<FP7-ICT-STREP>

Contract No. 258280

TWISNet

Trustworthy Wireless Industrial Sensor Networks

Deliverable D3.2.2

Specification of a framework for identity management, authentication and access control

Contractual date:	M30
Actual submission date:	M30
Responsible beneficiary:	CEA
Authors:	Nouha OUALHA (CEA), Alexis OLIVEREAU (CEA), Laura Cristina GHEORGHE (UPB), Silvia STEGARU (UPB), Emil Slusanschi (UPB), Mario GIROD (HTW), Markus WEHNER (HTW), Dirk BURGGRAF (HTW), Axel SCHMIDT (HTW), Christian MOSCHNER (HTW), and Sven ZEISBERG (HTW)
Work package:	WP3
Security:	PU
Nature:	Report
Document name:	TWISNet_WP3_D3.2.2.doc
Version:	2.0

REVISION HISTORY

Date (dd.mm.yyyy)	Version	Author	Comments
10-02-2011	0.1	Nouha Oualha	added ToC
06-05-2011	1	Laura Gheorghe	added state of the art part of HTW
26-05-2011	2	Nouha Oualha	added state of the art part of CEA
09-08-2011	3	Laura Gheorghe	added conclusions for HTW sota
09-08-2011	4	Nouha Oualha	added conclusions for CEA sota
12-10-2011	5	Nouha Oualha	added architecture modules
14-10-2011	6	Markus Wehner	added subsystem and module descriptions for secure routing and packet forwarding
18-10-2011	7	Nouha Oualha	added module description for ID privacy and authentication and access control subsystems
14-11-2011	8	Nouha Oualha	added task architecture figure
24-11-2011	9	Nouha Oualha	updated module description for ID privacy and authentication and access control subsystems
08-02-2012	10	Nouha Oualha	added ToC for chapter 3
23-02-2012	11	Markus Wehner	added draft technical description for secure routing/packet forwarding modules
23-02-2012	12	Nouha Oualha	added brief description to the authentication and access control and ID privacy subsystems
08-03-2012	13	Markus Wehner	refined chapter 3 SR and PF modules
26-03-2012	14	Markus Wehner	minor changes to SRP and PF
30-03-2012	15	Nouha Oualha	draft version of D3.2.1
09-04-2012	16	Laura Gheorghe	document review
13-04-2012	17	Nouha Oualha	Final version of D3.2.1
25-01-2013	0.2	Nouha Oualha	ToC for D3.2.2 based on D3.2.1's materials
21-02-2013	0.3	Markus Wehner	updated SRP and PF modules
07-03-2013	0.4	Markus Wehner	Updated SRP and PF; added

			figures; updated list of authors
10-03-2013	0.5	Nouha Oualha	Updated ID privacy module and integration of authentication module
11-03-2013	0.6	Nouha Oualha	Updated NAC module
18-03-2013	0.7	Nouha Oualha	Protocol implementation of grouped authentication and re-authentication
19-03-2013	0.8	Nouha Oualha	Added numerical analysis for grouped authentication
29-03.2013	0.9	Laura Gheorghe, Silvia Stegaru, Emil Slusanschi	Entire document review.
04-04-2013	0.10	Nouha Oualha	Addressed reviewers' comments
09-04-2013	0.11	Markus Wehner	update SRP/PF based on review comments
09.04.2013	0.12	Nouha Oualha	Revised introduction and conclusion chapters
10.04.2013	2.0	Nouha Oualha	Edited final version

Abstract:

Over the past years, the deployment of sensor networks into industrial environments attracted a lot of business domains. Therefore, an increasing number of applications are developed, ranging from defence and public security, to energy management, traffic control and health care. Sensor networks are particularly interesting due to their ability to control and monitor physical environments. Nevertheless, several technical (e.g. remote management, deployment) and security-related (e.g. user's privacy, data confidentiality and reliability) challenges deter that integration. The TWISNet (Trustworthy Wireless Industrial Sensor Networks) project aims at supporting and securing the integration of sensor networks into large scale industrial environments.

The present deliverable focuses on designing a framework for identity management, authentication and access control in industrial Wireless Sensor Networks. In such a framework, sensor nodes acquire pseudonymous identifiers to hide their real identity. Based on this identity model, nodes should still be able to authenticate and access the network, while supporting node mobility. After gaining access to the network, routing and packet forwarding decisions should be performed in a secure and energy-efficient manner.

To build such a framework, the state of the art of solutions and techniques from literature works, collaborative projects, existing standards and available commercial products is first reviewed. From this state of the art study, the security modules for the identity management framework are identified, specifically ID randomization and resolution, authentication, network access control, mobility management, secure routing and packet forwarding modules. Then, an architecture describing these security modules and their connections is presented. Finally, a detailed technical description of tasks, actions and protocols is provided for each of the security modules.

Keyword list:

Security, privacy, pseudonymity, authentication, network access control, mobility management, routing, packet forwarding

TABLE OF CONTENTS

List of Abbreviations *8*
1. Introduction *9*
2. State of the art *10*
2.1 Research literature **10**
2.1.1 Private identities 10
2.1.2 Authentication and access control 12
2.2 Collaborative projects **15**
2.2.1 Private identities 15
2.2.2 Authentication and access control 16
2.3 Standards **16**
2.3.1 Private identities 16
2.3.2 Authentication and access control 17
2.4 Commercial products **18**
2.4.1 Private identities 18
2.4.2 Authentication and access control 18
2.5 Summary **19**
3. Architecture *20*
3.1 Overview **20**
3.2 Presentation **20**
3.3 Modules Description **20**
3.3.1 ID privacy 22
3.3.2 Authentication and access control 20
3.3.3 Secure routing 22
4. Modules Technical Description *24*
4.1 Authentication and access control **24**
4.1.1 Authentication 24
4.1.2 Key diversification 26
4.1.3 Network access control 27
4.1.4 Re-authentication 28
4.2 ID privacy **31**
4.2.1 ID randomization/resolution 31
4.3 Secure routing **35**

4.3.1 Modules 35
4.3.2 Secure routing protocol 36
4.3.3 Packet forwarding 40
5. Conclusion 43
6. Acknowledgement 44
7. References 45

LIST OF ABBREVIATIONS

6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AAA	Authentication Authorization Accounting
AC	Access Control
AES	Advanced Encryption Standard
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LANs
FP6/FP7	Sixth/Seventh Framework Program
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
MAC	Medium Access Control; Message Authentication Code
PANA	Protocol for Carrying Authentication for Network Access
PSK	Pre-Shared Key
QoS	Quality of Service
RFC	Request For Comments
RPL	IPv6 Routing Protocol for Low power and Lossy Networks
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TWISNet	Trustworthy Wireless Industrial Sensor Networks
UDP	User Datagram Protocol
WSN	Wireless Sensor Network

1. INTRODUCTION

This deliverable is produced within task 3.2. It addresses the design of security services related to identity management, authentication, and network access control where security is not the only design factor, as performance and particularly energy efficiency are to be taken into great consideration.

The starting point is a review of existing solutions and techniques with respect to efforts in the research literature, collaborative projects results, existing standards, and available commercial products, presented in chapter 2.

Chapter 3 describes the architecture with a set of modules that compose the addressed framework, which are: ID randomization and resolution, authentication, network access control, mobility management, secure routing and packet forwarding modules. The architecture shows the interactions between the identified modules within the TWISNet framework and other modules from the framework.

A detailed description of these security modules is given in chapter 4. In particular, the actions and tasks achieved by each module are specified, along with the protocol and technologies to be used to realize them.

2. STATE OF THE ART

This chapter reviews existing solutions that provide privacy, authentication and network access control in an industrial Wireless Sensor Network. It organizes the reviewed security solutions into those derived from research literature works, collaborative projects results, existing standards, and commercial products.

2.1 Research literature

2.1.1 Private identities

2.1.1.1 Pseudonymity

Privacy protection for WSNs may arise beyond data content and may focus on context information such as sensor ID and its location.

Several solutions aiming at hiding sensor ID have been proposed in the literature. A naive solution consists in encrypting sensor IDs with pair-wise keys shared between communicating sensors. This solution prevents the disclosure of sensor IDs; but, it incurs costs to sensors with respect to their CPU usage since each intermediary sensor must decrypt and then re-encrypt ID information. Moreover, data transmissions experience longer delays.

To ensure concealment of sensor ID, several solutions suggest using pseudonymous IDs. Sensor pseudonyms should be frequently changed; otherwise, an attacker can infer the true ID behind a pseudonym by linking location and/or time information to the static pseudonym.

The authors of [23] have proposed the Simple Anonymity Scheme (SAS) where sensors draw their pseudonyms from contiguous ranges of pseudonyms pre-assigned to them before deployment. After deployment, each sensor associates each pseudonym range with one of its neighbors. Whenever, the sensor wants to send a message to its neighbor, it uses a random pseudonym from the appropriate range.

The authors have also proposed a second anonymity scheme called the Cryptographic Anonymity Scheme (CAS) [24]. In this scheme, sensors securely share the information related to a keyed hash function used to generate pseudonyms. When compared to the SAS, the CAS is more computationally expensive in exchange for memory efficiency.

In [2], two methods based on one-way hash chains have been described to dynamically change sensor IDs. The second method uses the chain in the reverse order. The advantage of these methods over CAS [24] is that, if the keys are compromised, the attacker cannot reveal the old pseudonyms. For the second method, it cannot impersonate the sensor, neither.

The proposed solution in [25] has the particularity to counter Sybil attacks where a sensor makes use of multiple identities to launch attacks. The solution relies on a certification authority (CA) only to bootstrap a domain of identities for sensors. Then, sensors can issue by themselves multiple self-certified pseudonyms, based on CA's certificates. This solution is suitable to be deployed in a Wireless Sensor Network in an infrastructureless mode where sensors communicate only with each other.

Even with frequently changing pseudonyms, attackers can correlate different pseudonyms of a given mobile sensor based on mobility patterns. To reduce the effectiveness of such correlations, silent periods [26] can be introduced, whereby sensors intentionally do not transmit between different sessions.

Alternatively, as a spatial version to silent periods, mix zones [27] reduce correlations between two pseudonyms of a mobile sensor. A mix zone is a spatial region, in which sensors do not transmit. When an attacker detects a mobile sensor entering a mix zone, it cannot distinguish this sensor from any other sensors emerging from the mix zone.

2.1.1.2 Anonymization techniques

Privacy can be protected through the use of anonymization techniques. Anonymization should be assured at the communication layer for providing protection against traffic analysis.

Wadaa et al. propose a dynamic virtual infrastructure for sensor networks and an energy-efficient protocol that assures the anonymity of the infrastructure [1]. The protocol provides structure anonymity, which refers to the anonymity of any network communications or infrastructure operations, which can be observed from the exterior of the network. The authors propose an efficient scheme for managing the anonymity of the coordinate system, cluster and routing structures while the network is in the setup phase. The sensor nodes obtain information about the virtual infrastructure in a secure manner and the sensor nodes remain silent during network setup in order to minimize communication.

Ouyang et al. developed two methods to provide anonymity through one-way hash chain that is used to change the identity of sensor nodes dynamically [2]. The two schemes are Hashing-based ID Randomization (HIR) and Reverse Hashing-based ID Randomization (RHIR). In HIR, each sensor node uses one-way keyed hash chain to produce its ID. In RHIR the IDs are assigned backwards from the end of the chain to the beginning, in order to improve the security of the scheme. The scheme is able to provide anonymity even in the case when the shared secret keys are obtained by an attacker.

Mitseva et al. propose privacy protection mechanisms for hybrid hierarchical WSNs [3]. Their contributions are context aware privacy protection mechanisms and trust establishment mechanisms for hybrid hierarchical architectures. The anonymity of level 2 nodes is protected using the context mix concept. This context mix concept provides anonymity through the change of identifying information in specific situations.

Sheu et al. designed an Anonymous Path Routing (APR) protocol for sensor networks, in which data is encrypted using pair-wise keys and kept anonymous between neighbour nodes, and between source and destination nodes in multi-hop environments [4]. APR includes three anonymization schemes: anonymous one-hop communication, anonymous multi-hop path routing and anonymous data forwarding. In the anonymous one-hop communication, each node generates two identities for each link with a neighbour. The anonymous multi-hop path routing finds a two-way path in an anonymous way and assigns a pseudonym to this path, the PathID. The anonymous data forwarding uses the PathID in order to forward packets anonymously.

SHALON is a lightweight anonymization technique based on open standards developed by Panchenko et al. [5]. The technique is based on onion routing and tries to reduce complexity while achieving high bandwidth. The fact that is based on standardized protocols makes Shalon easier to understand, develop and deploy. Shalon uses out-of-the box nested TLS connections to establish anonymous communications on top of HTTP/SSL suite.

Zhang et al. designed a Secure Anonymous Path Routing Protocol for WSNs that provides routing anonymity, location privacy, source and destination identity confidentiality and provides backward and forward security [6]. The protocol has been designed with reduced computational complexity in order to be appropriate for sensor networks. For this reason, a symmetric key is used instead of asymmetric keys and the modular exponentiation operation is replaced with the exclusive OR operation.

Buttyan and Holcze propose a private aggregator node election protocol, a private data aggregation protocol and a private query protocol, which protect the identity of the aggregators from external malicious nodes or compromised nodes [7]. In the election protocol, each node takes the local decision whether to become an aggregator based a probabilistic method. After that, through an anonymous veto protocol, the other nodes learn about the existence of at least one aggregator in the cluster, but they do not know its identity. This measure of safety protects the aggregator nodes against the compromised nodes.

The aggregation protocol uses a specific broadcast communication scheme, in which the cluster nodes form a ring and the packets go around the ring and are aggregated by the aggregator nodes. The query protocol responds to queries from the base station without revealing the identity of the aggregator nodes: a query token goes around the ring and each non-aggregator node adds some noise and the aggregator nodes adds noise and the data result. The base station knows how to obtain only the data from the token.

2.1.2 Authentication and access control

2.1.2.1 Authentication mechanisms

In WSNs, authentication schemes are generally based on simple symmetric cryptographic primitives to be suitable for sensor networks with low computational resources. Schemes have been proposed for authentication that takes place between a sensor node and a mobile agent or between two neighboring sensor nodes.

The authentication scheme may rely on a centralized trusted authority, similar to Kerberos. As proposed in [28], the authentication scheme allows the mutual authentication between a mobile user agent and a sensor node. The scheme adopts the Kerberos-like protocol; however, it does not require synchronization. Instead, the scheme depends on the internal clock counter at the sensor node. Additionally, the scheme provides privacy protection, since user identity is not exposed, based on a hash function and a fresh random number.

For authentication between sensor nodes, the protocol in [29] allows nodes to authenticate to their neighbors based on challenge-response tuples that are pre-calculated beforehand with a key that is later erased. It uses a key hash chain for authentication of nodes like in TESLA (version adapted to WSNs [38]); but, it does not require time synchronization between nodes. The scheme is based on cheap computation operations (hash functions, symmetric encryption) and requires storage space proportional to the number of nodes. The proposed protocol is therefore designed for poorly dense networks and static or quasi-static scenarios.

2.1.2.2 Mobility-support for authentication

When a sensor node moves from a given position where it has already authenticated to the network to another new position, it should perform again an authentication procedure in order to get access to the network. Generally, the authentication procedure caused by user mobility is called re-authentication.

The Proactive Key Distribution (PKD) approach proposed in [49] to render re-authentication fast within IEEE 802.11i authentication framework introduces a data structure, named

Neighbor Graph, which dynamically tracks the potential APs, to which a station may handoff to. In the PKD approach, the AAA server and the potential AP establish pairwise master keys (PMKs) before the re-association. This approach is enhanced in [50] using IEEE Inter-Access Point Protocol (IAPP) [72] context transfer in order to perform a pre-distribution of pairwise transient keys (PTKs). The station will use these keys to temporarily re-associate with a target AP. After that, the station engages immediately a PKD authentication with its new access point, while continuing its data transmission. The pre-distributed PTK keys are computed by the serving AP and sent to the target AP. To remediate this security issue, the PKD approach is further enhanced with a ticket-based approach, whereby the station generates by itself the PTK keys and securely sends them to the target AP through the serving AP. This enhancement does not introduce very much of signalling overhead compared to the PKD pre-authentication approach, while ensuring the conformance with the IEEE 802.11i security requirements.

The paper [51] proposes a ticket-based approach (similar to Kerberos) that allows the fast re-authentication of a mobile node with its target access network. The mobile node creates a ticket containing a protected master key that will be shared with the target access router. The ticket will be sent through a handover notification message to the current access router and will be forwarded proactively by this latter to the target access router. The mobile node re-authenticates with the target access router by proving knowledge of the ticket's content. The proposed approach defines an additional RADIUS attribute and uses the optional data field of EAP-Identity-Messages.

The authors of [46] propose another ticket-based fast authentication protocol, with which network clients authenticate simply to mesh access points without involving the authentication server. The protocol uses a type of tickets called "transfer tickets" generated by one of the mesh access points to some client that dispenses that client from re-authenticating to a new mesh access point. By avoiding multi-hop authentication, the re-authentication protocol is faster and even has been demonstrated to be outperforming the EAP-TLS protocol of IEEE 802.11s. The protocol relies on the assumption that the authenticators are static nodes and share pair-wise keys with each other. These keys are used to secure the transmission of security information for ticket validation.

The authors of [47] propose to use membership verification for re-authentication. Based on the BGN homomorphic encryption scheme [48], verification of membership is handed out to cluster heads without revealing the secret information shared by the service provider. Even though, the approach provides mutual authentication and non-linkability between user sessions, it is computationally expensive from the cluster head side (exponential operations for large number of sensor nodes).

Mobile nodes may migrate into foreign domains. In the absence of a single authentication server, it is a challenge to provide re-authentication of mobile nodes in a multi-domain context.

The Efficient Mobile Authentication (EMAS) scheme proposed in [53] is based on a trust delegation approach as in [54] where a mobile station (MS) registered to a home location register (HLR) proves its registration to a visited location register (VLR). The scheme does not assume honest VLR compared to [54]. The MS shares a secret with its HLR that is used to prove its registration to the HLR. The MS sends a signed message to the VLR that can be verified based on a public certificate published by the HLR. Then, the VLR requests a communication key from the HLR after being authenticated to it. Off-line authentication can be provided if the HLR sends some information (i.e. tokens) to both, the MS and the VLR, before leaving. The EMAS scheme is efficient since it reduces the number of exchanged messages, but it does not support the authentication of the VLR by MSs.

The protocol proposed in [52] is a security protocol that allows mutual authentication between a mobile user and a foreign network server using a self-verified token generated by its home network server; thus, avoiding DoS and deposit attacks. The protocol is based on elliptic curve cryptography and endeavours to shift most of computation operations from the mobile user side.

2.1.2.3 Access control techniques

In WSNs, it is critical to restrict the network access only to eligible sensors, while messages from unauthorized nodes will not be forwarded. Otherwise, the network may be vulnerable to DoS attacks that aim to deplete the resources of sensor devices.

In the secure network access system in [30], nodes establish pair-wise keys using a self-certified Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol. The protocol is supplemented with a polynomial-based weak authentication scheme in order to mitigate DoS attacks. Network access maintenance is provided using Subset Difference Method (SDM) that allows the controller node to update the group key using a small subset of keys that cover the eligible nodes. The method is stateless since a node is able to decrypt future group keys even if it misses the current round of key update packets. It may even recover the current key without waiting the next round. The group key update method is further customized using Merkle hash trees for packet construction and one-way key chains organizing network access control keys.

Network access schemes have been proposed at lower layers. For instance, the LHAP hop-by-hop authentication protocol [31] resides between the network layer and the data link layer, which makes the protocol transparent and independent of the used routing protocol. With LHAP, a node joining the network needs to perform first TESLA localized broadcast operations to bootstrap trust relationship with its neighbors; though digital signatures are required to bootstrap a TESLA key chain. Then, the node switches to one-way key chains for traffic authentication. The protocol assumes loose time synchronization between all nodes, since it relies on TESLA.

The Lightweight Inter-layer Protocol (LIP) [32] is another hop-by-hop authentication protocol for network access control that relies like LHAP on local broadcast authentication. In LIP, nodes share cluster keys with their immediate neighbors. To avoid impersonation attacks, the protocol is used with other three techniques: one-time-cluster key, random neighborship, and neighborship estimation. The one-time cluster key technique is provided with one-way key chains. Impersonation attacks are thwarted by the triangular inequality of transmissions, if the sender is still in the transmission range of the receiver. In the second technique, the receiver verifies the authenticity of the received message with certain probability, using the pair-wise key shared between the sender and the receiver. In the third technique, verification is not performed randomly, but rather based on the knowledge of neighbors' locations.

The responsibility of access control can be delegated to a coalition of nodes close to the new comer. In [33], a threshold number of them enable the new comer and its intermediary neighbor to authenticate to each other and at the same time compute a shared symmetric key. The proposed scheme is based on Shamir's secret sharing. Since, polynomials are considered to be a lightweight class of functions, the scheme achieves low computation complexity. Communication usage is relatively high, because several nodes are involved in the authentication communication process, whereby a request packet is broadcasted and then multiple response packets are received in unicast. Moreover, the proposed protocol assumes that the network is already bootstrapped with an alternative authentication scheme.

2.2 Collaborative projects

2.2.1 Private identities

2.2.1.1 Pseudonymity

The Pseudonymization of Information for Privacy in e-Health (PIPE) project developed a system for the pseudonymization of health information, which securely integrates primary and secondary usage of the data [8]. It is based on an innovative concept for data sharing, data recovery and authorization in health care [9]. Data recovery mechanism allows the recovery of access to data when the security tokens with the keys are lost or stolen [10]. The patients are in full control of their data and who can access it; therefore, their privacy is assured.

Future of Identity in the Information Society (FIDIS) is a NoE (Network of Excellence) supported by the European Union under the 6th Framework Programme for Research and Technological Development within the Information Society Technologies (IST) priority in the Action Line: “Towards a global dependability and security framework”. FIDIS has been finalized in 2009 and provides research results regarding virtual identities [11].Virtual identities are used to provide pseudonymity and anonymity and have many use cases, from security to entertainment. The pseudonym represents the identity of the virtual person. In the case when a virtual person can be associated with a physical person, the pseudonym is the virtual identity of that physical person. When the virtual person cannot be associated with the physical person, the pseudonym provides anonymity for that physical person.

2.2.1.2 Anonymization techniques

The Phantom Project [34] aims at decentralized anonymization of network traffic. The protocol consists of three different parts. The first part is related to routing paths: exit paths for outgoing connections into the network, and entry paths that are used to accept incoming connections from the network. Routing paths consist of nodes connected to each other with SSL-connections. There are two types of nodes participating in routing paths: those that are used to help in path construction and those that will be added to the actual path. The second part of the protocol concerns the routing tunnels that are initiated by the owner of an exit path. Its request will be sent until the exit node that will try to connect to the entry node owned by the destination node. The third part that renders the protocol completely decentralized consists of a distributed hash table containing various information, in particular, a mapping that makes it possible to get the entry nodes for an AP-address and information describing other Phantom nodes (IP-addresses, ports along with their certificates).

The Invisible Internet Project (I2P) [35] is a peer-to-peer distributed communication layer network that applications can use to anonymously and securely send messages to each other. I2P is based on Layered-encrypted tunnels. Another layer of end-to-end encryption is required. Messages can be sent only in one way using outbound tunnels. To send messages back, an inbound tunnel is required. Each tunnel consists of a selected list of routers that has been made available by a network database (netDb). These routers are selected based on their behavior (e.g., latency, capacity, reliability to failures), that is constantly profiled by I2P. NetDB relies on a set of I2P routers that are organized based on the Kademlia algorithm to share network metadata, such as the information necessary for contacting a particular router or a particular destination. I2P is an unreliable-unordered-message based system, since it is an UDP-based transport system; even if it uses Secure Semi-reliable UDP (SSU).

I2P operates in a similar manner to the Phantom project. Like the Phantom project being intended for peer-to-peer networks, anonymity in I2P incurs large overhead for the network, routers and end-to-end nodes.

2.2.2 Authentication and access control

2.2.2.1 Authentication mechanisms

Ubiquitous Sensing and Security in the European Homeland (UbiSec&Sens) is a Specific Target Research Project (STReP) completed in 2008 in the thematic priority “Towards a global dependability and security framework” of the EU Framework Programme 6 for Research and Development. UbiSec&Sens develops an architecture for medium and large scale WSNs that are secure and trusted for all applications [12]. The project provides a complete security toolbox and includes efficient authentication protocols. The designed protocols are specific to certain applications and then develop a universal solution by combining the different schemes. They also investigate the possibility of data aggregation when using Message Authentication Codes (MAC) [13].

Automated VAlidatioN of Trust and Security of Service-oriented Architectures (AVANTSSAR) is a FP7 STREP project that has been completed in 2010 and worked on developing the AVANTSSAR Validation Platform [14]. This platform is an automated toolset that can be used to validate security and trust for service-oriented architectures. The project has also produced a library of validated composed services and service architectures. AVISPA tool is used for the examination of the SIP authentication method [15].

Secure Embedded Platform with advanced Process Isolation and Anonymity capabilities (SEPIA) is a Research and Development project ending in 2013 co-financed by the European Commission through the 7th framework programme. SEPIA works on the development of secure mobile and embedded computing systems [16]. The project aims to secure mobile platforms and develop cryptography and privacy technologies. Therefore, its purpose is to define the next-generation security architecture for mobile and embedded systems. It has been developed a Lightweight Anonymous Authentication using TLS and DAA for Embedded Mobile Devices [17] that provides device authentication against the collusions generated by a malicious service. Also, it has been designed an Anonymous Client Authentication for TLS that allows the establishment of anonymous authentication using secure channels [18].

2.3 Standards

2.3.1 Private identities

2.3.1.1 Pseudonymity

The IETF RFC 4941 [43] on Privacy Extensions for Stateless Address Auto-configuration in IPv6 defines a mechanism that allows a node to "create additional addresses based on a random interface identifier". This mechanism guarantees the quasi-randomness of the newly created temporary addresses. Temporary addresses have a certain lifetime: a new one has to be created and used for new connections after the former expires. An expired temporary address will still be used to exchange data as part of a pre-existing connection. The frequency at which temporary addresses change depends on how often the RFC4941-compliant device initiates connections. A default value of 1-day is suggested. A notable impact on the bootstrapping procedure is the following: a (quasi-)random value must be generated upon node bootstrapping, which may require fair randomness generation property on sensor nodes.

The section 12 of IETF RFC 3315 [44] on Dynamic Host Configuration Protocol for IPv6 (DHCPv6) defines a mechanism for the "Management of Temporary Addresses" by which a client may request the assignment of a temporary address. This mechanism may be used for location privacy purpose.

The use of 5.9 GHz DSRC (5GHz: Dedicated Short Range Communication) technology for CALM (Continuous Air interface for Long and Medium distance) is said in [45] to provide a location privacy for anti-tracking protection system, based on MAC address randomization. Cross-layer synchronization of the anonymization system is suggested by the mention that "security certificates may also be periodically changed".

2.3.1.2 Anonymization techniques

IP Flow Anonymization Support is an IETF RFC 6235 that presents techniques for anonymizing the fields of IP flow data and the parameters required for each anonymization technique [19]. The techniques for IP Address anonymization are: Truncation, Reverse Truncation, Permutation and Prefix-preserving Pseudonymization; for MAC Address anonymization are: Truncation, Reverse Truncation, Permutation and Structured Pseudonymization; for Timestamp anonymization: Precision Degradation, Enumeration, and Random Shifts; for Counter anonymization: Precision Degradation, Binning, and Random noise addition and the anonymization of Other Flow Fields: Binning and Permutation.

2.3.2 Authentication and access control

2.3.2.1 Authentication mechanisms

Standards like ZigBee and Bluetooth use symmetric encryption for authentication. In the Mutual Entity Authentication (MEA) protocol of ZigBee 2007 [36], an initiator two nodes mutually authenticate each other based on a secret key (NK). The devices authenticate each other by using random challenges with responses based on a NK.

The mutual authentication mechanism used by Bluetooth [37] relies on the exchange of random numbers as challenges and their encryption with SAFER+ (E1) using the unit key shared beforehand. The random numbers and addresses are exchanged in plaintext.

2.3.2.2 Mobility-support for authentication

The IETF RFC 5836 [41] on EAP Early authentication aims at making EAP client's re-authentication quicker upon roaming from one access point to another. Horizontal context transfer is quickly reviewed, and discarded for security reasons. Vertical handover is considered interesting, and studied in detail. Three early authentication models are detailed, in which a Mobile Device (MD) initiates authentication to a Candidate Attachment Point (CAP) while still attached at a given Serving Attachment Point (SAP):

- Direct pre-authentication model: direct authentication between MD and CAP through SAP. MD⇔CAP⇔Server
- Indirect pre-authentication model: communication occurs between MD and SAP, because direct communication between MD and CAP is not possible. MD⇔SAP⇔CAP⇔Server.
- Authenticated anticipatory model: there is no trust relationship between SAP and CAP, and pre-authentication traffic has to go through the EAP server. MD⇔SAP⇔Server⇔CAP.

The IETF RFC 5873 [42] on PANA pre-authentication support defines extensions to the PANA protocol to carry EAP messages related to pre-authentication. It is supposed to work in the direct pre-authentication model as defined in RFC 5836 and therefore describes exchanges between the PANA client and a candidate PANA authentication agent.

2.4 Commercial products

2.4.1 Private identities

2.4.1.1 Pseudonymity

Nym is a product that can offer practical Pseudonymity for Anonymous Networks [20]. It allows pseuodonymous access to Internet services through anonymizing networks such as Tor. The application builds a peseudonymity system based on blind signatures. The client uses a browser-based application to obtain the blind token through a TLS client certificate. The pseudonymous credential system has been developed to be used without an infrastructure from the government or industry. The application can be efficiently used to provide privacy protection for clients and abuse resistance for servers.

2.4.1.2 Anonymization techniques

Tor [39] is “a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet”. TOR operates in an overlay network of onion routers that employ encryption in a multi-layered manner. Each node periodically negotiates a virtual circuit through the Tor network. Tor does not protect against monitoring of traffic at the boundaries of the Tor network. Besides, Tor has not been yet adapted to the WSN context.

On the Internet, Anonymizer [40] allows surfing users to connect to the Anonymizer system through VPN and replace their IP address with new non-attributable ones. The system provides robust anonymity thanks to a secure IP rotating technology. The system provides also anonymous activities over wireless connections. The web site of the system does not give very much information about how the system works in this case; but clearly connections are redirected through VPN to replace IP addresses with anonymous ones.

2.4.2 Authentication and access control

2.4.2.1 Authentication mechanisms

The ultra low-power Atmel ATSHA204 is the first authentication device that contains a 4.5 Kbit EEPROM for secure storage and a hardware SHA-256 accelerator for the crypto algorithm [21]. The device is a member of Atmel CryptoAuthentication™ family and has optimized hardware security features that allow the authentication of objects, control the OEM supply chain, prevent software piracy and protect sensitive data. The product has the ability to generate, store and transfer secret keys in a secure manner and uses 256-bit keys for enhanced security. It allows the application developer to implement authentication check without cryptography knowledge. The device also includes a high-quality random number generator, which can be used in anti-replay mechanisms.

MAXQ1004 is a low-power 16-bit microcontroller that provides secure authentication to applications [22]. The microcontroller integrates a true random-number generator (RNG) and a high-speed AES encryption engine that uses keys of 128, 192 and 256 bits. It provides resistance against analytical and cryptanalysis attacks. It enables secure authentication that is used for protecting revenue streams, validating peripherals and implementing secure communication schemes. Other feature is that it consumes only 300nA in the lowest power

stop mode. The MAXQ1004 with 0.1 duty cycle will consume a 64mAh battery in 1.8 years and with 0.01 duty cycle in 10 years.

2.5 Summary

To protect the privacy of sensor nodes, their identity is the foremost element that should be hided. Each sensor node should use a pseudonym instead of its real identity. It should also frequently change such pseudonym to avoid being tracked. In this sense, several pseudonym-based approaches with a resolution mechanism, relying on computation or storage resources, have been proposed particularly in the literature. Even though, in these approaches, the use of pseudonyms may concern some specific layer sensor ID (e.g., IP or MAC addresses), it should be applied at all layers and cross-layer synchronization should be supported. Even security certificates should be periodically changed as suggested by CALM.

Anonymization mechanisms can be used to provide traffic privacy and protect against attacks. Several solutions that provide anonymity are described in the research literature and collaborative projects. Most of the described solutions for anonymization techniques are generally intended for the Internet and incur huge overhead in the network, which makes them difficult to be efficiently applied into the context of Wireless Sensor Networks.

Before gaining access to the network, sensor nodes are authenticated. The protocols that have been proposed in the context of Wireless Sensor Networks use low computation schemes like symmetric cryptographic schemes a la Kerberos or TESLA-inspired hash chains. Authentication is generally provided end-to-end between the node and the authentication server. On the other hand, network access control techniques allow the hop-by-hop authentication of sensor nodes in the network. In the literature, the majority of these techniques rely on lower layers; which make them transparent to the used routing protocol. Nodes agree on pair-wise keys based on these techniques to establish security associations.

When a mobile sensor node that has authenticated to the network, moves to a different location, it needs to re-authenticate. To render re-authentication faster, security contexts (e.g., keys) generated by the current network or security tickets proactively computed by mobile nodes are transferred to the new network. Some approaches in the literature propose even to delegate the authentication process to cluster heads through the use of security tickets or by membership verification without involving the authentication server. Re-authentication through anticipation has been also applied to the EAP protocol and specified by IETF through different models depending on the trust relationships and connectivity between the mobile node, and the old and the new attachment points.

A suggested approach to the identity management framework is to focus on privacy protection through the use of frequently changing pseudonyms and their associated resolution mechanism. Authentication and access control mechanisms should support multi-hop communication and the mobility of nodes in single or multi-domain contexts through fast re-authentication mechanism. Within these different contexts, secure and fair routing and forwarding of packets are to be provided in an energy-efficient manner in the network.

3. ARCHITECTURE

This chapter gives an overview of the architecture that will be used in task 3.2. The architecture consists of modules grouped into subsystems and distributed within data or control planes. A short functional description of each one of these modules is provided also in this chapter.

3.1 Overview

Task 3.2 in TWISNet addresses the identity model, as well as the authentication and network access control procedures where TWISNet identifiers will be used. The use of pseudonyms is considered when devising the identity model to protect sensor privacy. Additionally, the authentication and access control procedures provide support for node mobility. The mobility aspect with energy efficiency focus is also handled when providing secure routing in the network.

3.2 Presentation

The proposed architecture for this task consists of a set of sensors, a Gateway, and a Trust Center. The architecture adopts a modular design by dividing the task into separately-designed modules. Each entity holds a set of modules as illustrated in Figure 1.

3.1 Modules Description

3.1.1 Authentication and access control

Authentication and access control are mandatory procedures in the four scenarios as described in D2.1 [55]. Both are needed whenever a device would like to access the network. These procedures assume that devices have the necessary credentials (e.g., keys, tokens) to authenticate and access the network. These credentials are obtained from the bootstrapping procedure. They should also take into account the dynamic virtual identities of devices.

The subsystem comprises three modules. The first one consists of the authentication of network devices by an authentication server. The second module considers controlling access of these devices to the network. Finally, the third module deals with the fast authentication of mobile devices that regularly attach to new PANs.

3.1.1.1 Authentication

This module is composed of a client module at the sensor side and a server counterpart at another sensor side or at the Trust Center side, which communicate with each other through the network. Even though, this module proposes a mutual authentication procedure at both sides, the client and the sever modules may not be implemented similarly. For example, the server module may additionally include distribution of keys for network access.

This module interacts with the key management module at each side to retrieve the required credentials. It also interacts with all modules in the ID privacy subsystem in order to handle the dynamic use of pseudonyms by sensors instead of their real identities.

3.1.1.2 Network access control

This module allows the authentication of a sensor to its one-hop neighbor. The module is composed of similar counterparts at both sensors.

This module interacts with the key management module for key retrieval by sensors, and all modules in the ID privacy subsystem in order to handle sensor pseudonymity. It may closely interact with the authentication server module to remotely retrieve the network access control keys.

3.1.1.3 Mobility management

This module is built as a complementary extension to the authentication module. It supports the fast re-authentication of mobile sensors. The module is relevant for scenario 1 “sensors attached to a person moving from PAN to PAN”, since sensors, as described in D2.1 [55], frequently re-authenticate to new PANs that do not share the same keys. The module is also recommended for scenario 3, “sensor networks for the monitoring and control of an industrial process”, that considers mobile devices. Remote provisioning of keys and the anonymization of sensors are key issues in this module.

The fast re-authentication may be triggered proactively from the Trust Center or from the sensor itself based on context transfer. The Trust Center may hold a database containing the positions of mobile sensors and the potential PANs to which they may attach.

As the previously described modules, this module interacts with the authentication module, the key management module and all modules in the ID privacy subsystem.

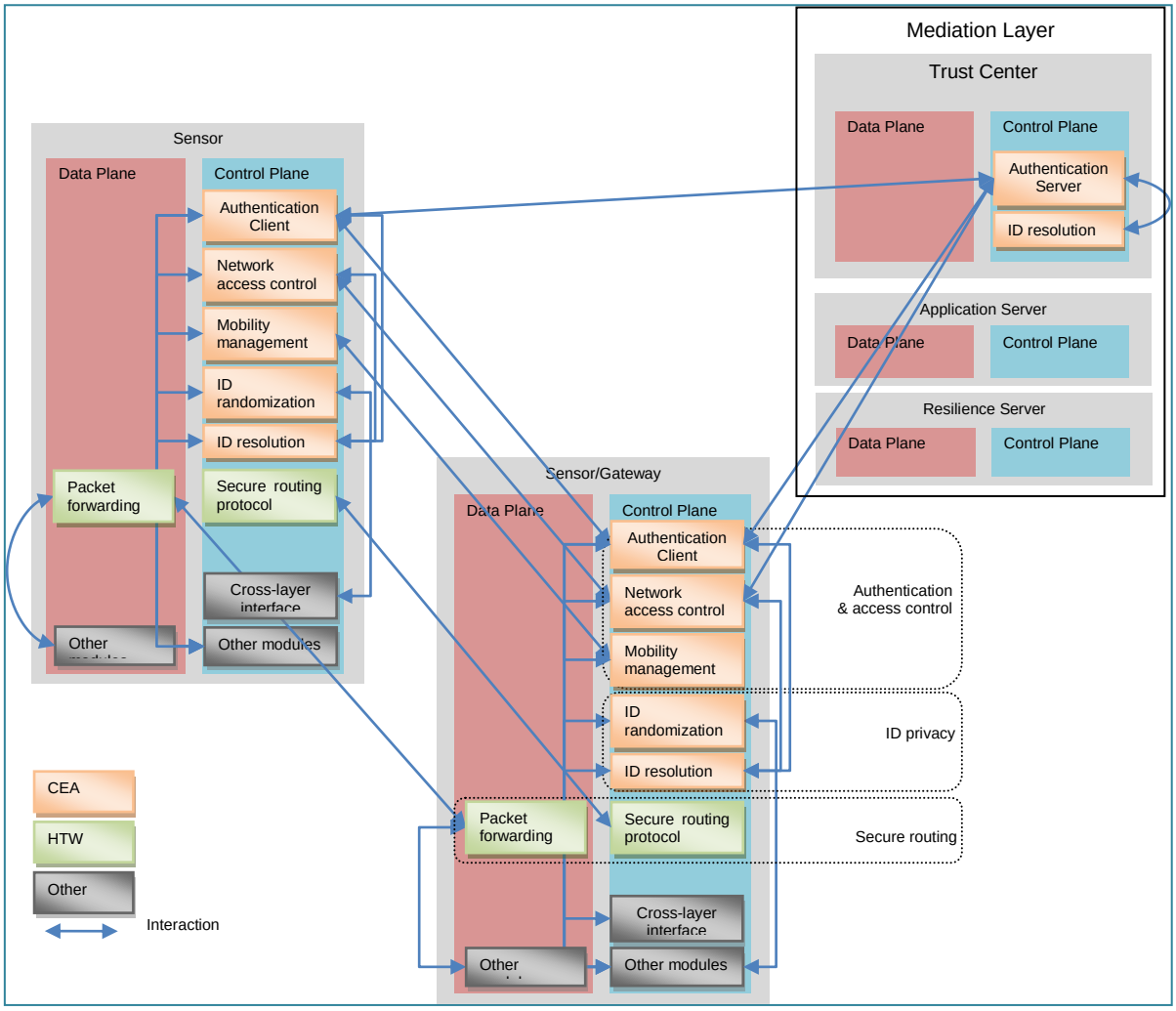


Figure 1. TWISNet architecture for task 3.2

3.1.2 ID privacy

To protect the privacy of sensors, the latter use randomly generated pseudonyms instead of their real identities. ID privacy modules are recommended for the four scenarios described in D2.1 [55]. The subsystem should operate at several layers, since ID randomization is needed not only for application addresses, but also for IP and MAC addresses.

This subsystem needs either security credentials or secret storage or both to enable the generation of new identities. It may have then to interact with the key management module. It also interacts with all modules in the authentication and access control subsystem.

The subsystem comprises there modules that have interactions with each other. Only the ID randomization and ID resolution modules are presented in this deliverable. The privacy manager module is described in D3.3.1.

3.1.2.1 ID randomization

This module allows the sensor to generate random pseudonyms as frequently as required. The module is recommended for scenarios 1, 2, and 3 described in D2.1 [55] where the data measured by sensors should be anonymized. The module uses security credentials (e.g., keys) to generate cryptographic pseudonyms or secure storage to retrieve pre-computed pseudonyms. These pseudonyms are used at multiple layers. Cross-layering interface is then needed for this module.

This module may interact with the key management module. It interacts with all modules in the authentication and access control subsystem and also all modules in the ID privacy subsystem.

3.1.2.2 ID resolution

This module is associated with the ID randomization module. It allows the sensor to resolve the received pseudonym and securely associate the pseudonym with the real sensor ID. It may use the same credentials or secure information as the ID randomization module. It may also use cross-layering capability; otherwise pseudonym resolution can be performed independently at each layer.

The module may interact with the key management module, and will clearly interact with all modules in the authentication and access control and ID privacy subsystems.

3.1.3 Secure routing

The secure routing subsystem is dedicated to energy-efficient, secure and fault-tolerant transport of data packets in the network including multi-owner systems. On the one hand, there is a need to establish a routing that especially fits the needs for energy efficiency, security and resilience, i.e. low latency in emergency situations, in any kind of network. Additionally, in a multi-owner network, the rights of various services to access the resources of the network need to be managed. Nodes from one service can route the packets of another with no direct benefit to services of the node routing the packet. Therefore, metrics have to be generated locally and over the network to allow decisions about optimal routing paths. Although the TWISNet framework is established between network layer and application layer, additional functionality has to be integrated with respect to the network layer. To separate functionality, two modules have been established as addons for an existing routing protocol. The Secure Routing Protocol (SRP) module is responsible with collecting routing relevant information and sending it to routing calculation instances. So this module may be quite independent of the used network stack and may be also used in conjunction with other routing protocols, e.g. RPL. The Packet Forwarding (PF) module is

responsible for calculation and establishment of the routes based on the information gathered by SRP and forwarding the packets on these routes. Using these two modules, the establishment of dedicated routes for certain services is provided.

3.1.3.1 Secure routing protocol

Using the Secure Routing Protocol, a local evaluation of routes to the neighbors shall be applied in terms of metrics as energy consumption and security. Therefore, links to the neighbors as well as local parameters of nodes are analyzed and sent to one or more routing calculating instances. The packet calculating instance, i.e. realized by the Packet Forwarding module, uses the metrics to calculate optimized routes. SRP is designed to work with other packet calculating instances, e.g. the routing calculation realized by the RPL protocol.

3.1.3.2 Packet forwarding

The Packet Forwarding module is responsible for performing packet forwarding towards the destination. Therefore, at routing calculation instances, routing decisions based on local evaluation by the Secure Routing Protocol module and, if available, further information (e.g. global evaluation based on the network access control and connection sharing modules) are calculated and propagated to the nodes. Establishment as well as maintenance of the routes is the main task of this module.

4. MODULES TECHNICAL DESCRIPTION

This chapter describes the technical solutions for the implementation of the modules proposed in task 3.2. The credentials (i.e., keys, security parameters) produced during authentication are used to enforce network access control module and provide privacy protection through ID randomization and resolution. Secure routing module in close relation to packet forwarding module, distributes locally-generated metrics of performance and security to make decisions on whether or not to forward packets.

4.1 Authentication and access control

This subsystem is concerned with authentication, re-authentication (due to mobility), and network access control procedures that are performed whenever a sensor node accesses the network. This subsystem is composed of three modules that interact with each other. Authentication should be provided not only for a static sensor node, but also when the node moves within the same PAN, or from PAN to PAN within the same administrative domain or even across different domains. The establishment of network access control enforcement points follows the authentication procedure and uses the credentials (e.g., pre-shared keys) provisioned after authentication.

4.1.1 Authentication

4.1.1.1 Tasks and actions

Since authentication is performed more often than bootstrapping, the resource constrains of the devices limit the choice of the authentication protocol, for instance, by favoring symmetric cryptography-based methods (e.g., EAP-PSK [57]) to asymmetric cryptographic ones (e.g., EAP-TLS [56]).

The authentication module allows a sensor node to gain access to the network. It should provide mutual authentication between the sensor node and the network. This module is mandatory for the four scenarios.

The authentication procedure occurs between the authenticating sensor node and the Trust Center i.e., the sensor node is the client side and the Trust Center is the server side.

Authentication may concern a large number of nodes at similar times (e.g., if nodes have the same mobility pattern, reaction to the same event). In this case, individual authentications could be regrouped into one authentication exchange, in order to avoid network congestion.

4.1.1.2 Protocol

The authentication is carried out for individual sensor nodes using the usual EAP authentication protocol. If a bulk of nodes require authentication at similar times, their authentication is combined in one exchange.

The Trust Center decides whether to perform simultaneous individual authentication of nodes or grouped authentication:

- **Individual authentication:** this procedure is the usual authentication procedure. Upon receiving multiple node authentication requests, the Trust Center can perform the authentication for each of these nodes simultaneously.
- **Grouped authentication:** if the Trust Center receives authentication requests from multiple nodes pertaining to the same group, it may aggregate their authentications in one exchange. On one side, one common challenge is broadcasted to sensor nodes in a multicast message using the group identity. On the other side, nodes answer to the

challenge and their responses are regrouped and sent back to the Trust Center. Aggregation of nodes' responses could be aggregated at routers (i.e., 6LoWPAN routers) back to the gateway. Even with aggregated responses, the Trust Center should be able to check nodes' responses in order to authenticate each of these nodes (refer to Figure 2 for an example of protocol implementation based on EAP-PSK). For instance, pollution attacks should be mitigated based on lower-layer encryption and limited aggregation. If group authentication is successful, the Trust Center provisions the gateway with necessary keying materials specific for each of the authenticated nodes from the group, in order to enable the network access control module. Otherwise, the Trust Center will initiate usual individual authentication procedure with each sensor node.

As for individual authentication, the mechanism of grouping multiple authentications of devices in one exchange can be applied for fast re-authentication (refer to subsection 4.1.4).

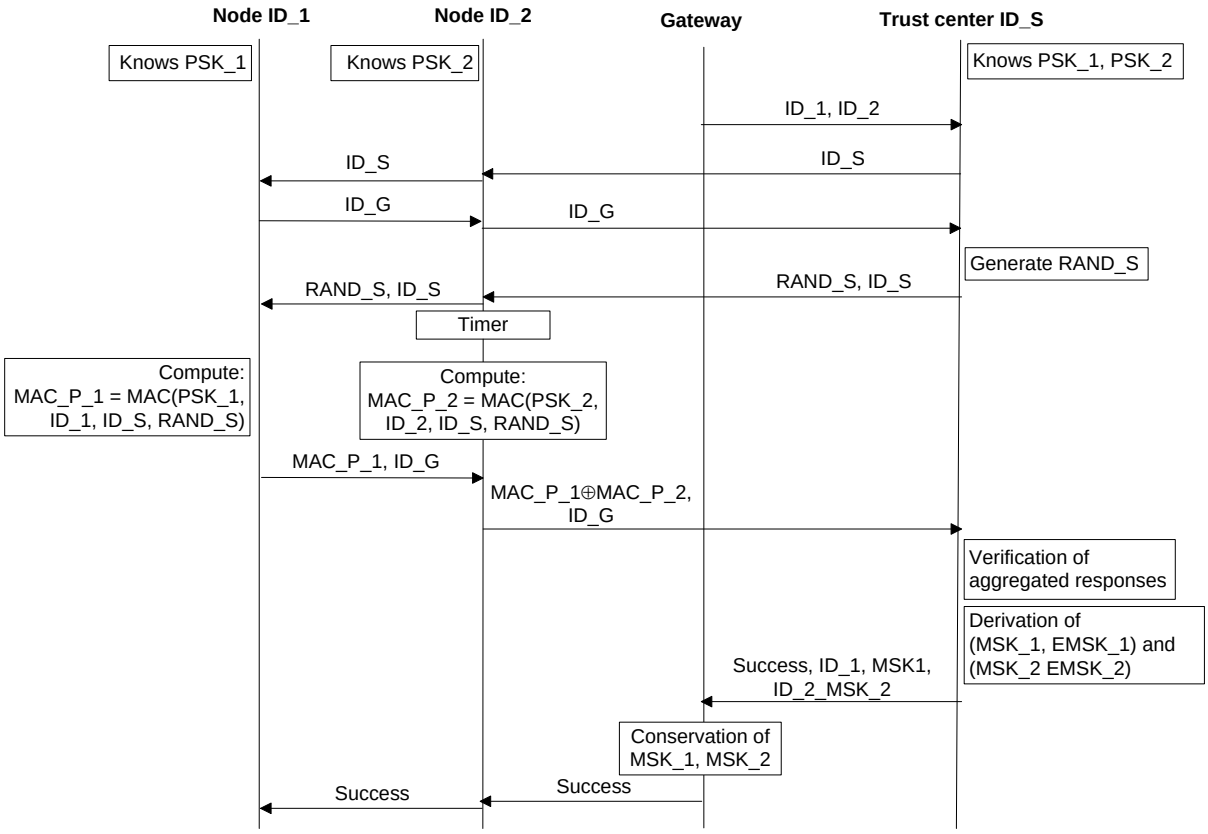
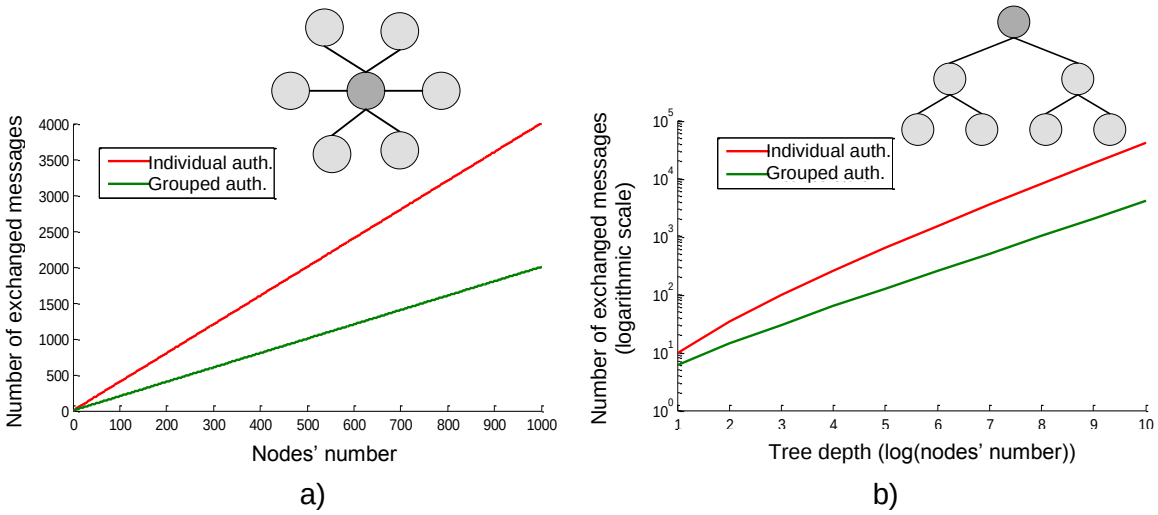


Figure 2. EAP-PSK based grouped authentication (2 nodes are authenticated simultaneously)

The aim of aggregating authentication operations of multiple nodes in one exchange is to reduce the number of messages exchanged during authentication. As illustrated in Figure 3, the number of exchanged messages during the grouped authentication is exponentially reduced compared to the traditional authentication when increasing the number of authenticating nodes. This result is obtained for two different network topologies (i.e. star and tree topologies). Reducing the number of exchanged messages allows improving battery life

at routing nodes since an aggregated (compact) message is routed instead of multiple messages, and moreover it avoids WSN congestion.



a) b)

Figure 3. Numerical analysis of the number of exchanged messages for authentication using traditional method and grouped method in two perfect network topologies: a) star topology and b) tree topology

If the sensor node cannot directly reach the Gateway because, for example, it may not have a configured global IP address yet, it relies on other nodes from the network to communicate with the Gateway. A node in the path to the authenticator may play the role of a PANA Relay Element (PRE) [59], in order to enable PANA messaging between the node and the Gateway. After a successful authentication, the authenticating node reconfigures its IP address with an address (Post-PANA Address) that is usable for exchanging messages through the enforcement points.

4.1.2 Key diversification

The base interaction between the authentication module and the other modules results from the keys used by these modules that are derived from the key bootstrapped after successful authentication. The TWISNet modules concerned with this kind of interaction are: the mediation layer (application), fast re-authentication, network access control, server-assisted key exchange (SAKE), and ID privacy modules.

The used protocols for authentication are based, for example, on the standard method EAP-PSK [57]. The pre-shared key used for authentication is bootstrapped at first during the device initial authentication based, for instance, on EAP-TLS [56]. Other types of keys used for re-authentication, network access control, ID privacy, server-assisted key exchange and application security are also derived. The key diversification process summarized in Figure 4 may employ, as example, the key derivation function proposed in [69].

After bootstrapping, a device derives a shared key with the Trust Center that is used as a pre-shared PSK key for subsequent authentication. After each authentication, a device derives a key shared with only the Trust Center (i.e., EMSK). This key is used to derive application keys (Application Master Session Key-AMSK), and also, as detailed in subsection 4.1.4, fast re-authentication keys within intra-domain and cross-domain settings (i.e., rRK,

pRK, nKGS). The EMSK key may be also used to derive ID privacy keys (detailed in subsection 4.2), along with server-assisted key exchange (SAKE) keys (i.e., PKs), as specified in D3.1.2 SAKE module. With the EMSK, the device derives a key (i.e., MSK) that is distributed to the Gateway. This key is used to derive keys (i.e., PEMK) to enforce network access control in the WSN.

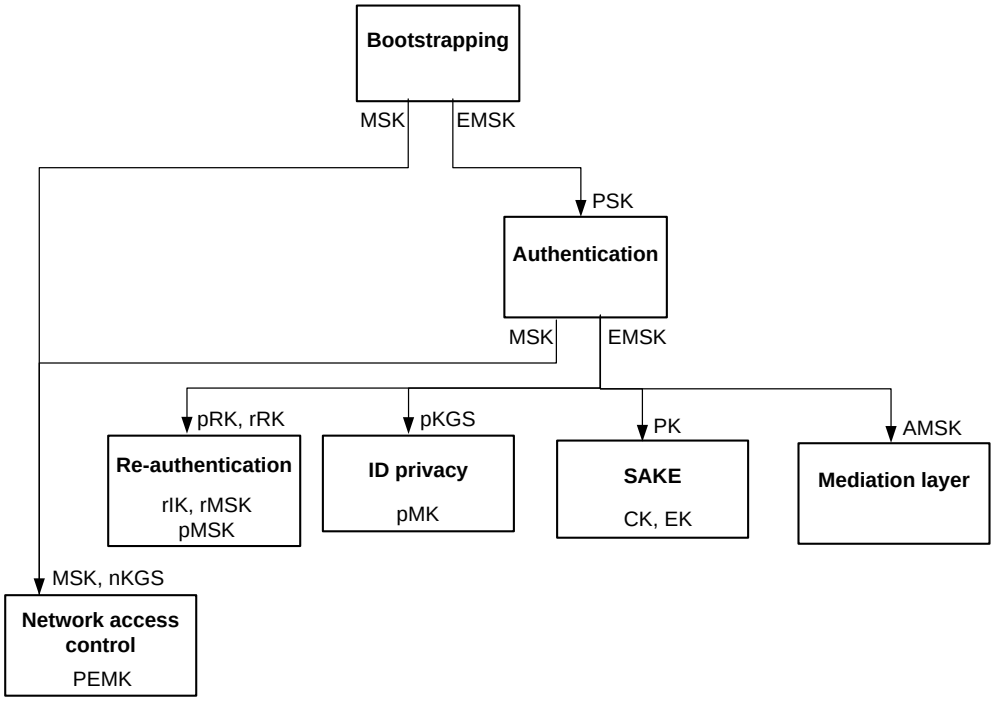


Figure 4. Key diversification in EAP-based protocols

4.1.3 Network access control

4.1.3.1 Tasks and actions

After authenticating the sensor node, the network updates information at its control points. The proposed solution for network access control relies on cryptographic filtering. The control points will retrieve the necessary cryptographic materials (e.g. keys, access rights) from the authentication module. The control points may also require information to resolve pseudonymous identifiers, if used, by interacting with the ID resolution module.

The network access control enforcement is performed at different points in the network. It may require different cryptographic materials if these enforcement points are heterogeneous in terms of resources or pertain to different administrative domains.

4.1.3.2 Protocol

The network access control can be enforced through either link-layer security or upper-layer security (over the IP protocol). The first approach may rely on group keys or pairwise keys; while in the second approach, pairwise keys are generally employed. The first approach provides earlier protection against Denial of Service (DoS) attacks than the second one, since intermediary devices between the device and the enforcement points in the second approach route received messages without DoS protection.

In the TWISNet framework, the proposed approach for network access control relies on link-layer security whereby the network access control is enforced at one-hop from the device. The upper-layer (e.g., UDP) access control approach will be also investigated. In this case, the enforcement point can be selected at multiple hops from the device. For example, the enforcement point role can be played solely by the Gateway (i.e., network access control and network access enforcement functionalities are collocated), thus providing simplified access control management.

The keys used are derived by the Gateway and shared between the device and its corresponding enforcement points. Multiple enforcement points are selected by the Gateway; thus allowing continued connection of the device, when this latter moves within the WSN. In order to select the enforcement points for the device, the Gateway may rely on information collected during the initial authentication of the device e.g., information about the PRE [59], information from the neighbor discovery phase (e.g. [63]) performed by the device and sent to the Gateway.

The network access control depends on the result of the authentication. For instance, upon successful EAP authentication, the Gateway is provided with a master session key (MSK) from the Trust Center. The key will be used to derive additional keys e.g., PEMK (PaC-EP Master Key) [60] that are securely delivered to enforcement points in the network. The distribution of PEMKs to enforcement points may use the mechanism proposed in [68].

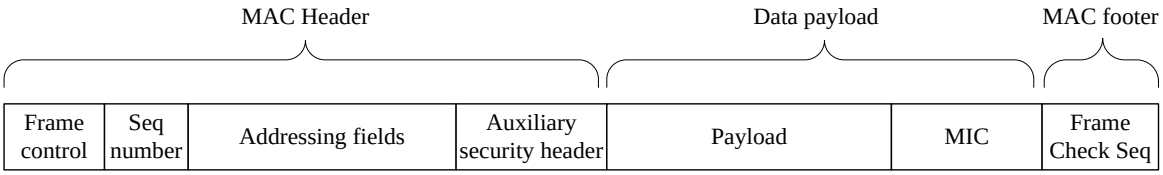


Figure 5. Packet format with 802.15.4 AES-CBC-MAC security suite [70]

After being provisioned with cryptographic materials, enforcement points can establish security associations with the authenticating device. To simplify this process, the device may just derive locally, from the MSK key, the 512-bit PEMK key from which another 128-bit key is derived and used by lower-layer security (e.g. 802.15.4 security suites). The device sends packets with a Message Integrity Code (MIC) appended to each MAC-layer frame. As example, the device may use the security suite AES-CBC-MAC of 802.15.4, as in Figure 5, that provides data authenticity. MIC ensures the integrity of the MAC header and the payload data attached. As discussed in [70], an auxiliary security header is included in the MAC header that specifies, in particular, a frame counter field that offers a protection against replay attacks.

4.1.4 Re-authentication

4.1.4.1 Tasks and actions

Some sensor nodes are mobile and move within the same PAN or from one PAN to another one (e.g. scenarios 1 and 4). Re-authentication and network access control are carried out more often for a mobile sensor node than for a static one; therefore, these operations should be realized in a fast and lightweight fashion.

The mobility management module is an optional module that extends both the authentication and network access control modules. The cross-domain context is supported by the module

enabling the mobile sensor node to re-authenticate to its home domain through a different domain network. The mobile sensor node will also be able to securely establish security associations (SAs) with the sensor nodes from its home domain within a foreign domain network.

For the mobility management module, four cases are considered:

1) *Fast re-authentication of a mobile sensor node to a Gateway:* the sensor node moves within a PAN. The node may connect directly to the Gateway using its allocated IP address (no need for a PRE [59]). Generally, the node re-authenticates to the Trust Center through the Gateway. Since, the node has been authenticated to the Gateway in the past, it may rely on the established SA to proactively request from the Gateway to provision its new neighbors with the required credentials to establish SAs with them.
2) *Fast authentication of a mobile sensor node to a Gateway:* the sensor node moves from PAN to PAN. Based on ERP/AAK [61], the new Gateway will be provisioned in advance with the required credentials (derived from pMSK) to authenticate the sensor node.
3) *Fast authentication of a mobile sensor node to a foreign Gateway:* the sensor node moves from one PAN to a new PAN subscribed to a different administrative domain. Similarly to ERP/AAK, the foreign AAA server will receive initial credentials (i.e. pMSK) allowing the authentication of the mobile sensor node through multiple Gateways from the foreign administrative domain.
4) *Home network access control through a foreign Gateway:* the sensor node moves to a new PAN from a foreign domain. The PAN may be composed of nodes from the same domain as the sensor node. The home Trust Center will provide integrity and confidentiality protected credentials to the sensor node enabling this latter to establish SAs with its neighbors from the same domain as itself. Based on channel bindings exchange [62] used to prevent the lying network access server (NAS) problem, these credentials will be securely provided to the sensor node.

The following sub-section proposes a solution to the fourth case.

4.1.4.2 Protocol

The proposed solution consists of an extension to the authentication protocol, e.g., EAP, that aims at bootstrapping security associations between a newly authenticated node and those of its neighbors that belong to the same domain, without letting intermediary foreign entities gain any knowledge of the exchanged key material.

The solution is made of four phases (illustrated in Figure 6): (1) initially, the joining node discovers the identities of its neighbors; (2) it then undergoes an unchanged authentication procedure; (3) this authentication phase concludes with an end-to-end exchange between the node and the Trust Center; (4) finally, security associations with the neighbors belonging to the same domain are established.

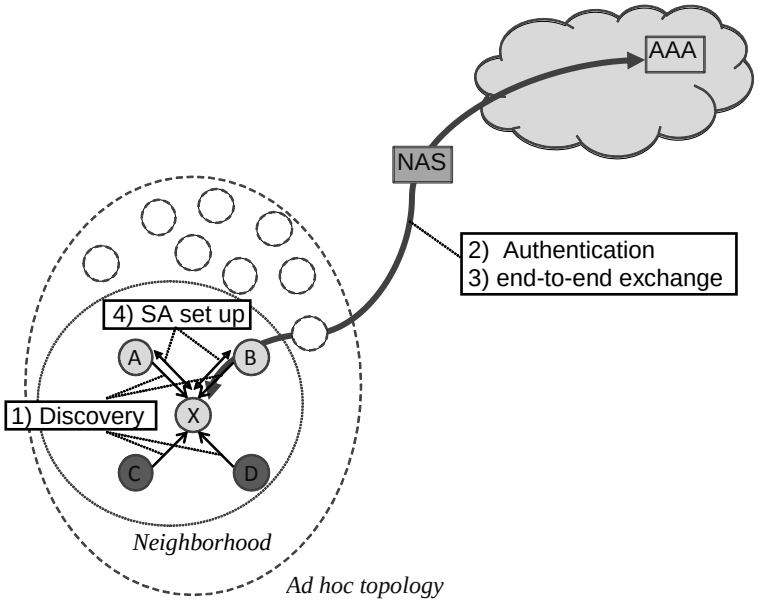


Figure 6. Phases of the mobility management protocol

1) Neighborhood discovery

A node joining a new infrastructure has to discover its immediate neighbors prior to carrying out authentication for network access; this is a well-known requirement, emphasized in ad-hoc communications [63]. In its first phase, the proposed solution leverages on the neighborhood discovery system in place in the visited network to let the joining node identify its neighbors and recognize those that belong to the same domain, for example, using the ”realm” domain of its neigbor nodes Network Access Identifiers (NAI) [71].

2) Regular authentication procedure

The authentication procedure between the joining client node and the Trust Center is kept unchanged by the proposed solution.

3) End-to-end exchange

The end-to-end exchange between the joning node and the Trust Center e.g., channel bindings exchange [62], is used to carry a set of keys, called *neighbor Master Session Keys* (nMSKs), corresponding to the previously identified neighbors.

4) Set-up of security associations

Security associations between the joining node and its neighbors are set-up using nMSK as a shared secret. While the joining node has received nMSK within the previous phase, each neigbor is able to generate it from its stored keys, namely a derived seed that we call nKGS (neigbor Key Generation Seed), and joining node’s identity received in the beginning of a security association protocol run. IKE [64] is an example of such security association protocol that can leverage on an existing shared secret between two nodes.

A protocol implementation of the proposed solution is described in Figure 6.

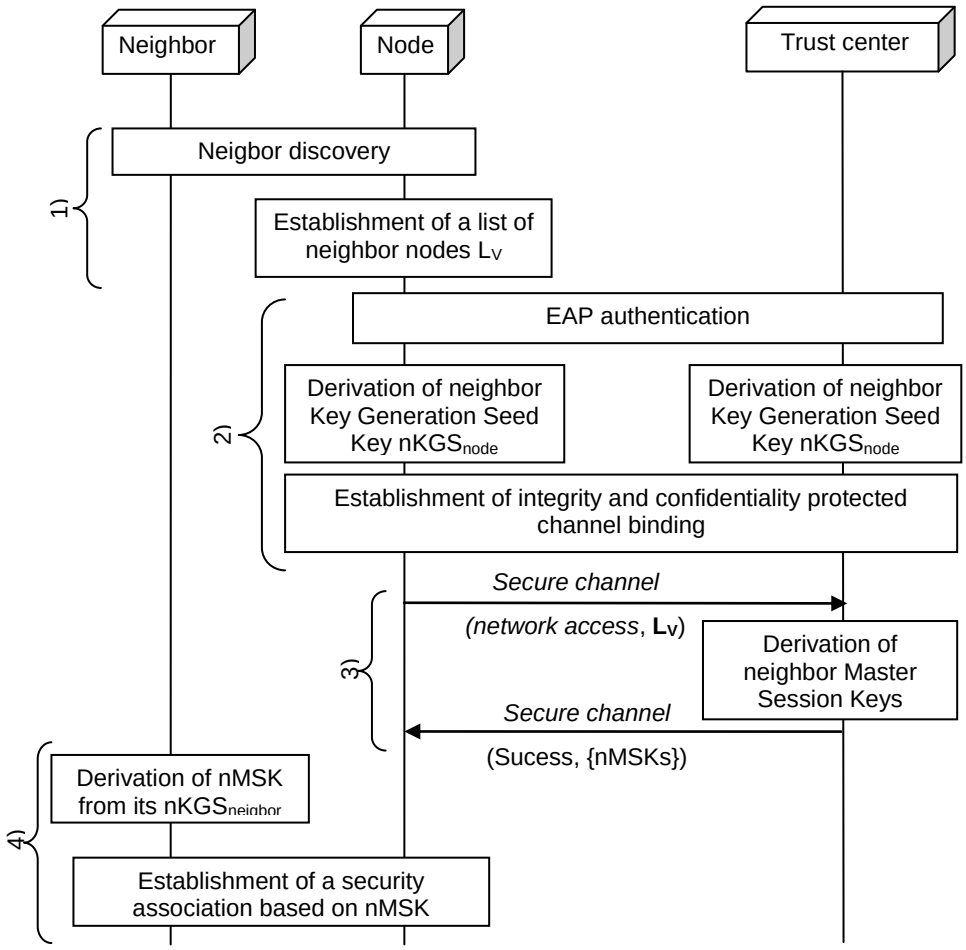


Figure 7. Cross domain EAP-based re-authentication and network access control

4.2 ID privacy

The ID privacy subsystem includes ID randomization and resolution modules and a privacy manager (this module is described in D3.3.1). As stated previously, these modules interact with the authentication and network access control modules. They also interact with the key management module.

The sensor mobility and cross-domain management contexts should be supported by ID randomization and particularly ID resolution modules.

4.2.1 ID randomization/resolution

4.2.1.1 Tasks and actions

The ID randomization module is implemented at all sensor nodes that need to be privacy protected (e.g., scenarios 1 and 4). Randomization is applied to all identifiers, but not all randomized identifiers need to be resolved. Some of the identifiers (e.g., MAC address) are simply randomized. Others identifiers (e.g., IP address, certificates) are derived based on cross-layer synchronization. These identifiers should be resolvable by some network entities (e.g., Gateway, network access control enforcement points).

The ID resolution module is implemented at network access control points. The ID resolution module provides likability between multiple pseudonyms, but do not reveal the real identity of the sensor node. Only the Trust Center can resolve the real identity of the sensor node for application-related operations.

The Trust Center is responsible of pseudonyms generation and their secure distribution to control points. Generating pseudonyms by a trusted authority rather than the sensor node itself avoids the issue of pseudonym ownership proof and verification. As example, if MOBIKE [65] is used to change IP addresses chosen by the node, the control points should perform a “return routability” check for each new address.

4.2.1.2 Protocol

We propose a pseudonym-based approach for ID randomization and resolution. Anonymisation is applied at the different levels of the communication stack with cross-layer synchronization. Some of the anonymized identifiers can be encrypted, and only nodes holding decryption keys can resolve these pseudonyms. Some other identifiers are derived rather based on lightweight cryptographic operations (e.g., hash functions). Other identifiers are simply generated randomly and uncorrelated as in [43] or [45].

We distinguish between three groups of identifiers:

- **Applicative identifiers:** these identifiers consist of identifiers used in upper layer headers. Since their resolution is required only at the communication end-points, encryption operations can be used for ID anonymisation.
- **Networking identifiers:** these identifiers consist of identifiers used in networking layer headers. Their resolution is required at multiple intermediate nodes (e.g., routers, access control enforcement points). Lightweight cryptographic operations can be used for ID randomization and resolution.
- **Link-based identifiers:** these identifiers consist of identifiers used in lower layer headers. In the context of a WSN, these identifiers can be randomized and their resolution may be omitted.

The mechanism introduced in the following sub-sections focuses on providing anonymization for routing identifiers.

4.2.1.2.1 ID randomization

The Trust Center is responsible of generating pseudonyms for sensor nodes. Pseudonyms are generated by means of a keyed function. We opted for keyed hash chains used in the reverse order (e.g., [2]). The sensor node generates pseudonyms by computing the keyed hash chains and using them in reverse order.

A keyed hash chain is derived by successive application of a keyed hash chain, denoted Hash, using a key pMK (Privacy Master Key), over a random number, denoted r. A pseudonym P_i derived from a keyed hash chain used in reverse order is computed as follows:

$$P_i = Hash^{(m+1-i)}(pMK, r) \quad (4.1)$$

Where $Hash^{(m-i)}$ means that the hash function is applied (m+1-i) times, m being the hash chain length. The root of the hash chain in reverse order is given by $Hash^{m}(pMK, r)$. A generated pseudonym P_i matches one of the pseudonymous identifiers depending on the used Hash function (output function space). The key pMK could be derived from the keys boostrapped by the authentication module (e.g., from EMSK).

The pseudonym information consists of roots of multiple keyed hash chains, their corresponding keys and random numbers from which chains have been derived. For a given sensor node, such pseudonym information is generated by the Trust Center. Only keys and root hash chains are provisioned to control points.

After their generation by the Trust Center, pseudonyms are securely distributed to control points during bootstrapping (first authentication) and re-authentication. The authentication protocol EAP can be enhanced to distribute such information in a secure way based on channel binding exchanges [62]. After successful EAP authentication, the authenticator, i.e. the Gateway, receives credentials (e.g., MSK). These credentials will contain also the pseudonym information. The authenticator will securely distribute credentials to the PANA enforcement points (EPs) that are implemented in separate devices as described in [60]. Credentials contain the key and the root of a keyed hash chain. With this information, each enforcement point can verify the anonymous messages received from a legitimate sensor node.

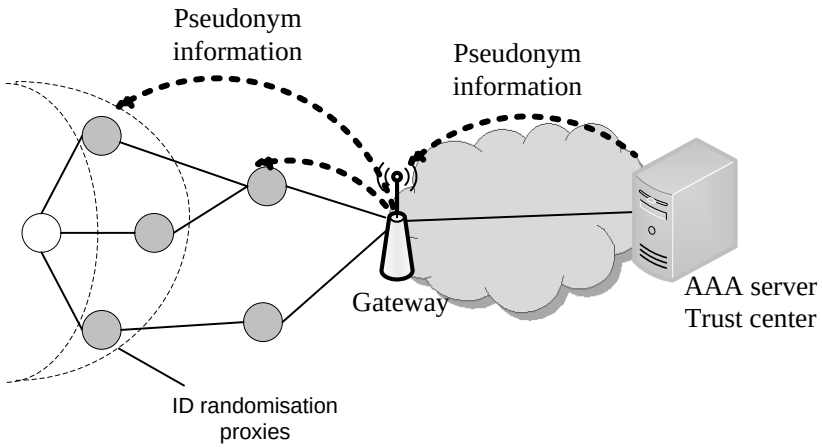


Figure 8. Proxy-based ID randomisation

At the anonymous device level, its IDs can be randomized in two ways, depending on the sensor node capabilities:

a) The sensor node can be capable of randomizing by itself its IDs. It can generate pseudonymous network addresses based on the pseudonym information received from the Trust Center during node authentication. In this case, the sensor node is provisioned with the keys and random numbers to be able to generate the chains by itself. Such keys could be derived from the keys generated after successful authentication. For instance. The device may derive a seed key pKGS (Privacy Key Generation Seed) from EMSK, from which it derives multiple rMK keys. To offload the computation load on the sensor node, an alternative way is to securely provision the sensor node with a list of already-computed pseudonyms.

b) The approach proposed in the previous subsection for ID randomisation requires from the sensor device to regularly change all its IDs in a synchronized way. This can be performed by only some sensor nodes from the network (e.g., routing nodes), but it may not be practicable for end devices that are may be stateless and having sleeping cycles. In order to continue to provide privacy protection for these devices, the proposed approach could be enhanced by relying on proxies distributed within the

WSN and responsible with the ID randomisation of these highly-resource-constrained devices. Proxies should be located at one-hop from the devices (refer to Figure 8). The role of proxies for ID randomisation could be played by the one-hop enforcement points introduced by the network access control module in subsection 4.1.3. Proxies secretly receive a set of pseudonyms generated for the anonymous devices as described earlier in this subsection, from the Gateway, using for example the mechanism in [68]. The pseudonymous information received by proxies is distributed and managed by the Gateway, since this latter is responsible of selecting proxies associated with the anonymous devices. Whenever proxies receive messages from the devices to be routed toward the Gateway, they produce new messages including the relayed messages from the devices and encrypted ID information on these devices containing, for examples, their IP address and UDP port numbers. Messages from proxies are sent using pseudonyms as source addresses. The proposed approach does not require any actions from the anonymous devices since proxies perform the ID randomisation on behalf of them; however, the approach provides ID privacy protection only beyond one-hop from the anonymous devices.

4.2.1.2.2 ID resolution

The Trust Center retrieves a large list of pseudonym information of this form: $\{(pMK_j, Hash^m(pMK_j, r)\}_{1\leq j\leq l}$. Subsets of this list are distributed to Gateways, to which the sensor network is attempting to authenticate, either from within its home domain or a foreign domain. Gateways will distribute the key and the root associated with a chain to each enforcement point located in the vicinity of the sensor node.

We consider three levels of control points (Figure 9):

- **First level:** the first level consists of the home domain Trust Center that is deemed to be the highest security authority in our considered architecture. The Trust Center is in charge of providing a subset of pseudonym information to the following level control points.
- **Second level:** this level generally consists of Gateways to which the sensor node connects. After being provisioned with pseudonym information, Gateways are in charge of providing in their turn a subset of this information to the third level control points.
- **Third level:** this level may consist of nodes used as enforcement points (e.g., PANA EPs) to control access of the sensor node to the network. Generally, these enforcement points are not collocated with the Gateway (e.g., the access point). For example, the first-hop neighbors of the senor node can be responsible of controlling access to the network.

Optionally, other control point levels could be considered like for example, defining a different level for Gateways or enforcement point nodes subscribed to a different administrative domain from the sensor node domain.

Each control point is provided with the capability to link pseudonyms of a given sensor node. This capability is limited in time according to the control point level, i.e. lower levels have shorter time capability than higher levels. The control points need to be provisioned regularly with pseudonym information in order to be able to verify the legitimacy of the sensor node.

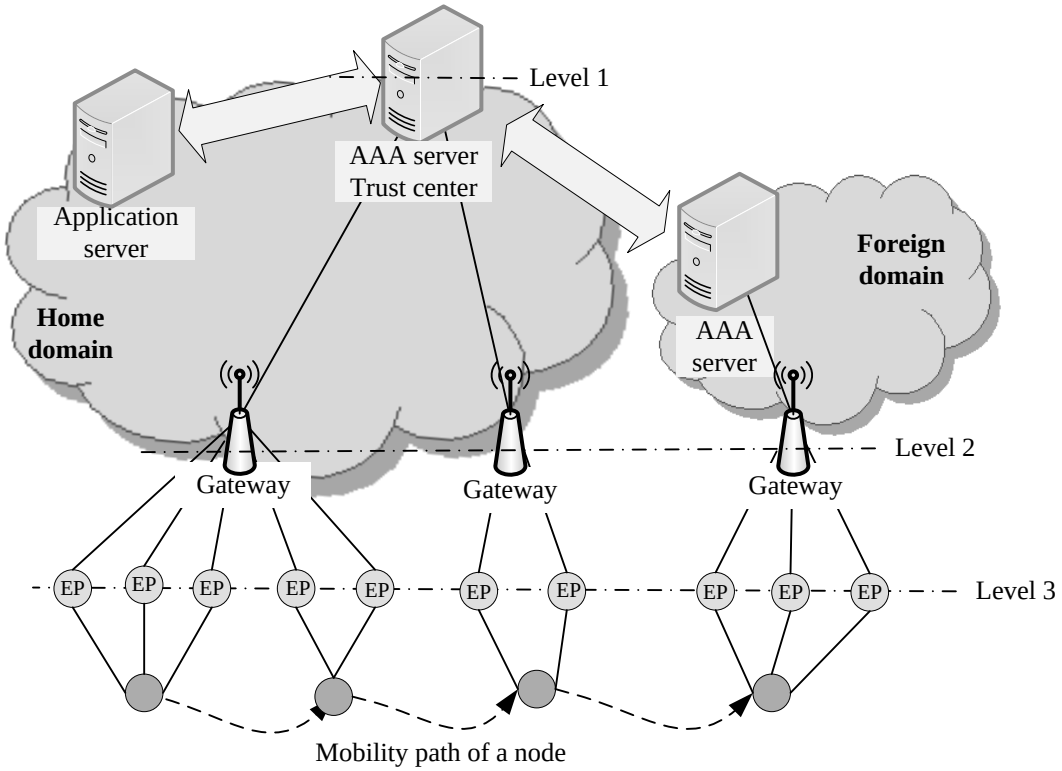


Figure 9. A mobile sensor node authenticating to its home domain trust center in a multi-domain infrastructure. Three levels of control points: enforcement points (EP) at level 3, Gateways at level 2, and Trust Center (authentication server) at level 1.

The control points resolve the used pseudonyms based on the secret pseudonym information provisioned to them. For instance, they will compute a keyed hash over the received pseudonym and compare it with the previously used pseudonyms. If there is a match, the pseudonym is valid and is linked to the communication flow with the old pseudonym. Only these control points are able to link pseudonyms of a given sensor node.

4.3 Secure routing

4.3.1 Modules

The secure routing subsystem is dedicated to energy-efficient, secure and fault-tolerant transport of data packets in the network including multi-owner systems. On the one hand, there is a need to establish a routing that especially fits the needs for energy efficiency and security, i.e. low latency in emergency situations, in any kind of network. Additionally, in a multi-owner network, the rights of various services to access the resources of the network need to be managed. Nodes from one service can route the packets of another with no direct benefit to services of the node routing the packet. Therefore, metrics have to be generated locally and over the network to allow decisions about optimal routing paths. Although the TWISNet framework is established between network layer and application layer, additional functionality has to be integrated with respect to the network layer. To separate functionality, two modules have been established as add-on for an existing routing protocol. The Secure Routing Protocol (SRP) module is responsible for collection of routing relevant information and sending it to routing calculation instances. So this module may be quite independent of the used network stack and may be also used in conjunction with other routing protocols, i.e.

RPL. The Packet Forwarding (PF) module is responsible for calculation and establishment of the routes based on the information gathered by SRP and forwarding the packets on these routes. Using these two modules, the establishment of dedicated routes for certain services is provided.

4.3.2 Secure routing protocol

4.3.2.1 Tasks and actions

The Secure Routing Protocol applies a local evaluation of routes to the neighbors in terms of metrics as energy consumption and security. Therefore, links to the neighbors as well as the local parameters of nodes are analyzed and send to one or more routing calculating instances. The packet calculating instance, i.e. realized by the Packet Forwarding module, uses the metrics to calculate optimized routes. SRP is designed to work with other packet calculating instances, i.e. the routing calculation realized by the RPL protocol [66].

To enable energy-efficient and secure routing, local metrics have to be defined to improve fair and secure distribution of packets for routing also in multi-owner mesh networks. A number of fair routing schemes have been developed, which rely on additional information from the neighbors, i.e. energy supply type (mains powered or battery), battery status, ownership and the number of routed packets from a certain source. By using this information as additional additive or multiplicative link or node weights in the network graph, either constraints can be established to force using routes with certain parameters (i.e. use nodes of owner A and B only) or it can be used as metric to find optimum routes with respect to certain parameters. This module only takes local metrics into account, meaning information that a node is able to obtain locally in cooperation with its direct neighbors. As most networks are not full meshed networks, we do not assume a full meshed network here but at least a network topology, which allows some routing path options. For example, an additional tree topology with additional links between router devices in order to have a kind of mesh links.

We propose to basically rely on a subset of metrics proposed in [66] and to adapt and extend it by parameters needed for multi-owner network security. The scheme is intended to work with RPL routing [67] but can be used by other routing procedures too. It defines a set of link and node metrics and constraints for low power and lossy networks as well as techniques for their application. Further functionality may be added later.

In detail, the following node and link local information is defined in so called objects to be used as constraint or metric.

- A Node Energy metric is used to gather information about the energy status of a node. This includes characteristics on power source, current power consumption and estimated lifetime.
- A Hop Count metric reports the number of traversed nodes along a certain route regarding a central node.
- A Link Throughput object is used to report the currently available and maximum throughput of a certain link.
- A Latency object gives information on latency regarding certain links or paths.
- A Link Reliability object can be used to gather information on the link quality level and on probability of communication success.
- A Node Color object is used to mark certain links by users or the nodes itself in order to avoid or prefer them.

For the TWISNet architecture, these metrics are extended by the following objects.

- A Node Owner object gives information about the owner of a certain node and reports parameters of the availability of this node for certain services of other owners.
- A Node Trustworthiness object contains information gathered by monitoring the network to report trustworthiness of a certain node.
- A Node Security Capability object contains information of the security features supported by a node.

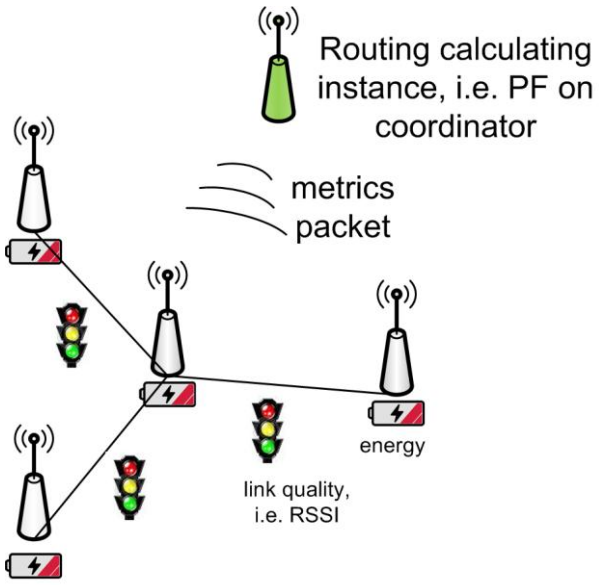


Figure 10: Example network running SRP; the central router node collects local available information like its energy state and the link quality with the neighboring nodes and sends it to the routing calculating instance

Further objects may be added easily in the future.

From the security point of view, the metrics have to be protected against attackers regarding possible abuses. False good metrics, which an attacker may set to route certain packets over their own nodes or over certain routes have to be detected. The attack on a certain link to manipulate a metric like link quality has to be coped but is not a task of the routing protocol. The visibility of these metrics has to be protected in general, to avoid presenting weaknesses of a node or a link to an attacker, e.g., a low energy level.

4.3.2.2 Protocol

In case of TWISNet, a balance between energy consumption and security has to be implemented also in establishment of dedicated routes. This can be achieved by a dynamic prioritization scheme of several metrics by using adequate objective functions. This allows using higher security but maybe less energy efficient paths for certain services whereas energy optimized paths are used for less security critical services.

Following metrics are defined to be used as metrics or constraints in detail based on the metrics defined in [66].

a) Node Energy metric
The Node Energy (NE) metric contains information about the self-evaluation of the energy consumption and storage of a node. It contains the following attributes:

- Node Type: This attribute describes the power source of a node, which may be either mains-powered, battery-powered or an energy harvesting device.
- Estimated-Energy: This parameter reflects a self-evaluation of the nodes energetic state. According to [66], for battery powered devices, E-E is the current expected lifetime divided by the desired minimum lifetime, in units of percent.

This metric is delivered to all neighboring nodes during the association process and updated periodically, i.e. added to normal data packet transmission.

b) Hop-Count Metric
The HP metric is used to report the number of traversed nodes along a certain path. In TWISNet network topology, the HP contains the number of hops to the coordinator of the network.

This metric is delivered to all neighboring nodes during the association process and updated periodically, i.e. added to normal data packet transmission.

c) Throughput Metric
The Throughput metric is used to report the currently available and maximum throughput of a certain link, which strongly depends on duty cycle and so, on battery consumption. Throughput is expressed in bytes per second.

This metric is generated in cooperation with neighboring links on a link by link basis.

d) Latency Metric
The Latency metric gives information on latency regarding certain links when using it as recorded metric or regarding certain paths when using it as aggregated metric. Latency is expressed in microseconds.

This metric is generated in cooperation with neighboring links on a link by link basis.

e) Link Reliability
The Link Reliability (LR) metric is used to gather information on the link quality level and on the probability of communication success.

The LR object contains the following attributes whereas at least one has to be present.

- The Link Quality Level (LQL) indicates the link quality. In case of TWISNet architecture, this is represented by a RSSI value.
- The Expected Transmission Count (ETX) metric is the number of transmissions a node expects to make to a destination in order to successfully deliver a packet. This is based on the packet error rate.

This metric is generated in cooperation with neighboring links on a link by link basis.

f) Link Color Object
The Link Color (LC) consists of a number of flags used to mark certain links by users or the nodes itself in order to avoid or prefer them.

In case of TWISNet, this is extended to establish a service-path matrix, which is used to constrain certain services to dedicated paths only.

This metric is set by the user locally.

g) Node Owner Metric

A Node Owner (NO) metric gives information of the owner of a certain node and reports parameters regading the availability of this node for certain services of other owners.

The availability is marked by a flag to indicate the general binary permission to be used by other owner's services. A finer granularity is achieved first by giving permissions for certain users only and second by adding flags for certain services, e.g., routing or cooperative behavior monitoring. In this way, a simple local user control with the entries user and service is established.

This metric is delivered to all neighboring nodes during the association process and updated periodically, i.e. added to normal data packet transmission.

h) Node Trustworthiness Object

A Node Trustworthiness (NT) object contains information gathered by monitoring the network to report the trustworthiness of a certain node.

The trustworthiness is defined with respect to certain services. It may use the evaluation results of the FABD and DTE modules.

This metric is delivered by the central trustworthiness agent to all nodes neighboring a certain node.

i) Node Security Capability

The Node Security Capability object contains information of the security features supported by a node. This includes supported security services and algorithms, for example public/private key encryption, authentication and encryption hardware support.

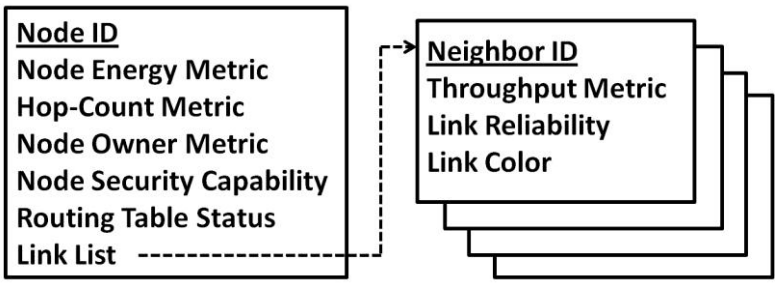


Figure 11: SRP node entry example; the node contains its own available node metrics as well as a list of link metrics to its neighbors

This metric is delivered to all neighboring nodes during the association process and updated periodically, i.e. added to normal data packet transmission.The mentioned metrics are collected by SRP locally on each node and send to routing calculation instances. There, a routing calculation unit, i.e. TWISNet PF or RPL may calculate optimized routes based on SRP metrics and additional information.To protect the metrics against attackers regarding possible abuses, the following actions are taken.

- False good metrics, which an attacker may set to route certain packets over their own nodes or over certain other routes have to be coped. As the detection itself is hard to perform in case the metrics are correct, attributes can be set to use certain routes only for certain services (see LC object).

- The attack on a certain link to manipulate a metric like link quality has to be coped but is not a task of the routing protocol. The attack can be detected by analyzing improbable metric changes, i.e. using TWISNet FABD.

The visibility of these metrics has to be protected in general, to avoid presenting weaknesses of a node or a link to an attacker, e.g., a low energy level. This is achieved by using authentication and sufficient confidentiality levels for communication.

4.3.3 Packet forwarding

4.3.3.1 Tasks and actions

The Packet Forwarding (PF) module performs packet forwarding towards the destination by creating routing decisions based on metrics and constraints gathered by the Secure Routing Protocol module and other available information, i.e. from the Network Access Control and Connection Sharing modules.

Therefore, PF runs at routing calculation instances, i.e. at the coordinator of a WSN, and calculates routing decisions and propagates it to the nodes. Establishment as well as maintenance of the routes is main task of this module.

As most networks are not full meshed networks, we do not assume a full meshed network here but a topology, which features at least some additional routes to offer routing path options. This allows applying the security concepts to a variety of existing network topologies without excluding mesh network based security advantages.

The basic concept of PF is the establishment of dedicated routes additional to an existing standard routing protocol. It is assumed that the PF instance is aware of the actual network structure and able to calculate optimal routes for certain criteria. Optimized routes are propagated to the nodes in dedicated routing tables and can be used if needed. The proposed scheme features energy efficiency, scalability and mobility by using a hybrid approach of proactive routing, where all nodes know a part of the whole network and reactive routing where a route is determined when it is needed.

Basically, the routing scheme relies on knowledge of the metrics described in the Secure Routing Protocol and additional information regarding their associations in the network.

4.3.3.2 Protocol

For proof of the security concepts, we propose a network featuring at least a mesh-like topology like an extended tree topology with a coordinator as central node, several routers, which are able to have more than one child node and end nodes, which are leaf nodes in the topology. Additionally, dedicated routers are allowed to create associations with other routers to create a kind of mesh topology. This allows to proof security and energy efficiency concepts, which rely on having different routing options to send a message between two nodes.

We propose a routing scheme, where any router gathers the information described in the Secure Routing Protocol section from its neighboring routers and updates it regularly. Updates may be done by requesting a neighboring node for its actual metric or by receiving an indication of a neighboring node to update a certain value. The information is used at the routing calculation instance where optimized routes are calculated using the Dijkstra algorithm. This saves network traffic and memory compared to a distributed routing scheme.

We propose at least three standard objectives for routing.

The standard objective for normal operation is energy efficient routing. Here, latency and throughput are less important than the node energy and hop count metrics. If possible, the optimization tries to use nodes with highest energy reserves available whereas the hop count does not exceed a maximum of the hop count of the shortest path plus a predefined offset, e.g., 20%.

In case of firmware or credential updates over the air, reliability and trustworthiness of links is set as most important metric for routing. Therefore, routes are chosen that are assumed to be failure resistant and that satisfy certain security constraints, e.g., using a dedicated encryption scheme.

For emergency situations, dedicated routes featuring low latency and high reliability are taken as constraints.

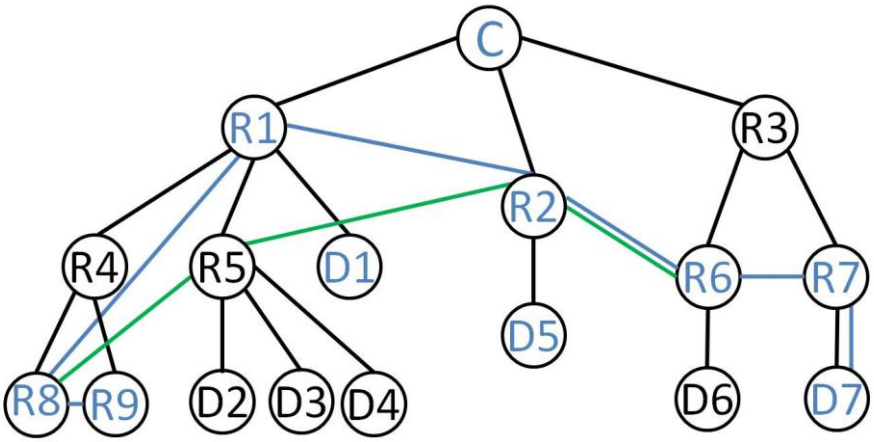


Figure 12: Example network structure using PF; the black lines indicate standard routing; the blue and green lines indicate additional PF routes optimized on certain criteria; note that only routers (R) are able to connect to more than one node in common WSN; end devices (D) may be start or end points of PF only

Further objectives may be defined additional to these standard objectives to satisfy dedicated user needs. Therefore, PF includes a configurable structure where a number of objectives can be stored and activated packet-wise individually. Unique objective IDs are defined for any standard and user defined objective. A sender marks a packet with an objective ID that the receiver is able to determine the best next hop based on the objective function. If the receiver does not know the function belonging to a certain objective ID, it requests it from the sender of the packet.

Dedicated routes with respect to the objective functions may be established additional to the exiting routing. A route from A to B regarding an objective function is requested by a higher layer application or by a router in the network. The optimized route is requested from the routing calculating instance, i.e. the coordinator. The coordinator then sends the information of the full path to the first node A of the path with an establishment packet. Node A stores the criteria ID and the next hop in a dedicated PF routing table and sends the remaining path information to the next hop on the path. This one also stores the criteria ID and the next hop as well as optionally the previous hop to allow bidirectional communication. In most application cases, a unidirectional path may be sufficient, e.g., when sending information to the coordinator. Nevertheless, if an acknowledgement or answer is needed to be routed by the same criteria, the channel has to be bidirectional. The other nodes on the path apply the

same protocol until B is reached. Therefore, not only an optimized route from A to B is established regarding the objective functions but also from all intermediate nodes to the end node B or to A in bidirectional case.

The routers can store additional channels until the additional routing table is filled. The information on load of the routing table can be seen as additional metric gathered by SRP. Therefore, the coordinator is able to include this information in the objective function and not to use this router or to send a delete request of a certain channel to the router to allow the establishment of new routes. Delete packets work like establishment packets to delete certain channels.

A route can include 48 hops when using an UDP/6LoWPAN stack as there are 96 Byte of payload and 2 Byte short addresses used. This may be extended by establishing continuous paths, like routing from A to B: first routes from A to C and then from C to B.

The coordinator saves all established routes for maintenance reasons. Also, higher layers may be allowed to access a list of established routes. In case of a broken link, the PF on a router, which detects that a link is not valid anymore, sends a new request for establishment to the coordinator to repair the route by calculating a new route and deleting the old one.

5. CONCLUSION

This deliverable describes the security solutions relative to task 3.2 that are used in the TWISNet security framework.

After a state of the art study, the security solutions focused on providing ID randomization and resolution mechanism, authentication and network access control extensions supporting fast re-authentication in single and multi-domain contexts, and secure routing allowing for fairness and energy-efficiency.

The deliverable presents the architecture of the task framework with the identified security solutions as modules. The architecture description shows that the identified modules interact mostly with each other.

A detailed description of these modules is presented. Based on the Authentication and Mobility Management (AMM) module, authentication of multiple nodes can be provided through either simultaneous operations or an aggregated exchange. The Network Access Control (NAC) module proposes extensions allowing the provision of mobile nodes with the necessary cryptographic materials to establish security associations in particular within a foreign network. The ID Privacy (IDP) module introduces an ID randomization and resolution mechanism that relies on changing pseudonyms associated with a given node generated by a Trust Center and distributed only to the control points in the network and the node in question. Secure routing mechanism with multi-level metrics is proposed to provide fairness and energy efficiency. It manages energy-efficient, secure and fault-tolerant transport of data packets in the network, taking into account also multi-owner systems. To separate its functionality, two modules have been established as add-on for an existing routing protocol. The Secure Routing Protocol (SRP) module is responsible for collection of routing relevant information and sending it to routing calculation instances; whereas the Packet Forwarding (PF) module is responsible for calculation and establishment of the routes based on the information gathered by SRP and forwarding the packets on these routes. Using these two modules, the establishment of dedicated routes for certain services or owners is provided.

The described modules fit the general picture of the identity management framework. In particular, the selection of protocols for authentication (e.g., EAP over PANA or over LANs) supporting multi-domain sensor mobility (e.g., AAA protocols), and for routing and packet forwarding (e.g., RPL) will depend on the common security functionalities that will be provided by the TWISNet framework (e.g., secure UDP connection), as well as, the expected interactions with the other modules (e.g., key management, security adaptation, mediation layer) with the aim to ease the integration of these modules within the framework. The specification of the modules will be finalized in work package 4 by selecting appropriate cryptographic methods and functions (e.g., pre-shared keys, hash functions) based on the hardware implementation of sensor nodes in work package 4.

6. ACKNOWLEDGEMENT

The TWISNet consortium would like to acknowledge the support of the European Commission partly funding the TWISNet project under Grant Agreement FP7-ICT-STREP-258280.

7. REFERENCES

[1] A. Wadaa, S. Olariu, L. Wilson, M. Eltoweissy, and K. Jones, “On providing anonymity in Wireless Sensor Networks,” The Tenth International Conference on Parallel and Distributed Systems, 2004, pp. 411-418.
[2] Y. Ouyang, Z. Le, Y. Xu, N. Triandopoulos, S. Zhang, J. Ford, and F. Makedon. Providing anonymity in Wireless Sensor Networks. In Proceedings of *the IEEE International Conference on Pervasive Services*, pages 145-148, Istanbul, Turkey, July 15-20, 2007.
[3] A. Mitseva, M. Gerlach, and N.R. Prasad, “Privacy Protection Mechanisms for Hybrid Hierarchical Wireless Sensor Networks,” 2007 4th International Symposium on Wireless Communication Systems, Oct. 2007, pp. 332-336.
[4] J.P. Sheu, J.R. Jiang, and C. Tu, “Anonymous Path Routing in Wireless Sensor Networks,” 2008 IEEE International Conference on Communications, IEEE, 2008, p. 2728–2734.
[5] A. Panchenko, B. Westermann, L. Pimenidis, and C. Andersson, “SHALON: Lightweight Anonymization Based on Open Standards,” 2009 Proceedings of 18th International Conference on Computer Communications and Networks, Aug. 2009, pp. 1-7.
[6] Z. Zhang, C. Jiang, and J. Deng, “A Secure Anonymous Path Routing Protocol for Wireless Sensor Networks,” 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS), IEEE, 2010, p. 415–418.
[7] L. Buttyán and T. Holczer, “Perfectly anonymous data aggregation in Wireless Sensor Networks,” 2010 IEEE 7th International Conference on Mobile Ad hoc and Sensor Systems (MASS), IEEE, 2010, pp. 513-518.
[8] B. Riedl, V. Grascher, and T. Neubauer, “A Secure e-Health Architecture based on the Appliance of Pseudonymization,” Journal of Software, vol. 3, Feb. 2008, pp. 23-32.
[9] T. Neubauer and M. Kolb, “An Evaluation of Technologies for the Pseudonymization of Medical Data,” Computer and Information Science, 2009, pp. 47-60.
[10] PIPE, http://www.sba-research.org/research/data-security-and-privacy/pipe
[11] FIDIS, http://www.fidis.net
[12] UbiSec&Sens, http://www.ist-ubisecsens.org
[13] A.C.F. Chan and C. Castelluccia, “On the (Im)possibility of aggregate message authentication codes,” 2008 IEEE International Symposium on Information Theory, Jul. 2008, pp. 235-239.
[14] AVANTSSAR, http://www.avantssar.eu
[15] H. Abdelnur, T. Avanesov, M. Rusinowitch, and R. State, “Abusing SIP Authentication,” 2008 The Fourth International Conference on Information Assurance and Security, Sep. 2008, pp. 237-242.
[16] SEPIA, http://sepia-project.eu
[17] L. Chen, K. Dietrich, H. Löhr, A. Sadeghi, C. Wachsmann, and J. Winter, “Lightweight Anonymous Authentication with TLS and DAA for Embedded Mobile Devices,” 13th Communications Security Conference (ISC 2010), 2010.
[18] K. Dietrich, “Anonymous Client Authentication for Transport Layer Security,” Communications and Multimedia Security, Springer, 2010, p. 268–280.
[19] E. Boschi and B. Trammell. IP Flow Anonymization Support. IETF RFC 6235, May 2011. E. Boschi and B. Trammell. IP Flow Anonymization Support. IETF RFC 6235, May 2011.
[20] J.E. Holt and K.E. Seamons, “Nym: Practical pseudonymity for anonymous networks,” Internet Security Research Lab Technical Report, vol. 4, 2006, pp. 1-12.

[21] Atmel's New CryptoAuthentication Device Offers Improved Security for Microcontroller-based Systems, http://www.atmel.com/dyn/products/view_detail.asp?FileName=F2-110303-Crypto-SHA204.html
[22] Microcontroller with AES Authenticates Your Application for Only 300nA, http://www.maxim-ic.com/company/press_room/product.cfm/id/1746
[23] S. Misra and G. Xue. SAS: A simple anonymity scheme for clustered Wireless Sensor Networks. In Proceedings of *the IEEE International Conference on Communications*, 2006. ICC '06, volume 8, pages 3414-3419, June 2006.
[24] S. Misra and G. Xue. Efficient anonymity schemes for clustered Wireless Sensor Networks. *International Journal of Sensor Networks*. volume 1(1/2), 2006, pages 50-63.
[25] L. A. Martucci, M. Kohlweiss, C. Andersson, A. Panchenko. Self-certified Sybil-Free Pseudonyms. In Proceedings of *the 1st ACM Conference on Wireless Network Security*. April 2008, pages 154-159. Alexandria, VA, USA.
[26] T. Jiang, H. J. Wang, and Y. C. Hu. Preserving location privacy in wireless LANs. In *MobiSys '07: Proceedings of the 5th international conference on Mobile systems*, applications and services, pages 246–257, New York, NY, USA, June 2007. ACM Press.
[27] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2(1), pages 46–55, January 2003.
[28] Sungjune Yoon, Hyunrok Lee, Sungbae Ji, and Kwangjo Kim. A User Authentication Scheme with Privacy Protection for Wireless Sensor Networks. The 2nd Joint Workshop on Information Security, pp.233-244, Aug. 6-7, 2007, Tokyo, Japan.
[29] O. Delgado, A. Fúster, J. M. Sierra. A light-weight authentication scheme for Wireless Sensor Networks. Ad Hoc Networks. Elsevier. doi:10.1016/j.adhoc.2010.08.020. In press 2011.
[30] Kun Sun, An Liu, Roger Xu, Peng Ning, Douglas Maughan. Securing Network Access in Wireless Sensor Networks. In Proceedings of 2nd ACM Conference on Wireless Network Security (WiSec '09), March 2009.
[31] S. Zhu, S. Xu, S. Setia, and S. Jajodia. LHAP: A Lightweight Network Access Control Protocol for Ad-Hoc Networks. Elsevier Ad Hoc Networks Journal, Volume 4, Issue 5, Sept. 2006, pp 567-585.
[32] H. Hsu, S. Zhu, and A. R. Hurson. LIP: a lightweight interlayer protocol for preventing packet injection attacks in mobile ad hoc network. International Journal of Security and Networks, Vol. 2, Nos.3/4, pp. 202 - 215, 2007.
[33] Leonardo Maccari, Lorenzo Mainardi, Maria Antonietta Marchitti, Neeli R. Prasad, and Romano Fantacci. Lightweight, Distributed Access Control for Wireless Sensor Networks Supporting Mobility. Proceedings of IEEE International Conference on Communications, ICC 2008, Beijing, China, 19-23 May 2008.
[34] Johannes Schlumberger. Implementing the Phantom Protocol. Diploma Thesis in Computer Science, University of Erlangen-Nürnberg, 2010.
[35] I2P project (Invisible Internet Project): http://www.i2p2.de/
[36] E. Yüksel, H.R. Nielson, F. Nielson. ZigBee-2007 Security Essentials. In Proceedings of the 13rd Nordic Workshop on Secure IT-systems (NordSec 2008), pages 65-82, Copenhagen, Denmark, 2008.
[37] Bluetooth: https://www.bluetooth.org/apps/content/
[38] D. Liu and P. Ning. Multi-level mTESLA: Broadcast authentication for distributed sensor networks. ACM Trans. Embedded Computing Systems (TECS), vol. 3, no. 4, pp. 800-836, 2004.
[39] The TOR project: http://www.torproject.org/
[40] Anonymizer: http://www.anonymizer.com/
[41] Ohba, Y. and Zorn, G., Extensible Authentication Protocol (EAP) early authentication problem statement. IETF RFC. v5836.

[42] Ohba, Y., Pre-authentication support for PANA. IETF RFC. v5873.
[43] Narten, T., Draves, R. and Krishnan, S. *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, RFC 4941, September 2007.
[44] IETF *RFC 3315*. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). July 2003.
[45] CALM, Continuous Communications for Vehicle, SeVeCOM Workshop, Lausanne 1-2 February 2006, retrieved at http://www.sevecom.org/Presentations/2006-02_Lausanne/Sevecom_2006-02-02_E%20CALM.pdf (May 2011).
[46] Celia Li and Uyen Trang Nguyen. Fast authentication for mobility support in wireless mesh networks. *Wireless Communications and Networking Conference (WCNC)*, 2011 IEEE , vol., no., pp.1185-1190, 28-31 March 2011, doi: 10.1109/WCNC.2011.5779299
[47] Jangseong Kim, Joonsang Baek, and Taeshik Shon. An efficient and scalable re-authentication protocol over Wireless Sensor Network. *Consumer Electronics, IEEE Transactions on* , vol.57, no.2, pp.516-522, May 2011, doi: 10.1109/TCE.2011.5955187
[48] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF Formulas on Ciphertexts. In *Proceedings of Theory of Cryptography (TCC) '05*, Springer LNCS 3378, pp. 325-341, 2005.
[49] Arunesh Mishra, Min Ho Shin, Nick L. Petroni, Jr., T. Charles Clancy, and William A. Arbaugh. Proactive key distribution using neighbor graphs. *Wireless Communications, IEEE*, vol.11, no.1, pp. 26- 36, Feb 2004, doi: 10.1109/MWC.2004.1269714
[50] Mohamed Kassab, Jean Marie Bonnin, and Karine Guillouard. Securing fast handover in WLANs: a ticket based proactive authentication scheme. *Globecom Workshops, 2007 IEEE*, vol., no., pp.1-6, 26-30 Nov. 2007, doi: 10.1109/GLOCOMW.2007.4437783
[51] Ralf Wienzek and Rajendra Persaud. Fast Re-authentication for Handovers in Wireless Communication Networks. Networking 2006: 556-567
[52] Chin-Chen Chang; Hao-Chuan Tsai; , "An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks," Wireless Communications, IEEE Transactions on Wireless Communications, vol.9, no.11, pp.3346-3353, November 2010, doi: 10.1109/TWC.2010.092410.090022
[53] Caimu Tang and Dapeng Oliver Wu. An Efficient Mobile Authentication Scheme for Wireless Networks. Wireless Communications, IEEE Transactions on Wireless Communications, VOL. 7, NO. 4, APRIL 2008, doi: 10.1109/TWC.2008.061080
[54] Wei-Bin Lee and Chang-Kuo Yeh. A new delegation-based authentication protocol for use in portable communication systems. Wireless Communications, IEEE Transactions on wireless communications, vol.4, no.1, pp. 57- 64, Jan. 2005, doi: 10.1109/TWC.2004.840220
[55] Felix von Reischach, Nouha Oualha, Alexis Olivereau, David Bateman, and Emil Slusanschi. “Scenario Definitions and their Threat Assessment”. TWISNet Deliverable D2.1, March 2011.
[56] D. Simon, B. Aboba, and R. Hurst. The EAP-TLS Authentication Protocol. Internet Engineering Task Force RFC 5216, March 2008
[57] F. Bersani and H. Tschofenig. The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method. Internet Engineering Task Force RFC 4764, January 2007.
[58] Z. Cao, H. Deng, Y. Wang, Q. Wu, and G. Zorn. EAP Re-authentication Protocol Extensions for Authenticated Anticipatory Keying (ERP/AAK), Internet Engineering Task Force Internet-Draft, October 18, 2011.
[59] P. Duffy, S. Chakrabarti, R. Cragie, Y. Ohba, and A. Yegin. Protocol for Carrying Authentication for Network Access (PANA) Relay Element. Internet Engineering Task Force RFC 6345, August 2011.
[60] Y. Ohba and A. Yegin Definition of Master Key between PANA Client and Enforcement Point. Internet Engineering Task Force RFC 5807, March 2010

[61] Z. Cao, H. Deng, Y. Wang, Q. Wu, and G. Zorn. EAP Re-authentication Protocol Extensions for Authenticated Anticipatory Keying (ERP/AAK), Internet Engineering Task Force Internet-Draft, October 18, 2011.
[62] S. Hartman, T. Clancy, and K. Hoeper. Channel Binding Support for EAP Methods. IETF Internet-Draft (work in progress) draft-ietf-emu-chbind-13.txt, January 10, 2012.
[63] M. Poturalksi, P. Papadimitratos, and J.-P. Hubaux. Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility. ACM ASIACCS, Tokyo,Japan, Mar. 2008, pp. 189–200.
[64] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen. Internet Key Exchange Protocol Version 2 (IKEv2). Internet Engineering Task Force RFC 5996, September 2010.
[65] P. Eronen. IKEv2 Mobility and Multihoming Protocol (MOBIKE). IETF RFC 4555, June 2006.
[66] Vasseur et. al., Routing Metrics used for Path Calculation in Low Power and Lossy Networks, IETF draft-ietf-roll-routing-metrics-19, IETF ROLL, March 2011
[67] Winter et. al., RPL: IPv6 Routing Protocol for Low power and Lossy Networks, IETF draft-ietf-roll-rpl-19, IETF ROLL, March 2011.
[68] A. Yegin and R. Cragie. Encrypting the Protocol for Carrying Authentication for Network Access (PANA) Attribute-Value Pairs. IETF RFC 6786, November 2012.
[69] H. Krawczyk and P. Eronen. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). IETF RFC 5869, May 2010.
[70] Naveen Sastry and David Wagner. 2004. Security considerations for IEEE 802.15.4 networks. In Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04). ACM, New York, NY, USA, 32-42.
[71] B. Aboba and M. Beadles, "The Network Access Identifier", IETF RFC 2486, January, 1999.
[72] “802.11f IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11™ Operation”, IEEE 2003.