr H, Sadeghi AR, Winterhor J. Lightweight anonymous authentication with TLS and DAA for embedded mobile devices. In *Information Security*, vol. 6531, Burmester M, Tsudik G, Magliveras S, Ilić I (eds), LNCS. Springer Berlin: Heidelberg, October 2010; 84–98. SEPIA.
47. Dietrich K, Winter J. A secure and practical approach for providing anonymity protection for trusted platforms, *12th International Conference on Information and Communications Security (ICICS '10)*, Barcelona, Spain, December 2010; 311–324. SEPIA.
48. *Near Field Communication (NFC)*. (Avaiable from: http://www.nfc-forum.org/home) n.d.
49. Dietrich K. Anonymous RFID authentication using trusted computing technologies. In *Radio Frequency Identification: Security and Privacy Issues*, vol. 6370, Ors Yalcin SB (ed), LNCS. Springer Berlin: Heidelberg, 2010; 91–102. UNIQUE.
50. Dietrich K. An integrated architecture for trusted computing for Java enabled embedded devices, *ACM Workshop on Scalable Trusted Computing (STC '07)*, ACM New York, NY, USA, 2007; 2–6. SEPIA.
51. Armknecht F, Chen L, Sadeghi AR, Wachsmann C. Anonymous authentication for RFID systems. In *Radio Frequency Identification: Security and Privacy*

*Issues*, vol. 6370, Ors Yalcin SB (ed), LNCS. Springer Berlin: Heidelberg, June 2010; 158–175. UNIQUE.

52. Manolopoulos V, Papadimitratos P, Tao S, Rusu A. Securing smartphone based ITS, *11th IEEE International Conference on its Telecommunications (ITST)*, St. Petersburg, Russia, August 2011; 201–206. PRESERVE.
53. Alexiou N, Laganá M, Gisdakis S, Khodaei M, Papadimitratos P. VeSPA: vehicular security and privacy-preserving architecture, *2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (HotWiSec '13)*, ACM New York, NY, USA, 2013; 19–24. PRESERVE.
54. Alexiou N, Gisdakis S, Lagana M, Papadimitratos P. Towards a secure and privacy-preserving multi-service vehicular architecture, *IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '13)*, Madrid, Spain, June 2013; 1–6. PRESERVE.
55. Bibmeyer N, Petit J, Bayarou KM. CoPRA: conditional pseudonym resolution algorithm in VANETs, *10th Annual Conference on Wireless on-Demand Network Systems and Services (WONS '13)*, Banff, AB, Canada, March 2013; 9–16. PRESERVE.
56. Road vehicles – vehicle to grid communication interface – Part 1: general information and use-case definition, 2013.
57. Höfer C, Petit J, Schmidt RK, Kargl F. POPCORN: privacy-preserving charging for eMobility, *First Workshop on Security, Privacy and Dependability for Cybervehicles (CyCar '13) at 20th ACM Conference on Computer and Communications Security (CCS '13)*, ACM, New York, NY, USA, November 2013; 37–48. PRESERVE.
58. Zahariadis T, Ladis E, Leligou HC, Trakadas P, Tselikis C, Voliotis S. Trust models for sensor networks. In *50th International Symposium ELMAR-2008*, Grgić M, Grgić S (eds). Croatian Society Electronics in Marine – ELMAR: Zadar, Croatia, September 2008; 511–514. AWISSENET.
59. Zahariadis T, Leligou H, Voliotis S, Maniatis S, Trakadas P, Karkazis P. An energy and trust-aware routing protocol for large wireless sensor networks. *WSEAS Transactions on Communications* September 2009; **8**(9): 981–991, AWISSENET.
60. Kuntze N, Rudolph C, Paatero J. Establishing trust between nodes in mobile ad-hoc networks. In *Trusted Systems*, vol. 7711, Mitchell CJ, Tomlinson A (eds), LNCS. Springer Berlin: Heidelberg, December 2012; 48–62. SecFutur.
61. Oberle A, Rein A, Kuntze N, Rudolph C, Paatero J, Lunn A, Racz P. Integrating trust establishment into routing protocols of today's MANETs, *Wireless Communications and Networking Conference (WCNC '13)*, Shanghai, China, April 2013; 2369–2374. SecFutur.
62. Neumann A, Aichele C, Lindner M, Wunderlich S. Better approach to mobile ad-hoc networking (B.A.T.M.A.N.). *IETF Internet Draft – Experimental*, Network Working Group, 2008.
63. Karjalainen A, Kangasharju J. On interactions between routing and service discovery in wireless sensor networks, *International Conference on Information NETWORKING (ICOIN '10)*, Busan, South Korea, 2010. AWISSENET.
64. Fagiolini A, Valenti G, Pallottino L, Dini G, Bicchi A. Local monitor implementation for decentralized intrusion detection in secure multi-agent systems, *IEEE International Conference on Automation Science and Engineering (CASE '07)*, Scottsdale, AZ, USA, September 2007; 454–459. CHAT.
65. Fagiolini A, Babboni F, Bicchi A. Dynamic distributed intrusion detection for secure multi-robot systems, *IEEE International Conference on Robotics and Automation (ICRA '09)*, Kobe, Japan, May 2009; 2723–2728. CHAT.
66. García-Otero M, Álvarez-García F, Casajús-Quirós FJ. Securing wireless sensor networks by using location information, *16th International Workshop on Systems Signals and Image Processing (IWSSIP '09) – Special Session: Security in WSNS*, Chalkida, Greece, June 2009; 1–4. AWISSENET.
67. Zurutuza U, Ezpeleta E, Herrero Á, Corchado E. Visualization of misuse-based intrusion detection: application to honeynet data. In *Soft Computing Models in Industrial and Environmental Applications, 6th International Conference SOCO 2011*, vol. 87, Corchado E, Snášel V, Sedano J., Hassanien AE, Calvo JL, Ślęzak D (eds), Advances in Intelligent and Soft Computing. Springer Berlin: Heidelberg, April 2011; 561–570. pSHIELD.
68. Fiore M, Casetti EC, Chiasserini C, Papadimitratos P. Discovery and verification of neighbor positions in mobile ad hoc networks. *IEEE Transactions on Mobile Computing* 2013; **12**(2): 289–303, PRESERVE.
69. Bißmeyer N, Njeukam J, Petit J, Bayarou KM. Central misbehavior evaluation for VANETs based on mobility data plausibility, *9th ACM International Workshop on Vehicular Inter-Networking, Systems, and Applications (VANET '12)*, ACM New York, NY, USA, 2012; 73–82. PRESERVE.
70. Dietzel S, Petit J, Heijenk G, Kargl F. Graph-based metrics for insider attack detection in VANET multi-hop data dissemination protocols.

*IEEE Transactions on Vehicular Technology* 2013; **62**(4): 1505–1518, PRESERVE.
71. Wouter van der Heijden R, Dietzel S, Kargl F. SeDyA: secure dynamic aggregation in VANETs, *6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*, ACM, New York, NY, USA, November 2013; 131–142. PRESERVE.
72. Intanagonwiwat C, Estrin D, Govindan R, Heidemann J. Impact of network density on data aggregation in wireless sensor networks, *22nd International Conference on Distributed Computing Systems (ICDS '02)*, Vienna, Austria, July 2002; 457–458.
73. Castelluccia C, Soriente C. ABBA: a balls and bins approach to secure aggregation in WSNs, *6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops (WiOPT '08)*, Berlin, Germany, April 2008; 185–191. UbiSec&Sens.
74. Schaffer P, Vajda I. CORA: correlation-based resilient aggregation in sensor networks, *10th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '07)*, Chania, Crete, Greece, October 2007; 373–376. UbiSec&Sens.
75. Buttyán L, Schaffer P, Vajda I. CORA: correlation-based resilient aggregation in sensor networks. *Ad Hoc Networks* 2009; **7**(6): 1035–1050, UbiSec&Sens.
76. Sivrianosh M, Westhoff D, Armknecht F, Girao J. Non-manipulable aggregator node election protocols for wireless sensor networks, *5th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOPT '07)*, Limassol, Cyprus, April 2007; 1–10. UbiSec&Sens.
77. Holczer T, Buttyan L. Anonymous aggregator election and data aggregation in wireless sensor networks. *International Journal of Distributed Sensor Networks* 2011; **2011**, Article ID 828414WSAN4CIP. (Available from: http://www.hindawi.com/journals/ijdsn/2011/828414).
78. Francillon A, Castelluccia C. Code injection attacks on harvard-architecture devices, *15th ACM Conference on Computer and Communications Security (CCS '08)*, Alexandria, Virginia, USA, October 27–31 2008; 15–26. UbiSec&Sens.
79. Taddeo AV, Ferrante A. A security service protocol for MANETs, *6th IEEE Consumer Communications and Networking Conference (CCNC '09)*, Las Vegas, NV, USA, 2009; 1–2. AETHER.
80. Petit J, Feiri M, Kargl F. Spoofed data detection in VANETs using dynamic thresholds, *3rd IEEE Vehicular Networking Conference (VNC 2011)*, Amsterdam, The Netherlands, November 2011; 25–32. PRESERVE.
81. Reiter A, Neubauer G, Kapfenberger M, Winter J, Dietrich K. Seamless integration of trusted computing into standard cryptographic frameworks, *2nd International Conference on Trusted Systems (INTRUST '10)*, Bejing, China, December 2010; 1–25. SEPIA.
82. Díaz M, Garrido D, Reyna A. One step closer to the Internet of things: SMEPP, *International Workshop on the Future Internet of Things and Services – Embedded Web Services for Pervasive Devices*, Berlin, Germany, 2009. SMEPP.
83. OASIS. Devices profile for web services (DPWS), 2009. (Available from: http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01) Accessed 15/09/2014.
84. *SIRENA project*. (Available from: https://itea3.org/project/sirena.html) n.d. Accessed 15/09/2014.
85. SODA project. (Available from: https://itea3.org/project/SODA.html) n.d. Accessed 15/09/2014.
86. SOCRADES project. (Available from: http://www.socrades.eu) n.d. Accessed 15/09/2014.
87. MORE project. (Available from: http://www.hydramiddleware.eu/articles.php?article_id=18) n.d. Accessed 15/09/2014.
88. Schmutzler J, Bieker U, Wietfeld C. Network-centricv middleware supporting dynamic web service deployment on heterogeneous embedded systems, *14th International Conference on Concurrent Enterprising,* ICE, Lisbon, Portugal, June 2008; 95–102. MORE.
89. Device Profile for Web Services specification for Java (DPWS4J). (Available from: https://forge.soa4d.org/projects/dpws4j) n.d. Accessed 15/09/2014.
90. Open Service Gateway initiative (OSGi). (available from: http://www.osgi.org) n.d.
91. Timm C, Schmutzler J, Marwedel P, Wietfeld C. Dynamic web service orchestration applied to the device profile for web services in hierarchical networks, *ICSt/IEEE 4th International Conference on Communication System Software and Middleware*, Dublin, Ireland, June 2009; 18:1–18:6. MORE.
92. Kjær KE. A survey of context-aware middleware, *25th Conference on IASTED International Multi-Conference: Software Engineering*, Innsbruck, Austria, 2007; 148–155. HYDRA.
93. Zhang W, Hansen KM. An OWL/SWRL based diagnosis approach in a pervasive middleware, *20th International Conference on Software Engineering and Knowledge Engineering (SEKE '08),* Knowledge Systems Institute Graduate School, Skokie, Illinois, USA, 2008; 893–898. HYDRA.
94. Fiaschetti A, Lavorato F, Suraci V, Palo A, Taglialatela A, Morgagni A, Baldelli R, Flammini F. On the use of semantic technologies to model and control security, privacy and dependability in complex sys-

tems, Computer Safety, Reliability, and Security, 2011. pSHIELD.

95. Chowdhury MMR, Noll J. Securing critical infrastructure: a semantically enhanced sensor based approach, *2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE)*, Chennai, India, February 2011; 1–5. pSHIELD.
96. Noll J, Iqbal Z, Chowdhury M MR. *Integrating context- and content-aware mobile services into the cloud*. CWI/CTIF Seminar on Mobile Cloud Computing and Wireless Applications, Aalborg University, Copenhagen October 2011. pSHIELD.
97. Dini G, Savino IM. A security architecture for reconfigurable networked embedded systems. *International Journal of Wireless Information Networks* 2010; **17**(1–2): 11–25, CHAT.
98. Langendoerfer P, Peter S, Piotrowski K, Nunes R, Casaca A. A vmiddleware approach to configure security in WSN, *1st ERCIM Workshop on Emobility, in Conjunction with WWIC 2007*, Coimbra, Portugal, May 2007; 83–94. UbiSec&Sens.
99. Derin O, Diken E, Fiorin L. A middleware approach to achieving fault tolerance of kahn process networks on networks on chips. *International Journal of Reconfigurable Computing* 2011; **2011**, Article ID 295385MADNESS.
100. Heinig A, Engel M, Schmoll F, Marwedel P. Using application knowledge to improve embedded systems dependability, *Workshop on Hot Topics in System Dependability (HotDep '10)*, Vancouver, BC, Canada, October 2010. MADNESS.
101. Nunes G, Cardoso A, Santos A, Gil P. Multi-agent topologies over WSANs in the context of fault tolerant supervision. In *Technological innovation for sustainability*, vol. 349, Camarinha-Matos LM. (ed), IFIP Advances in Information and Communication Technology. Springer Berlin: Heidelberg, 2011; 383–390. GINSENG.
102. Nunes G, Cardoso A, Santos A, Gil P. Multi-agent based architecture for robust supervision over wireless sensor networks, *9th Portuguese Conference on Automatic Control (Controlo 2010)*, Coimbra, Portugal, September 2010. GINSENG.
103. Barbarán J, Díaz M, Esteve I, Garrido D, Llopis L, Rubio B. A real-time component-oriented middleware for wireless sensor and actor networks, *1st International Conference on Complex, Intelligent and Software Intensive Systems (CISIS '07)*, Vienna, Austria, 2007; 3–10. SMEPP.
104. Slamanig D, Pirker M. A framework for privacy-preserving mobile payment on security enhanced ARM TrustZone platforms, *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, Liverpool, United Kingdom, June 2012; 1155–1160. SEPIA.
105. Derler D, Potzmader K, Winter J, Dietrich K. Anonymous ticketing for NFC-enabled mobile phones. In *Trusted Systems*, vol. 7222, Chen L, Yung M, Zhu L (eds), LNCS. Springer Berlin: Heidelberg, 2012; 66–83. SEPIA.
106. Pirker M, Slamanig D, Winter J. Practical privacy preserving cloud resource-payment for constrained clients. In *Privacy Enhancing Technologies*, vol. 7384, Fischer-Hübner S, Wright M (eds), LNCS. Springer Berlin: Heidelberg, 2012; 201–220. SEPIA.
107. Pirker M, Winter J, Toegl R. Lightweight distributed heterogeneous attested android clouds. In *Trust and Trustworthy Computing*, vol. 7344, Katzenbeisser S, Weippl E, Camp LJ, Volkamer M, Reiter M, Zhang X (eds), LNCS. Springer Berlin: Heidelberg, 2012; 122–141. SEPIA.
108. Pirker M, Winter J, Toegl R. Lightweight distributed attestation for the cloud, Porto, Portugal, 2012; 580–585. SEPIA.
109. Nadjm-Tehrani S, Vasilevskaya M. Towards a security domain model for embedded systems, *13th IEEE International Symposium on High-Assurance Systems Engineering (HASE '11)*, Boca Raton, FL, USA, November 2011; 180–181. SecFutur.
110. Zhang Y, Hamid B, Gouteux D. A metamodel for representing safety lifecycle development process, *6th International Conference on Software Engineering Advances (ICSEA 2011),* XPS, Barcelona, Spain, October 2011; 550–556. TERESA.
111. Hamid B, Geisel J, Ziani A, Gonzalez D. Safety lifecycle development process modeling for embedded systems – example of railway domain. In *Software Engineering for Resilient Systems*, vol. 7527, Avgeriou P (ed), LNCS. Springer Berlin: Heidelberg, 2012; 63–75. TERESA.
112. Ziani A, Hamid B, Bruel JM. A model-driven engineering framework for fault tolerance in dependable embedded systems design, *38th Euromicro Conference on Software Engineering and Advanced Applications (SEAA '12),* IEEE Computer Society, Cesme, Izmir, Turkey, September 2012; 166–169. TERESA.
113. Hamid B, Gürgens S, Jouvray C, Desnos N. Enforcing S&D pattern design in RCES with modeling and formal approaches. In *Model Driven Engineering Languages and Systems*, vol. 6981, Whittle J, Clark T,

Kühne T (eds), LNCS. Springer Berlin: Heidelberg, 2011; 319–333. TERESA.

114. Trujillo S, Alonso I, Hamid B, Gonzalez D, Blanco M, Zhang HY. Towards variability support for security and dependability patterns: a case study, *15th International Software Product Line Conference (SPLC '11)*, ACM New York, NY, USA, 2011; 27:1–27:4. TERESA.
115. Jouvray C, Sall M, Kung A. Enforcing trust in embedded systems using models. In *International Workshop on Security and Dependability for Resource Constrained Embedded Systems (S&D4RCES '10)*, Hamid B, Rudolph C, Rulan C (eds). ACM, 2010; 1:1–1:8. TERESA.
116. Hamid B, Desnos N, Grepet C, Jouvray C. Model-based security and dependability patterns in RCES: the TERESA approach, 2010; 8:1–8:4. TERESA.
117. Krichen F, Hamid B, Zalila B, Jmaiel M. Towards a model-based approach for reconfigurable DRE systems, 2011; 295–302. TERESA.
118. Groll A, Holle J, Ruland C, Wolf M, Wollinger T, Zweers F. OVERSEE – a secure and open communication and runtime platform for innovative automotive applications, *7th Embedded Security in Cars Workshop (ESCAR 2009)*, Düsseldorf, Germany, November 2009. OVERSEE.
119. Groll A, Holle J, Wolf M, Wollinger T. Next generation of automotive security: secure hardware and secure open platforms, *17th ITS World Congress*, Busan, South Korea, October 2010. OVERSEE.
120. McGuire N, Platschek A, Schiesser G. OVERSEE – a generic FLOSS communication and application platform for vehicles, *12th Real-Time Linux Workshop*, Nairobi, Kenya, October 2010. OVERSEE. (Available from: https://www.osadl.org/RTLWS-Submitted-Papers.rtlws12-submitted-papers.0.html).
121. Griessnig G, Kundner I, Armengaud E, Torchiaro S, Karlsson D. Improving automotive embedded systems engineering at european level. *E & I Elektrotechnik und Informationstechnik* 2011; **128**(6): 209–214, CESAR.
122. Pedroza G, Idrees MS, Apvrille L, Roudier Y. A formal methodology applied to secure over-the-air automotive applications, *IEEE Vehicular Technology Conference (VTC Fall)*, San Francisco, CA, USA, September 2011; 1–5. EVITA.
123. Knorreck D, Apvrille L, de Saqui-Sannes P. TEPE: a SysML language for time-constrained property modeling and formal verification. *ACM SIGSOFT Software Engineering Notes* 2011; **36**(1): 1–8, EVITA.
124. Lackorzynski A, Warg A. Taming subsystems – "Capabilities as universal resource access control in L4", *2nd Workshop on Isolation and Integration in Embedded Systems (IIES '09)*, Nuremburg, Germany, March 2009; 25–30. TECOM.
125. Kost M, Freytag JC, Kargl F, Kung A. Privacy verification using ontologies, *6th International Conference on Availability, Reliability and Security (ARES '11)*, Vienna, Austria, August 2011; 627–632. PRESERVE.
126. Kung A, Freytag J, Kargl F. Privacy-by-design in ITS applications, *IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Lucca, Tuscany, Italy, June 2011; 1–6. PRESERVE.