Ashdin Publishing
International Journal of Sensor Networks and Data Communications
Vol. 1 (2012), Article ID 235548, 17 pages
doi:10.4303/ijsndc/235548

Research Article

A Survey on Measures for Secure Routing in Wireless Sensor Networks

Ansgar Kellner, Omar Alfandi, and Dieter Hogrefe

Institute of Computer Science, University of Göttingen, Germany
Address correspondence to Omar Alfandi, alfandi@cs.uni-goettingen.de

Received 13 February 2012; Revised 10 March 2012; Accepted 13 March 2012

Abstract In the near future, it is likely that wireless sensor networks (WSNs) become a major technology for the sensing in different application areas. One of the main challenges in WSNs is the secure routing of data through the network. This is resulting from the fact that WSNs are normally deployed in unattended or even hostile environments. While in last few years the routing approaches were mainly focussing on metrics such as robustness, energy preservation, etc., recently, different security solutions came to the fore that were taking also the security issues in WSNs into account. In this paper, different types of attacks on the routing layer of WSNs are investigated. Subsequently, measures for secure routing; including cryptography, key establishment, trust & reputation and secure localization; are reviewed, which were proposed by researchers in this area. Based on these findings, future prospects are discussed and final conclusions will be drawn.

Keywords wireless sensor networks; secure routing; WSNs

1 Introduction

Since years, the monitoring of areas of interest is a topic of great importance for civil as well as military applications, such as emergency scenarios, manufacturing environments, battle fields etc. Due to the advances in micro-electronics, highly integrated electronics and improved energy accumulators, in the last few years, the development of sensor nodes was intensified so that the sensor nodes got smaller and smaller, while the price per sensor went down at the same time. One of the major ideas was that the sensor nodes should form a collaborative wireless network to monitor events in arbitrary environments by acting in a self-configurable, self-organizing ad hoc manner, i.e. without the necessity of human interaction.

Due to the fact that the sensor's energy, in most cases a battery that should last for the sensor's lifetime, is strongly limited, the sensor nodes are constrained in their computational power, memory and transmission range. As a consequence, the nodes can neither perform computational intensive tasks nor deliver meaningful results by acting on their own. Therefore, the sensor nodes have to cooperate to be able to monitor bigger areas, aggregate measured values and transfer them to a point in the network were the data can be readout and evaluated.

One of the major research areas in WSNs is the routing of data packets from a source to a destination through the network. Because of the limited energy resources, energy is one of the primary design requirements for routing protocols in WSNs. To save energy the transmission range of each sensor is severely limited so that data packets that should be transmitted across the network have to be forwarded via multiple hops. Due to topology changes, interferences caused by environmental influences or adversaries, node failures or perishing energy resources, the routing has to be failure-tolerant and has to adapt permanently, while using as little energy as possible. With up-to-date routing information packets can be routed around critical areas so that a complete breakdown of the network can be avoided. Furthermore, the routing algorithm should take load balancing into account to avoid an overloading of certain nodes to reduce the risk of partitioning the network, leading to missing paths between the source and the destination. Moreover, the fusion of sensed data needs to be considered in WSN routing protocols to reduce redundant transmissions of the same data.

Although, the routing of data packets in WSNs is an essential service, which makes communication possible in the first place, security issues in the area of routing were mainly ignored. Instead, most of the current routing protocols aiming at metrics such as reliability, robustness, responsiveness and preserving energy. However, the non-consideration of possible security issues in the area of routing can be fatal because in almost all application areas in which WSNs are used, sensor nodes are deployed in hostile or unattended environments, providing the opportunity for adversaries to launch certain attacks against sensor nodes. Particularly, the capturing and compromising of nodes is a crucial problem because it is easy for adversaries to access the sensors physically.

In contrast to several other researches that dealt with general security issues of WSNs, *inter alia*; see, e.g. [8, 10,

68], in this paper security issues of WSNs with a special focus on the network layer will be discussed.

The remainder of the paper is organized as follows: in Section 2, the special characteristics of WSNs are discussed. In Section 3, the basic requirements for secure WSNs are presented and, afterwards, in Section 4, different types of attacks on WSNs, with a special focus on the network layer, are investigated. In Section 5, measures for secure routing in WSNs are discussed; including cryptography, key establishment, trust & reputation and secure localization; considering solutions proposed by other researchers in this area. Finally, future prospects of these security measures are discussed and conclusions will be drawn.

2 Characteristics of wireless sensor networks

In comparison to common wired or even today's wireless networks, Wireless Sensor Networks (WSNs) have certain characteristics that make them unique in terms of their offered features, but also in terms of the provided targets for adversaries. For that reason, the technical and architectural characteristics of WSNs are highlighted in the following section covering, on the one hand, the constraints of single sensor nodes and, on the other hand, the constraints of the overall WSN topology. Concluding, security considerations for the network layer in WSNs resulting from these characteristics are discussed. (see, e.g. [4,65,68])

2.1 Sensor node constraints

Memory limitation

The memory built into a sensor node is usually rather small (few KB). However, in general, about half of the memory is already used by the sensor's operating system. Among the most common OS for WSNs are TinyOS [63], Contiki [62], MANTIS [48], THINK [51], microC/OS-II [49] and nano-RK [16]. All further things, such as executable program code, buffered messages, routing tables etc. have to fit into the remaining memory.

Computational limitation

Also the computational power of the sensor nodes is severely constrained due to cost and energy-saving considerations. For that reason, most of the sensor nodes utilize weak processors with a clock-rate of 4–8 MHz such as Atmega128L [9] or MSP430 [13]. However, depending on the application area, in some cases, sensor nodes utilize stronger processors with a few hundred MHz, such as StrongARM [69] or SH4 [6], though at the expense of a shorter life-time of the nodes.

Power limitation

A sensor node has to economize with the shipped battery, i.e. the supplied energy must outlast the sensor's life. This is resulting from the fact that the sensor's battery can neither be replaced nor recharged, once deployed in a difficult to access area or hostile environment. The energy of a sensor node is consumed by mainly three essential components: the sensor unit, the communication unit and the computation unit. Because of the limited energy reserves, energy is often one of the primary metrics in WSNs routing algorithms [3]. Many operating systems for WSNs provide certain features to preserve energy [31].

Transmission range

To minimize the energy needed for communication it is very common that sensor nodes use a rather small transmission range. This results in the necessity of using multiple-hops to transfer data from a source to a destination node through a large network.

Physical accessibility

In comparison to wired networks, in which an attacker has to pass several physical lines of defence, such as gateways or firewalls, in WSNs an adversary can easily attack nodes because there are mostly deployed in an unprotected environment. Also additional physical threats, such as weather and radiation, can disturb the network.

2.2 Network constraints

Deployment uncertainty

Sensor nodes are normally deployed randomly and dynamically, i.e. there is no prior knowledge where the nodes will be located after their deployment and which node will be adjacent to which other nodes. However, after their deployment the sensor nodes should be self-organizing and self-configuring without further operator intervention.

Use of wireless links

The transfer in WSNs is not reliable because of the use of the wireless broadcast medium. In the wireless broadcast medium interferences can occur caused by environmental influences, adversaries or due to packet collisions. Furthermore, the communication between nodes is not limited on a peer-to-peer base, instead each packet is receivable for every node within the transmission range.

Latency

The packet-based multi-hop routing in WSNs increases the latency due to congestion in the network and the additionally required processing time. Besides, the routing process in WSNs is often causing delays: for example, if a routing algorithm uses different paths between a source and a destination to distribute the energy load, not always the shortest path is used so that additional delays are predictable.

Remote management

Due to the application area of sensor nodes in unattended environments, the sensor nodes have to be managed remotely after their deployment. For instance, in a military

scenario, in which the sensor nodes are placed behind enemy lines for reconnaissance, no direct access will be possible after deployment.

Network partitions

In a randomly deployed WSN it can happen that the network is divided into several sub-networks, so called network partitions, which are not able to communicate with each other. This issue can also occur after the deployment, if certain nodes are destroyed, run out of energy or move out of range.

Lack of a central management

In WSNs it is common that there is no special central facility that manages the network, instead entire WSNs work distributed, self-organizing and self-configuring on a peer-to-peer basis. This leads, on the one hand, to a very robust infrastructure with some kind of self-healing features, but on the other hand, additional challenges emerge.

Scalability

In general, a large amount of sensor network nodes are deployed to monitor certain areas. As a result, scalability has to be considered in the network protocols. It has to be ensured that the implemented mechanisms work the same way, no matter if there are just a few or a huge amount of sensor nodes.

Data aggregation

To obtain useful results from a WSN, the sensor nodes should not be considered individually, instead the monitored information should be aggregated to obtain more robust results and to preserve energy in the routing process at the same time.

Topology changes

Though, in most of the WSN scenarios the sensor nodes do not move, the topology of the WSN can change due to node failures resulting from hardware failures and battery depletion, but also based on outside influences such as environmental interferences or attacks.

2.3 Security considerations for the network layer

Both, the constraints of each single sensor node as well as the network constraints, do affect the security considerations on the network layer and thus, have to be considered:

First of all, the limited memory and the limited computational power of the sensor nodes have to be considered, when using certain security algorithms on the network layer. Most of the security algorithms that are state of the art on other devices, such as the "normal" public key cryptography, cannot be used on sensor nodes without adaptations due to energy limitations and performance issues. Particularly, cryptographic algorithms have to be optimized for sensor nodes considering less computations and a small number of keys as well as small key sizes. For that reason, many of the current cryptographic approaches in WSNs use symmetric key cryptography. However, currently there were a couple of researches that showed the usability of public key cryptography in WSNs under certain conditions (see, e.g. Section 5). Also hybrid cryptographic approaches can be an option, which try to combine the advantages of both approaches.

In general, the limited energy of the sensor nodes is a major concern for security mechanisms in WSNs. Thus, any additional computational and communication overhead for security measures needs to be kept as small as possible. From the security point of view, the limited energy provides adversaries with an additional target: an adversary could intentionally attack the sensors' power sources, e.g. by continuously requesting unnecessary routes to exhaust the nodes' batteries.

The use of multiple-hops, as consequence of the limited transmission range, provides adversaries with an additional target that needs to be considered in WSN routing protocols. For example, a compromised node on a path between source and destination enables adversaries to fabricate, replicate or modify data packets.

Moreover, adversaries with a higher transmission power can launch different types of attacks on the sensor nodes.

Lastly, the physical accessibility of network nodes has to be considered in WSNs. Because of the non-existent clear line of defence, each sensor node must be capable of defending itself against external threats. As a result, the relevant program code and particularly the secret keys have to be protected against physical attacks of adversaries. Although, tamper proof hardware could improve the situation, it is applied rather seldom due to the higher costs in comparison to algorithmic solutions.

The special network characteristics of WSNs does also strongly affect the security of routing in WSNs:

First of all, the deployment uncertainty has to be taken into account, particularly regarding the key distribution process, which is often needed for authentication and encryption to secure routing in the network. In some cases using pre-determined deployment patterns is an option, i.e. the sensor nodes can be pre-configured regarding their pre-determined neighbors.

Furthermore, the unreliable communication has to be considered for security measures because crucial data, such as cryptographic keys, have to be exchanged reliably. The security measures should be fault-tolerant so that temporary interferences do not make the entire system collapse. Besides, eavesdropping of the communication in the wireless medium should be prevented by suitable security measures.

If security measures are applied, it is obvious that further delays will be introduced. However, depending on the

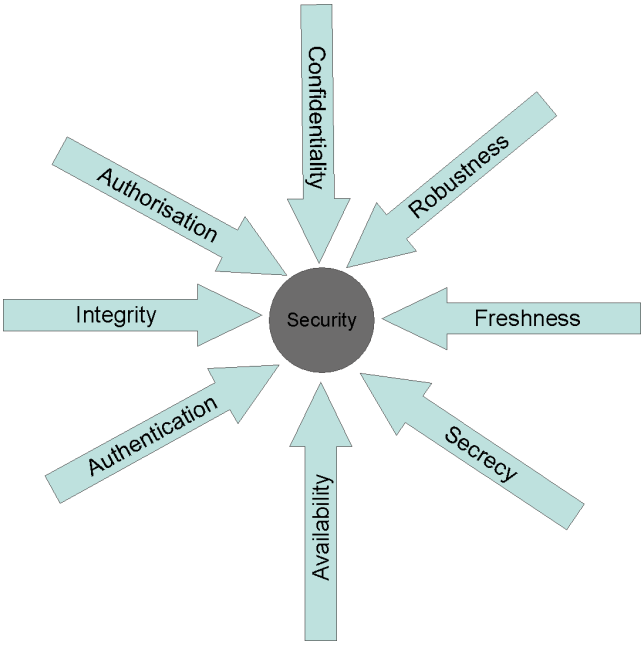


Figure 1: Basic security requirements in WSNs.

required level of security there must be a trade-off between the latency and the level of security.

From the security point of view, a possible partitioning of the network has to be considered: the security infrastructure should still be functional even if single nodes fail or cannot be reached any longer.

Due to the distributed nature of WSNs the applied security measures should ideally operate in a distributed manner. As a consequence, even multiple failing nodes or a partitioning of the network should not break the entire security infrastructure. Although, a distributed security solution may be more complex, the entire system would become more robust because a single point of failure is avoided.

Moreover, the scalability of the routing and the related security measures must be kept in mind: One of the main scalability challenges for the security of WSNs is the distribution of keys within the network, as basis for secure communication and authentication.

From the security point of view, the nodes that are aggregating information have to be protected particularly. Thus, the aggregation needs to be kept in mind for secure routing protocols, e.g. if the communication is protected by end-to-end cryptography, the data aggregation becomes more difficult because the aggregating intermediate nodes cannot directly access the data anymore.

Finally, the security measures have to be fault-tolerant and robust so that they will work even if the topology changes. Hence, security measures should work rather in a distributed fashion than relying on a certain node to avoid a single point of failure.

3 Basic security requirements in WSNs

To achieve secure routing in WSNs there are several basic security requirements that should be taken into account (see Figure 1) such as

- confidentiality;
- integrity;
- authentication;
- authorization/access control;
- availability;
- robustness;
- freshness;
- secrecy.

Ideally, all requirements should be considered, but it is more likely that because of latency issues or energy constraints a subset of those requirements is chosen, regarding the application area of the network and the level of security that should be complied. For a more detailed discussion of these basic requirements see [60,65,68].

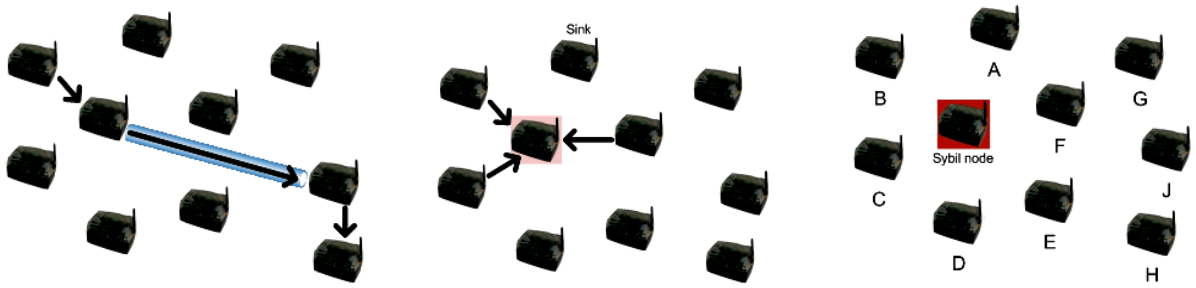
4 Attacks in WSNs

In the following section, first some basic types of attacks that can be launched in WSNs will be discussed. After that, a more specific look on WSN network layer attacks will be taken.

4.1 General types of WSN attacks

Basically, attacks on WSNs can be classified into one or more of the following categories (see, e.g. [60,68]):

- *Outsider vs. Insider attack*: in an outsider attack, a malicious node harms the WSN without being part of it. In contrast, in an insider attack the malicious node harms the WSN as (authorized) participant of the WSN.
- *Physical vs. Remote attack*: in a physical attack an adversary physically accesses the sensor node that should be harmed by tampering or destroying the sensor's hardware. In contrast, a remote attack is implemented from a (large) distance, e.g. by emitting a high-energy signal to interrupt the communication.
- *Passive vs. Active attack*: in a passive attack an adversary just eavesdrops or monitors the communication within the WSN. In contrast, in an active attack the adversary directly influences the communication in the WSN by modifying, fabricating or suppressing data packets.
- *Laptop-class vs. Mote-class attack*: a mote-class attack is an attack against a WSN that is implemented from a mote, i.e. the attacking device is of same type of hardware as the sensor nodes that should be attacked. In contrast, in a laptop-class attack, the adversary utilizes a device which is superior to the sensor nodes that should be attacked in terms of computational power and transmission power.



(a) Wormhole attack. (b) Sinkhole attack. (c) Sybil attack.

Figure 2: Attacks on the network layer.

4.2 Attacks on the network layer

There are several attacks that can be launched against the network layer in WSNs. Most of the attacks on the network layer can be classified in one of the following categories (see Figure 2):

- *Information disclosure*: disclosure of routing information by passive or active participation in the WSN.
- *Physical attack*: unauthorized access to sensor node through physical intervention.
- *Energy exhaustion*: intentional waste of energy resources by adversaries, e.g. by requesting unnecessary routes.
- *Denial of service*: flooding of the network with unnecessary routing requests.
- *Spoofed, altered or replayed routing information*: changing the routing behavior by spoofing, altering or replaying routing information.
- *Routing table overflow*: flooding of the routing table by creating multiple non-existing routes to make the routing algorithm collapse.
- *HELLO flood attack*: intentionally inject bogus HELLO messages to remote nodes to confuse the routing protocol.
- *Sybil attack*: creating a large number of pseudonymous entities to gain a greater influence on the network.
- *Sinkhole/Blackhole attack*: trying to obtain all network packets in a certain network area by "looking attractive" to surrounding nodes.
- *Wormhole attack*: making two nodes believe that they are neighbors by tunneling packets using a low latency link, though, in reality, they are far away from each other.
- *Selective forwarding*: forwarding only certain packets in the network to save resources, i.e. behaving selfishly.

For an in depth study of network layer attacks see [1,50, 54,68,77,78].

5 Measures for secure routing in WSNs

To improve the security of routing protocols in WSNs, various security measures can be applied. Although, most of the concepts are well-known concepts that were used in other areas of computer science for years, the special characteristics of WSNs have to be considered when applying them in WSNs. Furthermore, the emphasized basic security requirements as well as possible attacks that can be launched against WSNs should be kept in mind.

Based on these considerations, in the following, a selection of proposed security measures, which were recently discussed in the research community, is presented that can improve the security of WSN routing protocols.

5.1 Cryptography

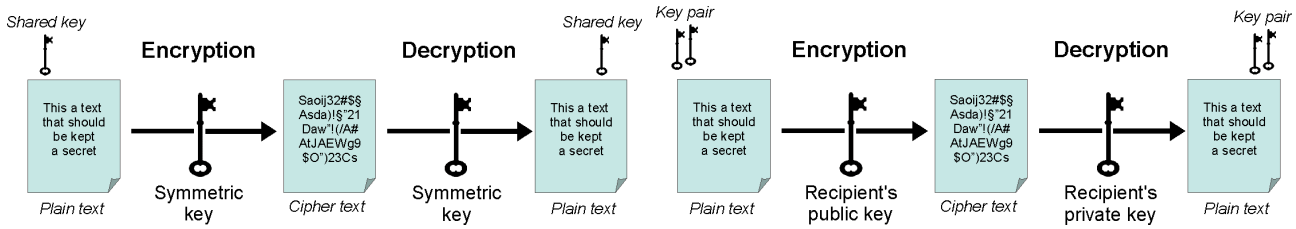
Often, cryptographic methods are utilized to meet the basic security requirements of confidentiality and integrity in networks. However, as mentioned before, sensor nodes are limited in their computational and memory capabilities so that the well-known traditional cryptographic techniques cannot be simply transferred to WSNs without adapting them.

Cryptography, as one of the main research focuses for securing WSN communication, affects several subtopics such as storage-efficiency and energy-efficiency. In the following, a short overview of current research topics in the area of WSN cryptography is given:

Symmetric cryptography

Since the beginning of the use of cryptography in the area of WSNs, the main focus was set on symmetric cryptography due to the assumption that symmetric cryptography has a higher effectiveness and requires less energy consumption, in contrast to public key cryptography (see Figure 3(a)). Therefore, there are several researches that deal with this topic:

Law et al. [38] investigate in their survey in the evaluation of block ciphers for WSNs, based on existing literature and authoritative recommendations. The authors do not only consider the security properties of the algorithms, but additionally they try to find the most storage- and energy-efficient ones. To compare the different block ciphers, benchmarks are conducted on the 16-bit RISC-based MSP430F149 considering different cipher



(a) Symmetric encryption.

(b) Asymmetric encryption.

Figure 3: Types of cryptography.

parameters, such as key length, rounds and block length; and different operation modes, such as cipher-block chaining (CBC), cipher feedback mode (CFB), output feedback mode (OFB) and counter (CTR). Based on a review of different cryptographic libraries, such as OpenSSL, Crypto++, Botan and Catacomb, most of the code was adapted from OpenSSL [72]. Ciphers without public implementations were implemented based on the original papers. For the compilation of the sources the IAR Systems' MSP430 C Compiler was used. The evaluation results of the conducted benchmarks show that the most suitable block ciphers for WSNs are Skipjack, MISTY1, and Rijndael, depending on the combination of available memory and required security level. As operating mode "Output Feedback Mode (OFB)" for pair wise links, i.e. a secured link between two peers, is suggested. In contrast, "Cipher Block Chaining (CBC)" is proposed for group communications, for example, to enable passive participation in the network.

Fournel et al. [27] investigate in their survey stream ciphers for WSNs. The chosen stream cipher algorithms (DRAGON, HC-256, HC-128, LEX, Phelix, Py and Pypy, Salsa20, SOSEMANUK) are all dedicated to software uses and were originally submitted to the European Project Ecrypt in the eStream call (Phase 2). To extend the selection of stream ciphers, the famous RC4, SNOWv2 and AES-CTR were considered for evaluation. The performed benchmarks on an ARM9 core based ARM922T aimed at finding the most storage-efficient and energy-efficient stream ciphers for this platform. Based on the methodology of the eStream testing framework [24], four performance measures were considered: encryption rate for long streams, packet encryption rate, key and IV setup, and agility. Furthermore, the code size required for each algorithm on the ARM9 platform was investigated. The used stream cipher algorithms, originally developed in C for the traditional PC platform, were executed on the ARM9 platform without any optimizations. The results of the benchmarks show that the stream ciphers Py and Pypy, the two most efficiently running algorithms on traditional PC platforms, do not work as fast on the ARM9 architecture. In contrast, SNOWv2, SOSEMANUK and HC-128 performed similarly fast on both platforms. For SOSEMANUK, the key setup was very huge in comparison to the key setup on the traditional PC platform.

Choi and Song [23] investigate the feasibility of various cryptographic algorithms for their use in WSNs, utilizing MICAz-type motes running TinyOS. The usage of resources including memory, computation time and power for each cryptographic algorithm were experimentally analyzed. As a result, RC4 and MD5 turned out as the most suitable algorithms for MICAz-type motes.

Passing and Dressler [53] verify with an experimental setup the runtime behavior of cryptographic algorithms (including AES) and hash-functions (including MD5 and SHA-1) for WSNs. The experimental setup consists of a PC running Linux connected to two BTnodes. The results show that for the hashing of arrays of different sizes MD5 outperforms SHA-1. The required time is linearly dependent to the amount of data. The overall results show that the examined cryptographic algorithms have high execution times (e.g. AES operation on a 1kByte array needs 1.67s).

Healy et al. [32] have a look on the benefits of using hardware encryption for symmetric encryption to reduce encrypting costs. Thus, the authors investigate the use of an AES encryption module that is available on the Chipcon CC2420 transceiver chip as used for MICAz and TmoteSKY nodes. In an experiment, three symmetric cryptographic algorithms were examined on MICAz and TmoteSKY nodes: AES (a hardware and a software variant), RC5 and Skipjack. The results show that the hardware version of AES outperforms the other algorithms in terms of using less memory, a decreased execution time and less power consumption.

Public key cryptography

Recently, there has been a change in the research community from symmetric cryptography to public key cryptography (see Figure 3(b)), which has been traditionally considered as computational too expensive for WSNs. Particularly, the emerging research field of *elliptic curve cryptography (ECC)* in WSNs seems to be a promising approach: in contrast to the common public key approaches, ECC is faster,

while reaching equivalent security with smaller keys at the same time. There are several researches that deal with the topic of public key cryptography in WSNs:

Gaubatz et al. [29] challenge the basic assumptions about public key cryptography in WSNs: instead of the common traditional software based approach, a hardware assisted public key approach is proposed which is based on optimized algorithms and associated parameters as well as low-power design. Two proof of concept implementations, the Rabin's Scheme and NtruEncrypt, which utilize a regular ASIC standard cell library, are presented to validate their approach regarding different metrics such as power consumption, throughput and level of security. The results show that public key cryptography with a power consumption of less than 20 μW is possible and therefore, it can be suitable for WSNs.

Lopez [47] draws a comparison between symmetric and public key cryptography for WSNs. Lopez highlights the aptitude of symmetric cryptography for WSNs due to its energy-efficiency, but also discusses the typical problems of symmetric cryptographic approaches, such as the pre-distribution of secret keys, which is a major problem especially in randomly deployed WSNs. Lopez investigates also the advantages of public key cryptography in terms of key management and authentication features, while not forgetting to emphasize the additional hardware and software requirements, which do not suit ideally to resource constrained sensor nodes. Moreover, the recent development of elliptic curve cryptography (ECC) and its promising use in WSNs is discussed. The general achievements in the area of public key cryptography in WSNs are underpinned by presenting public-key based solutions to WSN applications such as a hardware customization solution; an ECC-based key distribution solution for TinySec; an efficient software ECC-based implementation; and an end-to-end security architecture. Lopez expects further researches in the area of public key cryptography in WSNs and reminds to keep the evolution of WSN hardware in view.

Arazi et al. [7] describe the efficiency of public-key cryptography for WSNs and the corresponding issues that need to be considered. Particularly, ECC is highlighted as suitable technique for WSN which provides a good trade-off between key size and security.

Liu and Ning [41] also emphasize that ECC is one of the most efficient types of public key cryptography in WSNs. The steps of design, implementation and evaluation of TinyECC, a configurable and flexible library for ECC operations in WSNs, are presented. The library provides a number of optimization switches that can be combined according to the developer's needs for a certain application, resulting in different execution times and resource consumptions. The TinyECC library was also evaluated on several sensor platforms; including MICAz, Tmote Sky, and Imotel; to find the most computationally efficient and the most storage efficient configurations.

To improve the energy consumption of public key cryptography Gaubatz et al. [29,30] propose a custom hardware assisted approach using special purpose ultra-low power hardware implementations of public key algorithms to make public key cryptography feasible for WSNs. The authors conclude that the use of public key cryptography results in a lower protocol overhead, less packet transmissions and therefore, power savings. Furthermore, an in-depth comparison of three different public key cryptography implementations for WSNs is provided including Rabin's Scheme, NtruEncryptor and ECDSA/ECMV. The comparison considers the message payload; the cipher text; the time, average power and energy per message for encryption/decryption as well as signing/verification. The results show that due to its asymmetry Rabin's scheme is particularly suitable, if only encryption and signature verification are performed on the node. Ntru has the smallest average power consumption, but the largest message size. In contrast, ECC has a small message expansion for encryption and a high power consumption, but it requires the smallest number of packets. The overall result shows that the investigated public key cryptography algorithms are sufficiently fast and that the computational costs are within acceptable limits for the use in WSNs.

Hybrid cryptography

Both approaches, i.e. symmetric and asymmetric cryptography, can also be applied in combination to join the advantages of both approaches:

Pugliese and Santucci [56] discuss in their paper a novel hybrid cryptographic scheme for the generation of pairwise network topology authenticated keys (TAK) in WSNs, which is based on vector algebra in GF(q). For the ciphering and authentication model symmetric cryptography is used, while the key generation model is drawn on asymmetric cryptography.

Riaz et al. [57] propose in their paper a unified security framework with three key management schemes: SACK, SACK-P, and SACK-H. While SACK is based on symmetric key cryptography and SACK-P is based on asymmetric key cryptography, SACK-H uses a hybrid cryptography approach. SACK-H uses asymmetric cryptography during intra-cluster communication, whereas symmetric cryptography is used during inter-cluster communication. The evaluation of all key management schemes regarding different metrics, such as energy, resource utilization, scalability and resilience to node compromises, shows that SACK-P needs the most resources, but also provides the highest security level. In contrast, SACK needs the least resources, but provides the lowest security level. The

SACK-H, the hybrid approach, provides medium security with medium resource utilization.

Energy consumption

Another crucial topic is the energy consumption that is needed for cryptographic methods. Thus, many researches have been carried out in this area:

Wander et al. [66] quantify the energy cost of authentication and key exchange based on public key cryptography on an 8-bit Atmel ATmega128L low-power micro-controller. The two public key algorithms RSA and ECC are compared, considering mutual authentication between two parties. The results show that even software-based public key cryptography is feasible for an 8-bit micro-controller platform; however, ECC shows significant better results compared to RSA in terms of reduced computation time, amount of data that needs to be stored and transmitted. Consequently, ECC requires less energy than RSA.

Piotrowski and Peter [55] estimate the power consumption of the most common RSA and ECC operations, such as signature generation and verification, as well as the involved transmissions on common sensor platforms such as MICA2DOT, MICA2, MICAz and TelosB. The results of the experiment show that public key cryptography does not influence the sensors lifetime significantly, so that strong cryptography can be seen as feasible for WSNs. The authors claim that compared to the computational power, the transmission power is very low. However, because of the multiple hop architecture, the keys that need to be exchanged should be kept small and hardware accelerated cryptographic computations should be considered to reduce the overall energy consumption in WSNs.

Batina et al. [12] propose a low-cost public key cryptography scheme for WSNs providing services such as key distribution and authentication. To minimize the power consumption a hardware assisted approach is suggested implementing ECC. The used low-power ECC processor contains a modular arithmetic logical unit (MALU) for ECC field arithmetic. With an assumed operating frequency of 500 kHz the power stays between 20 and 30 μW, so that the authors conclude that public key cryptography, particularly ECC, is feasible for the use in WSNs.

Data aggregation

Moreover, as mentioned before, the interaction of data aggregation and cryptographic methods has to be coordinated. There are some researches that focus on this topic:

Castelluccia et al. [17] concentrate on the efficient additive aggregation of encrypted data in WSNs without decrypting them. The authors propose a homomorphic encryption scheme that allows an efficient aggregation of encrypted data using only one modular addition for cipher text aggregation. The security scheme is based on a standard cryptographic primitive, the indistinguishability property of a pseudo-random function (PRF). The approach provides a strong level of security, in contrast to end-to-end encryption without aggregation. Compared to hop-by-hop aggregation, the new scheme is less bandwidth efficient; however, the privacy level is much stronger than a naïve aggregation scheme using hop-by-hop decryption. Moreover, the communication load is distributed quite evenly among the nodes, resulting in a longer overall network lifetime. Additionally, an end-to-end aggregate authentication scheme, also based on the indistinguishability property of PRFs, is introduced to protect the integrity of the aggregated data against outsider-only attacks.

Wang et al. [67] propose a joint data aggregation and encryption scheme for efficient and secure data transmission in clustered WSNs. The optimal intra-cluster rate allocation problem is considered using the Slepian-Wolf theorem so that the overall energy of all nodes in a cluster, which is required to send encoded data, is minimized. Based on the Slepian-Wolf coding, a novel encryption mechanism, called spatially selective encryption, is introduced for each cluster. The members of each cluster send their data without encryption to the cluster head, while the cluster head encrypts its data to protect the members' data. The simulation results show that the new approach significantly improves the energy-efficiency in data transmission while providing a high level of security.

Ozdemir and Xiao [52] provide a comprehensive overview on secure data aggregation in WSNs. The authors present a taxonomy of secure data aggregation protocols based on current "state-of-the-art" work in this research area. Moreover, open research areas and future research directions for secure data aggregation concepts are discussed.

Existing secure routing protocols for WSNs

Based on these different security aspects some comprehensive routing protocols can be found in the research community that make use of encryption to protect the communication between the nodes in WSNs:

Ibriq and Mahgoub [36] present SHEER, a secure hierarchical energy-efficient routing protocol, which provides secure communication at the network layer. To improve the network energy performance and lifetime a probabilistic broadcast mechanism and a three level hierarchical clustering architecture is used. To secure the routing mechanism from the inception of the network, SHEER implements HIKES, a hierarchical key management and authentication scheme. The simulation results show that SHEER is more energy-efficient and better scalable than secure LEACH using HIKES.

Xiao et al. [70] introduce a secure extension for the SPIN protocol [33], a data centric routing protocol for

WSNs. To make the original SPIN protocol more secure, secure-SPIN uses cryptographic functions that require only small memory and little processing power. The authors claim that secure-SPIN increases the data communication security in WSNs.

Cheng et al. [22] propose a secure routing algorithms for WSNs based on curve-based greedy routing (CBGR) algorithm [75] and a suitable encrypting algorithm. Each forwarded packet is encrypted using a different key. The analysis of the new algorithm shows that in comparison to Direct Diffusion (DD) [37] and LEACH [34], the proposed algorithm has lower complexity, while assuring security to some extent.

Ali and Fisal [5] improve the existing routing protocol SRTLD [2]; which depends on optimal forwarding decision taking the link quality, packet delay time and the remaining power of next hop sensor nodes into account; by enhancing its security using encryption with authentication of the packet header. The proposed security measures counteracts HELLO flooding and selective forwarding attacks. The simulation results show that only about 216 bytes are required for the security mechanism and that the additional execution time is only 4.2 ms for one hop.

5.2 Key establishment

For almost all cryptographic methods some sort of key is required, but the question in WSNs is: how can these keys be established efficiently between randomly deployed sensor nodes? The well-known key exchange protocols, such as the Diffie-Hellman key exchange protocol, can often not be used due to the limited computational power and memory of the sensor nodes. Furthermore, the scalability of the key establishment protocol has to be kept in mind because normally hundreds or even thousand of nodes should cooperate in a WSN.

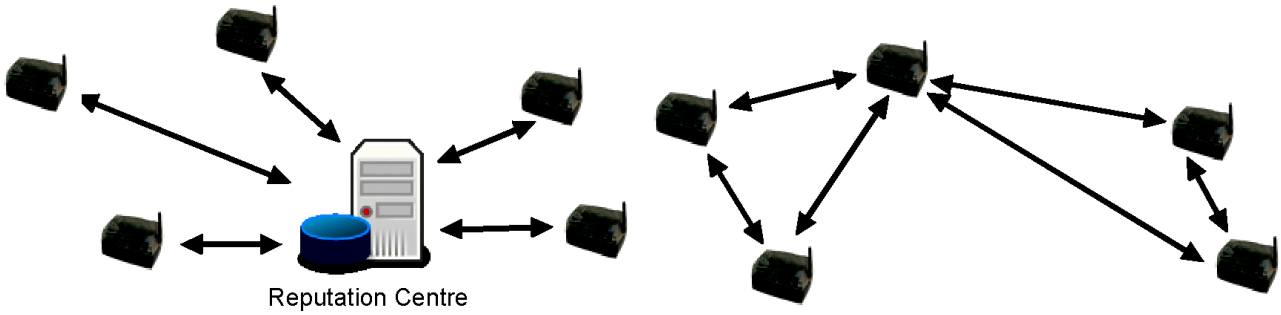
In the area of key establishing protocols various approaches can be found—in the following a few examples of current researches are discussed:

Chan and Perrig [18] addresses the lack of scalability of existing symmetric key distribution protocols by introducing "trusted intermediaries for key establishment" (PIKE), a new key-distribution scheme. The basic idea of PIKE is to use peer sensor nodes as trusted intermediaries to establish shared keys between nodes. Each node shares a unique pairwise key with a subset of other nodes in the network. The keys are deployed in a special way so that every two nodes A and B can find some node C in the network that shares a unique pairwise key with A and B. As a result, node C can be used as secure intermediary to establish a key between A and B. As along as C is not getting compromised, the established key is secure. Different extensions and parameters can be used to configure the trade-off between communication, memory and the level of security. The authors tested two configurations PIKE-2D and PIKE-3D: While PIKE-2D offers higher resilience against node capture, PIKE-3D is less resilient against active attacks, but achieves lower communication and memory overhead. The authors show that the communication and memory overheads of PIKE scale sub-linearly ($\mathrm{O}(n)$) with the number of nodes in the network. Moreover, PIKE uses a uniform communication pattern for key establishment, which is more difficult to attack for adversaries. Besides, in contrast to random-key pre-distribution mechanisms, in PIKE any two nodes in the network can establish a key.

Liu et al. [44] develop a general framework for establishing pairwise keys between sensor nodes using bivariate polynomials. The authors present two efficient instantiations of a general framework: a random subset assignment key pre-distribution scheme and a hypercube-based key pre-distribution scheme. The random subset assignment scheme generates a pool of random bivariate polynomials and assigns a subset of bivariate polynomials from the pool to each sensor node. As a result, there is a unique key for each pair of sensor nodes. In contrast, the hypercube-based scheme arranges polynomials in a hypercube space and assigns each sensor node to a unique coordinate in this space. Based on the coordinate in the hypercube, each node can identify the nodes it can directly establish a pairwise key with and the nodes that require an intermediate node to establish a pairwise key. The analysis of the schemes shows that both provide a high probability to establish pairwise keys, while tolerating node captures. Both schemes require only a little storage and the communication as well as the computation overhead is rather low. The two schemes were implemented and tested on MICA2 nodes running TinyOS. The simulation results show that the proposed schemes can be efficiently used in WSNs.

Unlu et al. [64] present a new practical deployment model in which the sensor nodes are deployed continuously over a line, one by one. To cover a two dimensional area, the sensors can be deployed over multiple parallel lines. On top of this deployment model two key distribution schemes are presented that make use of the deployment knowledge. The analysis and results of the simulations show that, in comparison to the approach of Du et al. [25], in which nodes are deployed in groups, the new key distribution schemes perform better in terms of connectivity, resiliency, memory and communication costs.

A novel random perturbation-based (RPB) scheme is proposed by Zhang et al. [76]. The scheme guarantees that any two nodes can directly establish a pairwise key without exposing any secret to other nodes. Even if some nodes are compromised in the network, the non-compromised nodes remain secure by the pairwise keys. The scheme provides low computational and communication overhead and adapts to network changes. The analysis and evaluation with a



(a) Centralized trust exchange with a reputation center.

(b) Decentralized trust exchange by forming a web of trust.

Figure 4: Types of trust exchange.

prototype implementation on MICA2 nodes shows that the RPB scheme is highly secure and efficient, while requiring only low storage. As a result, it is suitable for the current generation of sensor nodes.

Yu et al. [73] propose a constrained random perturbation vector-based (CRPV) pairwise key establishment scheme and a variant, the CRPV+ scheme for WSNs. The new CRPV+ scheme satisfies all requirements of the described "versatileness criteria." The versatileness criteria includes the five requirements for a key establishment scheme stated by Zhang et al. [76] (Resilience to large number of node compromise, guaranteed key establishment, direct key establishment, resilience to network topology, efficiency) plus the two additional requirements of scalability and independence to hardware, which were added by the authors. In comparison to RPB, CRPV+ has less computation and communication overhead of hash values. Moreover, CRPV+ provides a better scalability because of the non-existence of special ID constraints.

Huang et al. [35] derive two probability models to design and analyze pairwise key establishment schemes for large-scale sensor networks. The new model applies the binomial distribution as well as a modified binomial distribution and analyzes the key path length in a hop-by-hop fashion. The models enable designers to analyze the pairwise key establishment phase by studying the key graph connectivity as well as the path length. The results of the systematic validation of the two models show their robustness.

Liu et al. [43] introduce a framework for a group-based deployment model to improve the performance of key pre-distribution in WSNs. In this model, sensor nodes are required to be deployed in groups so that sensor nodes in the same group are close to each other after their deployment. Two instantiations of this framework, a hash key-based scheme and a polynomial-based scheme, are presented: the results of the evaluation show that the proposed schemes work efficiently.

5.3 Trust and reputation

Due to compromised sensor nodes or node failures the correctness of measurements and routing issues cannot be verified. By introducing a trust and reputation system this problem can be tackled: the huge number of sensor nodes can cooperate in a collaborative manner trying to find out what is wrong or right in terms of the nodes' behaviors. Either a centralized or a decentralized trust exchange can be used to exchange the trust values between the nodes (see Figure 4). Based on a trust and reputation system, further decisions can be made such as finding a better, more trustworthy routes or isolating misbehaving sensor nodes.

Although, this idea has been considered in related areas, such as ad hoc networks and peer-to-peer networks, for while, trust and reputation systems in WSNs just caught recently the researchers' attention. In the following, a few of those approaches are discussed:

Srinivasan et al. [61] propose a novel reputation-based scheme, called distributed reputation-based beacon trust system (DRBTS), for excluding malicious beacon nodes, which provide false location information, in the network. Every beacon node monitors its 1-hop neighbors for misbehavior and updates its reputation table correspondingly. To share the knowledge, each node publishes its reputation table to its 1-hop neighbors. If a deviation test is passed, the obtained second hand information is used to update the reputation table. Based on a simple majority scheme, each node can decide whether to use the information of certain beacon nodes or not. The results of the simulations show that the scheme works robustly in dense networks and that it can be adapted to certain application domains.

Chen et al. [21] propose a reputation-based trust system based on probability, statistics and mathematics analysis. The new term of "certainty" is introduced to emphasize that positive or negative outcomes for a certain event are not enough information to make a decision in WSNs. The authors build up a reputation space and trust space and

define a corresponding transformation from the reputation to the trust space. Moreover, some important properties about the relationship among positive outcomes, negative outcomes, total outcomes, positive trust, negative trust and certainty both in reputation space and trust space are discussed. However, the proposal is rather theoretical so that there is no implementation and therefore, no experimental results.

Boukerch et al. [14] propose a novel agent-based trust and reputation management scheme (ATRM) for clustered WSNs with backbone. The new scheme effectively manages trust and reputation locally with minimal overhead in terms of extra messages and time delay. Each node in the network stores its own trust and reputation information—due to the fact that a node cannot create its own trust and reputation values the procedure is as follows: Each node holds a mobile agent that is responsible of administrating the node's trust and reputation. Before a transaction between two nodes can take place, the mobile agent of the requester is sent to the provider node to obtain a certificate. Based on this certificate a decision is made whether the transaction will take place or not. After the transaction, the requester creates an evaluation of the obtained quality of service for the transaction. This evaluation value is sent via the requester's mobile agent to the provider's mobile agent. Based on the collected evaluations a mobile agent periodically issues an updated certificate. The experimental results show that ATRM has low latency and requires minimal overhead so that it is feasible for the use in WSNs.

Ganeriwal et al. [28] investigate a generalized and unified approach for providing information about the data accuracy in WSNs, the so called Reputation-based Framework for Sensor Networks (RFSN). The authors present a trust and reputation system middleware for WSNs in which sensor nodes form a community of trust based on reputation metrics. Each sensor node maintains reputation metrics about the other nodes. A Bayesian formulation (beta reputation system) is used to compute the reputation of each node, considering the past behavior as well as the possible future behavior of the nodes. The middleware was ported to the WSN operating systems TinyOS and SOS and tested in different contexts, i.e. on MICA2 motes in a test-bed, with simulations using the Avrora network simulator and with real sensor data collected in James Reserve. The results show that the memory and the energy overhead of the new reputation system middleware is low.

Chen et al. [19] propose the new protocol ETSN to construct an event-based trust framework model for WSNs. The model contains two types of nodes: the agent nodes and the sensor nodes. Each agent node monitors the behavior of sensor nodes within its radio range. Based on the monitored data, the agent computes the trust rating and then, broadcast it. The trust rating is event-related, i.e. the agents distinguish several trust ratings—one trust rating for each event. All sensor nodes, which are within the agent's radio range, receive the trust rating and update their trust rating value. On the basis of the updated trust rating a decision is made whether to cooperate or not. The simulation results and analysis show that ETSN is fast in detecting malicious nodes and scales well. Furthermore, ETSN can also distinguish trust ratings of different events. In comparison to the other examined schemes ATSN [20] and RFSN [28], ETSN is more suitable for WSNs.

Shaikh et al. [59] investigate the energy consumption of reputation-based trust management schemes. The authors propose the Generic Communication Protocol (GCP) that can be used to exchange trust values. Based on GPC, a theoretical energy consumption analysis and evaluation of three state-of-the-art reputation-based trust management schemes (GTMS [58], RFSN [28] and PLUS [71]) for WSNs are presented. The results show that GTMS consumes less energy compared to PLUS and RFSN for the tested peer recommendation scenario.

Under the EU-funded seventh framework (FP7) within the AWISSENET project [11], Zahariadis et al. [74] propose Ambient Trust Sensor Routing (ATSR), a new secure routing protocol, which relies on a distributed trust model considering direct and indirect trust. ATSR adapts the geographical routing principle to cope with large network dimensions. For a better load balancing and network lifetime, the remaining energy of each neighbor is taken into account for the routing decision. The simulation results show that significant energy is consumed for routing and trust purposes and thus, the frequency of exchange of this information should be very well considered.

5.4 Secure localization

Securing the localization of sensor nodes is a requirement for secure location-based routing algorithms. The securing is necessary for two reasons: on the one hand, each sensor node should be capable of determining its own position accurately, even in a hostile environment; and, on the other hand, compromised nodes should be thwarted to announce false location information in the network. Secure location-based routing can be used against wormhole attacks and Sybil attacks.

In the area of secure localization various researches were conducted:

Liu et al. [42] introduce a suite of techniques to detect and remove compromised nodes that supply misleading location information in order to protect location discovery services in WSNs. A simple method is proposed to detect malicious beacon signals and additionally, methods for detecting replayed beacon signals are investigated to avoid false positives. Moreover, a method is presented that enables the base station to reason about the suspiciousness of beacon nodes and revoke them accordingly. The results show that

the presented techniques are practical and effective to detect malicious beacon nodes in WSNs.

Lazos et al. [40] propose a robust localization system, called Robust Position Estimation (ROPE), that allows sensors to estimate their own location without the assistance of a central authority. Moreover, ROPE provides a location verification mechanism that aims at the verification of the locations claimed by the sensors, before any data is gathered. The proposed approach is resistant against attacks such as wormhole attack, node impersonation etc. The introduced metric "Maximum Spoofing Impact," which is used to evaluate the impact of possible attacks, applied on ROPE shows that ROPE limits this metric even for low density deployment of reference points.

Another approach by Lazos and Poovendran [39], called SeRLoc, proposes a novel distributed range-independent localization algorithm based on a two-tier network architecture. The algorithm allows sensor nodes to passively determine their location in an untrustworthy environment without interacting with other nodes. In an analytical evaluation the probability of sensor displacement due to security threats, such as wormhole attack or Sybil attack, is investigated. The results of the simulation show that, in comparison to other state-of-the-art range-independent localization schemes, SeRLoc localizes sensors with higher accuracy, but with fewer reference points and lower communication overhead. As a result, SeRLoc outperforms the other compared schemes.

Capkun and Hubaux [15], analyze the resistance of positioning techniques to position and distance spoofing attacks. Afterwards, the authors propose a mechanism, called Verifiable Multilateration (VM), for secure positioning of wireless devices. VM enables the secure computation and verification of node positions in the presence of attackers. With SPINE (Secure Positioning In sensor NEtworks), a system for secure positioning in a network of sensors is proposed, which is based on VM. The results of the simulation show that SPINE resists against distance modification attacks from a large number of attacker nodes.

A further work by Liu et al. [45] deals with two methods to tolerate malicious attacks against range-based location discovery in WSNs. The first method filters malicious beacon signals based on "consistency" among multiple beacon signals. In contrast, the second method tolerates malicious beacon signals by adopting an iteratively refined voting scheme. The EARMMSE scheme with incremental evaluation as well as the voting-based scheme are working both effectively. The results of the field experiment with MICAz nodes as well as the simulation show that the proposed EARMMSE scheme with incremental evaluation is the most suitable for the investigated sensor platforms.

A statistic location verification algorithm for randomly deployed sensor networks is proposed by Liu et al. [46]. Three types of different node roles are defined: the claimer, the witness and the verifier. While the claimer broadcasts the position message, the witnesses rebroadcast it and reports the distance as well as the lowest hop information to the verifier. Finally, the verifier decides, based on a χ-test, whether the claimer reported its location correctly or not. The results of the simulation show that the probability for claiming a correct location is more than 80% , while the probability for claiming a faked position is less than 40% in average. As future work, the investigation into counter measures against Sybil attacks is suggested.

Ekici et al. [26] propose a secure probabilistic location verification method for randomly deployed dense sensor networks. The proposed algorithm, called Probabilistic Location Verification (PLV), leverages the probabilistic dependence of the number of hops a broadcast packet traverses to reach a destination and the Euclidean distance between the source and the destination. A small set of verifier nodes determine the plausibility of the claimed location, represented by a real number between zero and one. Based on the plausibility metric an arbitrary amount of trust levels in the claimed location can be created. The results of the simulation show that the proposed algorithm has a high accuracy and effectiveness. Therefore, PLV is feasible as light-weight location verification system for WSNs.

5.5 Future prospect

In this section, the future prospects of the investigated research areas regarding secure routing will be discussed:

The presented researches about *symmetric cryptography* confirm the assumption that most of the well-known symmetric cryptographic algorithms from the traditional PC platform cannot be directly applied to the sensor platform due to its specific constraints.

As a result, in the future, either light-weighted symmetric cryptography algorithms have to be developed or the existing solutions have to be adapted so that they can run more efficiently on the sensor network platform. Nonetheless, symmetric cryptography provides good results on sensor nodes due to its modest computation and memory requirements. Although, most of the researchers give some sort of recommendation, which algorithms to use, it is difficult to compare the different approaches because of the variety of used sensor platforms. As a consequence, as future work, the different symmetric cryptographic algorithms should be compared on a common platform to find the most suitable approach for the chosen platform.

Although, *public key cryptography* for WSN was neglected for a long time, recent researches show its aptitude for WSNs, particularly in terms of an increased level of security. One of the most promising approaches seems to be the elliptic curve cryptography (ECC), which is offering a

good trade-off between the required resources, such as little key size, and the level of security. If the permanent use of public key cryptography still is a too great burden, a *hybrid cryptography* approach may be worth considering.

If encryption is used, always the energy consumption should be kept in mind because encryption causes additional costs in terms of computation, storage and transmission. As stated before, the algorithms that should be used on a sensor platform have to be chosen carefully and have to be optimized in respect of the used hardware to achieve optimal efficiency. For the energy consumption always the overall energy consumption should be borne in mind, i.e. in this case not only the encryption itself, but also the related key setup and needed communication overhead.

Often *hardware assisted approaches* are proposed for both, symmetric as well as public key cryptography, to improve the efficiency. In general, a hardware assisted approach leads to better performance, efficiency and thus, energy savings. However, if additional hardware is required the costs per unit will increase so that the cost-benefit ratio has to be considered for huge amounts of sensor nodes. Besides, special hardware is mostly limited to certain cryptographic algorithms. Nevertheless, special encryption hardware is a promising approach, which can reduce the additional computational costs significantly, so that especially the more computational expensive public key cryptography can benefit from it.

Also the special requirement of data aggregation in the WSN has to be considered regarding the encryption of data: The secure end-to-end cryptography is mostly not feasible because intermediate nodes cannot access the data to aggregate it. Therefore, encryption mechanisms for WSN have to consider this special requirement in WSNs to enable in-network aggregation.

There are several proposed routing algorithms for WSNs that make use of encryption techniques to protect the communication between the nodes in the network. However, the situation is ambiguous because different approaches choose different algorithms on different platforms so that no recommendation can be given.

The *key establishment* in WSNs is crucial as a basis for a lot of security services based on cryptographic measures. However, the limited storage on the sensor nodes as well as the random deployment of the sensor nodes makes the key establishment in WSNs difficult. Furthermore, existing approaches, particularly centralized approaches are not really suitable for WSN so that they should not be transferred directly to the area of WSNs without modifications.

One of the proposed ideas to ease the key establishment between sensor nodes, is to create deployment models that determine *a priori* the location of each sensor node in the network. As a consequence, the nodes at certain locations know their neighbors in advance so that corresponding keys can be assigned by pre-distribution. However, such a deployment model makes the positioning of the sensors inflexible: the grouping and the deployment order of the nodes have to be determined in advance, the keys have to be distributed correspondingly and the deployment has to be executed exactly according to the previously planned topology. Furthermore, the subsequent integration of additional nodes to an existing network is complicated. As a result, this sort of deployment models can only be used for certain application scenarios.

One of the latest and promising research developments is the key establishment based on probabilistic models: in this area, there are still a lot of open research questions and open issues left to reduce the probability of neighboring nodes that cannot communicate due to missing keys.

The robustness of the key establishment is also an important factor, because node failures, environmental interferences as well as attacks might prevent a correct key establishment between certain nodes. As a result, the key establishment should work rather in a distributed fashion and should not rely on certain nodes.

Due to the fact that the energy of the sensor nodes is limited, the energy requirements for the key establishment process have to be kept as small as possible so that extra storage and communication overhead should be minimized.

Finally, it has to be remarked that the key establishment is obviously strongly connected to the cryptographic measures that should be used in the WSN. Therefore, the key establishment has to be optimized regarding the cryptographic requirements creating as little overhead as possible.

The idea of *trust and reputation*, i.e. using the experiences and observation of other nodes to find out whether a certain node is trustworthy or not, has been proposed in many different ways in the related area of P2P and ad hoc networks. However, to use a similar approach in a WSN its special characteristics have to be considered: for example, in a WSN all nodes are normally deployed by the owner of the network so that "selfishness," a common problem in ad hoc or P2P network, is non-existent.

If second hand information is used by the system, i.e. observations of other nodes are considered, an efficient distribution of this information has to be ensured. There are several ideas starting from using agents to transport trust and reputation information, to sharing trust and reputation information only locally in the neighborhood, to sharing this information just with the base station. However, with the sharing of information, adversaries are provided with a new target: for instance, several colluding compromised nodes can use bad-mouthing or praising to manipulate the system.

Furthermore, the decision making process, i.e. to decide who is trustworthy and who is not, offers several opportunities: from simple majority schemes to complex statistical

Reference	Cryptography	Centralized/decentralized	Energy consumption	Simulation/implementation	Comments
[23,27,32,38,53]	Symmetric	n/a	Considered	Implemented	Block cipher, stream cipher
[12,29,30,41,47,55,66]	Asymmetric	n/a	Considered	Implemented, n/a, implemented	—, comparison available
[56,57]	Hybrid	n/a	Considered	—	—, comparison available
[17,67]	Data aggregation	n/a	Considered	Implemented, simulated	—
[5,36,70]	Secure routing	Decentralized, —, —	Considered	Simulated, implemented, simulated	—
Reference	**Key establishment**	**Key distribution**	**Energy consumption**	**Simulation/implementation**	**Comments**
[18,43,44,64,73,76]		Pre-distributed	Considered	Implemented	—
Reference	**Trust and reputation**	**Centralized/decentralized**	**Second hand/first hand**	**Simulation/implementation**	**Comments**
[14,19,28,59,61,74]		Decentralized	First and second hand	Simulated, implemented, implemented, simulated	—, energy considered, —, —, energy considered
Reference	**Secure localization**	**Centralized/decentralized**	**Verification/localization**	**Simulation/implementation**	**Comments**
[15,26,39,40,42,45,46]		Centralized, decentralized	—, verification	Implemented, simulated	Detect and remove compromised nodes, —, passive localization

Table 1: Secure routing mechanisms in WSN.

schemes everything is possible. Also the question "What factors to consider?" and the weighting of the factors. In this area a lot of future work can be conducted.

A further question is how to react to a misbehaving node. Counter measures, such as excluding the node, need to be discussed as well as the mistakenly exclusion of nodes due to temporary environmental interferences.

Another open research question is how long these different types of systems need to be equilibrated to be fully functional after the deployment.

However, as already indicated, with the introduction of a trust and reputation system, the system itself becomes a target so that the vulnerability of this type of system should also be addressed in future researches.

The *secure localization* of the sensor nodes enables routing algorithms to work more reliable due to the knowledge of correctness of node positions. In the area of secure localization there are several researches and approaches that seem to work well so that common attacks, such as Sybil attack or wormhole attacks, can be identified. However, some of the approaches are specialized on detecting certain attacks so that in the future these mechanisms should be extended to be resilient against more types of attacks at the same time.

6 Conclusion

For a long time, the monitoring of events in certain areas has been in the research focus of the civilian as well as the military sector. In the last few years, the miniaturization of electronic components has accelerated the development of sensors for WSNs rapidly so that the devices could get smaller and smaller, while their performance as well as their energy-efficiency could be improved.

One of the crucial services that is required in WSNs to make the sensor nodes cooperate and communicate is the routing protocol. Until now most of the developed routing protocols for WSNs were mainly focused on common network metrics such as throughput, energy preservation, robustness—while security measures have mainly been ignored. However, ignoring security measures for WSN routing protocols is negligent because WSNs are often deployed in unattended or hostile environments in which private data and communication need to be secured.

For that reason, in this paper several security issues have been discussed that affect the routing in WSNs. As highlighted, traditional security measures cannot be transferred directly to the area of WSNs without adaptations so that novel security approaches have to be developed that take the special characteristics of the sensor nodes, the basic security requirements of WSNs as well as the possible attacks on WSNs into account. Four major related areas for secure routing were identified and discussed including cryptography, key establishment, trust and reputation and secure localization. For each area, several current researches were presented and open questions as well as future research were emphasized. An overview of the considered approaches is shown in Table 1.

Due to the complexity and variety of the presented security solutions the "one" solution that solves all problems cannot be recommended: depending on the application area in which the WSN should be deployed, security measures have to be carefully chosen to find a balance between a sufficient level of security and using as little resources as possible to increase the lifetime of the sensors.

Although, this paper focused specifically on the security of the network layer in WSNs, the other layers and particularly their points of contact should be kept in mind. A holistic view of WSN security should be considered in future researches to keep the special features of each layer in mind, while not forgetting their vulnerabilities. Nonetheless, security in the area of WSNs still provides a

huge research area that needs to be explored in the future to find optimal solutions that provide high security, while using as little resources as possible.

References

[1] N. Ahmed, S. S. Kanhere, and S. Jha, *The holes problem in wireless sensor networks: a survey*, ACM SIGMOBILE Mobile Computing and Communications Review, 9 (2005), 4–18.

[2] A. Ail, R. A. Rashid, S. H. F. Arriffian, and N. Fisal, *Optimal forwarding probability for real-time routing in wireless sensor network*, in Proc. of the IEEE International Conference on Telecommunications and Malaysia International Conference on Communications (ICT-MICC '07), Penang, Malaysia, 2007, 419–424.

[3] K. Akkaya and M. Younis, *A survey on routing protocols for wireless sensor networks*, Ad Hoc Networks, 3 (2005), 325–349.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, *Wireless sensor networks: a survey*, Computer Networks, 38 (2002), 393–422.

[5] A. Ali and N. Fisal, *Security enhancement for real-time routing protocol in wireless sensor networks*, in Proc. of the 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN '08), Surabaya, East Java, Indonesia, 2008, 1–5.

[6] F. Arakawa, O. Nishii, K. Uchiyama, and N. Nakagawa, *SH4 RISC multimedia microprocessor*, IEEE Micro, 18 (1998), 26–34.

[7] B. Arazi, I. Elhanany, O. Arazi, and H. Qi, *Revisiting public-key cryptography for wireless sensor networks*, Computer, 38 (2005), 103–105.

[8] F. Armknecht, A. Hessler, J. Girao, A. Sarma, and D. Westhoff, *Security solutions for wireless sensor networks*, in Proc. of the 17th Wireless World Research Forum Meeting, Heidelberg, Germany, 2006.

[9] I. Atmel, *ATmega128L datasheet, 8-bit microcontroller with 128K bytes in-system programmable flash*, Cited on, (2006), 9.

[10] S. Avancha, J. Undercoffer, A. Joshi, and J. Pinkston, *Security for wireless sensor networks*, in Wireless Sensor Networks, C. S. Raghavendra, K. M. Sivalingam, and T. Znati, eds., Kluwer Academic Publishers, Norwell, MA, 2004, 253–275.

[11] AWISSENET Consortium, *AWISSENET (Ad-hoc personal area network & WIreless Sensor SEcure NETwork)*. Available online: http://www.awissenet.eu/home.aspx, 2010.

[12] L. Batina, N. Mentens, K. Sakiyama, B. Preneel, and I. Verbauwhede, *Low-cost elliptic curve cryptography for wireless sensor networks*, in Proc. of the 3rd European conference on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS '06), vol. 4357 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2006, 6–17.

[13] L. Bierl, *MSP430 family mixed-signal microcontroller application reports*, Texas Instruments, Inc., Dallas, TX, 2000.

[14] A. Boukerch, L. Xu, and K. El-Khatib, *Trust-based security for wireless ad hoc and sensor networks*, Computer Communications, 30 (2007), 2413–2427.

[15] S. Capkun and J.-P. Hubaux, *Secure positioning of wireless devices with application to sensor networks*, in Proc. of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05), vol. 3, Miami, Florida, 2005, 1917–1928.

[16] Carnegie Mellon University, *Nano-RK*. Available online: http://www.nanork.org/, 2009.

[17] C. Castelluccia, A. Chan, E. Mykletun, and G. Tsudik, *Efficient and provably secure aggregation of encrypted data in wireless sensor networks*, ACM Transactions on Sensor Networks (TOSN), 5 (2009).

[18] H. Chan and A. Perrig, *PIKE: peer intermediaries for key establishment in sensor networks*, in Proc. of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05), vol. 1, 2005, 524–535.

[19] H. Chen, H. Wu, J. Hu, and C. Gao, *Event-based trust framework model in wireless sensor networks*, in Proc. of the International Conference on Networking, Architecture, and Storage (NAS '08), Chongqing, China, 2008, 359–364.

[20] H. Chen, H. Wu, X. Zhou, and C. Gao, *Agent-based trust model in wireless sensor networks*, in Proc. of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD '07), vol. 3, Qingdao, China, 2007, 119–124.

[21] H. Chen, H. Wu, X. Zhou, and C. Gao, *Reputation-based trust in wireless sensor networks*, in Proc. of the International Conference on Multimedia and Ubiquitous Engineering (MUE '07), Seoul, Korea, 2007, 603–607.

[22] F. Cheng, J. Zhang, and Z. Ma, *Curve-based secure routing algorithm for sensor network*, in Proc. of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '06), Pasadena, CA, 2006, 278–281.

[23] K. J. Choi and J.-I. Song, *Investigation of feasible cryptographic algorithms for wireless sensor network*, in Proc. of the 8th International Conference on Advanced Communication Technology (ICACT '06), vol. 2, Phoenix Park, Korea, 2006, 1379–1381.

[24] C. De Cannière, *eSTREAM Optimized Code HOWTO*. Available online: http://www.ecrypt.eu.org/stream/perf/, 2005.

[25] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, *A key management scheme for wireless sensor networks using deployment knowledge*, in Proc. of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '04), vol. 1, Hong Kong, 2004, 586–597.

[26] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, *Secure probabilistic location verification in randomly deployed wireless sensor networks*, Ad Hoc Networks, 6 (2008), 195–209.

[27] N. Fournel, M. Minier, and S. Ubéda, *Survey and benchmark of stream ciphers for wireless sensor networks*, in Information Security Theory and Practices: Smart Cards, Mobile and Ubiquitous Computing Systems, D. Sauveron, K. Markantonakis, A. Bilas, and J.-J. Quisquater, eds., vol. 4462 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2007, 202–214.

[28] S. Ganeriwal, L. Balzano, and M. Srivastava, *Reputation-based framework for high integrity sensor networks*, ACM Transactions on Sensor Networks (TOSN), 4 (2008).

[29] G. Gaubatz, J. Kaps, and B. Sunar, *Public keys cryptography in sensor networks – revisited*, in 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS '04), vol. 3313 of Lecture Notes in Computer Science, Springer-Verlag, Heidelberg, 2004, 2–18.

[30] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, *State of the art in ultra-low power public key cryptography for wireless sensor networks*, in Proc. of the 3rd IEEE International Conference on Pervasive Computing and Communications Workshops, 2005, 146–150.

[31] M. Healy, T. Newe, and E. Lewis, *Power management in operating systems for wireless sensor nodes*, in Proc. of the IEEE Sensors Applications Symposium (SAS '07), San Diego, CA, 2007, 1–6.

[32] M. Healy, T. Newe, and E. Lewis, *Analysis of hardware encryption versus software encryption on wireless sensor network motes*, in Smart Sensors and Sensing Technology, S. C. Mukhopadhyay and G. S. Gupta, eds., vol. 20 of Lecture Notes in Electrical Engineering, Springer-Verlag, Berlin, 2008, 3–14.

[33] W. Heinzelman, J. Kulik, and H. Balakrishnan, *Adaptive protocols for information dissemination in wireless sensor networks*, in Proc. of the 5th Annual ACM/IEEE International Conference

on Mobile Computing and Networking (MobiCom '99), ACM, New York, 1999, 174–185.

[34] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, *Energy-efficient communication protocol for wireless microsensor networks*, in Proc. of the 33rd Annual Hawaii International Conference on System Sciences, Maui, Hawaii, 2000.

[35] D. Huang, M. Mehta, A. van de Liefvoort, and D. Medhi, *Modeling pairwise key establishment for random key predistribution in large-scale sensor networks*, IEEE/ACM Transactions on Networking (TON), 15 (2007), 1204–1215.

[36] J. Ibriq and I. Mahgoub, *A secure hierarchical routing protocol for wireless sensor networks*, in Proc. of the 10th IEEE Singapore International Conference on Communication Systems (ICCS '06), Singapore, 2006, 1–6.

[37] C. Intanagonwiwat, R. Govindan, and D. Estrin, *Directed diffusion: a scalable and robust communication paradigm for sensor networks*, in Proc. of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '00), ACM, New York, 2000, 56–67.

[38] Y. W. Law, J. Doumen, and P. Hartel, *Survey and benchmark of block ciphers for wireless sensor networks*, ACM Transactions on Sensor Networks (TOSN), 2 (2006), 65–93.

[39] L. Lazos and R. Poovendran, *SeRLoc: robust localization for wireless sensor networks*, ACM Transactions on Sensor Networks (TOSN), 1 (2005), 73–100.

[40] L. Lazos, R. Poovendran, and S. Capkun, *ROPE: robust position estimation in wireless sensor networks*, in Proc. of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05), Los Angeles, CA, 2005, 324–331.

[41] A. Liu and P. Ning, *TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks*, in Proc. of the International Conference on Information Processing in Sensor Networks (IPSN '08), St. Louis, MO, 2008, 245–256.

[42] D. Liu, P. Ning, and W. Du, *Detecting malicious beacon nodes for secure location discovery in wireless sensor networks*, in Proc. of the 25th IEEE International Conference on Distributed Computing Systems, Columbus, OH, 2005, 609–619.

[43] D. Liu, P. Ning, and W. Du, *Group-based key predistribution for wireless sensor networks*, ACM Transactions on Sensor Networks (TOSN), 4 (2008).

[44] D. Liu, P. Ning, and R. Li, *Establishing pairwise keys in distributed sensor networks*, ACM Transactions on Information and System Security (TISSEC), 8 (2005), 41–77.

[45] D. Liu, P. Ning, A. Liu, C. Wang, and W. Du, *Attack-resistant location estimation in wireless sensor networks*, ACM Transactions on Information and System Security (TISSEC), 11 (2008).

[46] Y. Liu, H. Zhou, and B. Zhao, *Secure location verification using hop-distance relationship in wireless sensor networks*, in Proc. of the 2nd IEEE Asia-Pacific Service Computing Conference, Tsukuba Science City, Japan, 2007, 62–68.

[47] J. Lopez, *Unleashing public-key cryptography in wireless sensor networks*, Journal of Computer Security, 14 (2006), 469–482.

[48] MANTIS Group at CU Boulder, *MANTIS*. Available online: http://mantis.cs.colorado.edu/tikiwiki/tiki-index.php, 2009.

[49] Micrium Technologies Corporation, *microC/OS-II*. Available online: http://micrium.com/page/products/rtos/os-ii, 2010.

[50] Networking Working Group, *A security framework for routing over low power and lossy networks (draft-tsao-roll-security-framework-01)*, Tech. Report expires 24 March 2010, IETF, 2009.

[51] ObjectWeb Consortium, *THINK*. Available online: http://think.ow2.org/, 2010.

[52] S. Ozdemir and Y. Xiao, *Secure data aggregation in wireless sensor networks: a comprehensive overview*, Computer Networks, 53 (2009), 2022–2037.

[53] M. Passing and F. Dressler, *Experimental performance evaluation of cryptographic algorithms on sensor nodes*, in Proc. of the IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Vancouver, BC, 2006, 882–887.

[54] A. S. K. Pathan, H.-W. Lee, and C. S. Hong, *Security in wireless sensor networks: issues and challenges*, in Proc. of the 8th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 2006, 1043–1048.

[55] K. Piotrowski, P. Langendoerfer, and S. Peter, *How public key cryptography influences wireless sensor node lifetime*, in Proc. of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '06), ACM, New York, 2006, 169–176.

[56] M. Pugliese and F. Santucci, *Pair-wise network topology authenticated hybrid cryptographic keys for Wireless Sensor Networks using vector algebra*, in Proc. of the 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS '08), Atlanta, GA, 2008, 853–859.

[57] R. Riaz, A. Naureen, A. Akram, A. H. Akbar, K.-H. Kim, and H. F. Ahmed, *A unified security framework with three key management schemes for wireless sensor networks*, Computer Communications, 31 (2008), 4269–4280.

[58] R. Shaikh, H. Jameel, B. d'Auriol, H. Lee, S. Lee, and Y. Song, *Group-based trust management scheme for clustered wireless sensor networks*, IEEE Transactions on Parallel and Distributed Systems, 20 (2009), 1698–1712.

[59] R. Shaikh, Y. Lee, and S. Lee, *Energy consumption analysis of reputation-based trust management schemes of wireless sensor networks*, in Proc. of the 3rd International Conference on Ubiquitous Information Management and Communication (ICUIMC '09), ACM, New York, 2009, 602–606.

[60] E. Shi and A. Perrig, *Designing secure sensor networks*, IEEE Wireless Communications, 11 (2004), 38–43.

[61] A. Srinivasan, J. Teitelbaum, and J. Wu, *DRBTS: distributed reputation-based beacon trust system*, in Proc. of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, IN, 2006, 277–283.

[62] Swedish Institute of Computer Science, *Contiki*. Available online: http://www.sics.se/contiki/, 2009.

[63] U.C. Berkeley EECS Department, *TinyOS*. Available online: http://www.tinyos.net/, 2009.

[64] A. Ünlü, O. Armağan, A. Levi, E. Savas, and O. Erçetin, *Key predistribution schemes for sensor networks for continuous deployment scenario*, in Proc. of the 6th International IFIP-TC6 Conference on Ad Hoc and Sensor Networks, Wireless networks, Next Generation Internet (Networking '07), Atlanta, GA, 2007, 239–250.

[65] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, *Wireless sensor network security: a survey*, in Security in Distributed, Grid, and Pervasive Computing, Y. Xiao, ed., CRC Press, Boca Raton, FL, 2007, 367–410.

[66] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, *Energy analysis of public-key cryptography for wireless sensor networks*, in Proc. of the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom '05), 2005, 324–328.

[67] P. Wang, J. Zheng, F. Yang, and C. Li, *Joint data aggregation and encryption using Slepian-Wolf coding for clustered wireless sensor networks*, Wireless Communications and Mobile Computing, 10 (2010), 573–583.

[68] Y. Wang, G. Attebury, and B. Ramamurthy, *A survey of security issues in wireless sensor networks*, IEEE Communications Surveys & Tutorials, 8 (2006), 2–23.

[69] R. Witek and J. Montanaro, *StrongARM: a high-performance ARM processor*, in Compcon '96. 'Technologies for the Information Superhighway' Digest of Papers, Santa Clara, CA, 1996, 188–191.

[70] D. Xiao, M. Wei, and Y. Zhou, *Secure-SPIN: secure sensor protocol for information via negotiation for wireless sensor networks*, in Proc. of the 1ST IEEE Conference on Industrial Electronics and Applications, Singapore, 2006, 1–4.

[71] Z. Yao, D. Kim, and Y. Doh, *PLUS: parameterized and localized trust management scheme for sensor networks security*, in Proc. of the IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS), Vancouver, BC, 2006, 437–446.

[72] E. A. Young, T. J. Hudson, and R. S. Engelschall, *OpenSSL*. Available online: http://www.openssl.org/, 2010.

[73] C. Yu, T. Chi, C. Lu, and S. Kuo, *A constrained random perturbation vector-based pairwise key establishment scheme for wireless sensor networks*, in Proc. of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '08), ACM, New York, 2008, 449–450.

[74] T. Zahariadis, H. Leligou, S. Voliotis, S. Maniatis, P. Trakadas, and P. Karkazis, *An energy and trust-aware routing protocol for large wireless sensor networks*, in Proc. of the 9th WSEAS International Conference on Applied Informatics and Communications (AIC '09), World Scientific and Engineering Academy and Society (WSEAS), Stevens Point, WI, 2009, 216–224.

[75] J. Zhang, Y. Lin, M. Lin, P. Li, and S. Zhou, *Curve-based greedy routing algorithm for sensor networks*, in Proc. of the 3rd International Conference on Networking and Mobile Computing (ICCNMC '05), X. Lu and W. Zhao, eds., vol. 3619 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2005, 1125–1133.

[76] W. Zhang, M. Tran, S. Zhu, and G. Cao, *A random perturbation-based scheme for pairwise key establishment in sensor networks*, in Proc. of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '07), ACM, New York, 2007, 90–99.

[77] T. Zia and A. Zomaya, *Security issues in wireless sensor networks*, in Proc. of the International Conference on Systems and Networks Communications (ICSNC '06), Tahiti, French Polynesia, 2006, 40.

[78] W. Znaidi, M. Minier, and J. Babau, *An ontology for attacks in wireless sensor networks*, Tech. Report 6704, INRIA, 2008.