RESEARCH ARTICLE OPEN ACCESS

An analysis on Wireless Sensor Networks of Measures Secure Routing

KiranbenV.Patel [1], Megha R. Dave [2], Dr. Harshadkumar P. Patel [3]

SakalchandPatel University, India, Gujarat - Visnagar

ABSTRACT

Wireless sensor networks (WSNs) are expected to overtake other sensing technologies in the near future for a variety of application areas. The safe transmission of data via networks is one of the primary issues with WSNs. The reason for this is that WSNs are typically placed in hostile or unmanaged environments. While in recent years routing systems have mostly concentrated on metrics like resilience, energy preservation, etc., different security solutions have recently emerged that also take into account the security challenges in WSNs. This study investigates various sorts of attacks on the routing layer of WSNs. Then, secure localization, trust and reputation management, key establishment, cryptography, and other procedures for routing security.

Keywords: - wireless sensor networks; secure routing; WSNs

I. INTRODUCTION

Since many years, monitoring of interest regions has become crucial for both civil and military uses, including emergency situations, manufacturing environments, combat zones, etc. The development of sensor nodes has intensified recently, resulting in smaller and smaller sensor nodes while also lowering the cost per sensor. This is due to advancements in micro-electronics, highly integrated electronics, and improved energy accu-mulators. One of the key concepts was that the sensor nodes should collaborate to create a wireless network that can monitor events in a variety of surroundings while functioning in an ad hoc, self-configurable, and self-organizing manner, i.e. without the need for human contact.

The sensor nodes are bound in their computational power, memory, and transmission range due to the sensor's energy, which is often provided by a battery that should last the sensor's lifetime. As a result, the nodes are unable to carry out computationally intensive activities or produce significant results on their own. As a result, in order to monitor larger regions, the sensor nodes must work together to aggregate measured values and send them to a location in the network where the data can be read out and assessed.

The movement of data packets from a source to a destination through the network is one of the main research areas in WSNs. Energy is one of the main design criteria for routing protocols in WSNs due to the restricted energy resources. Data packets that need to be transported throughout the network must be passed over several hops because each sensor's transmission range is severely constrained in order to conserve energy. The routing must be failure-tolerant, adapt continuously, and consume as little energy as feasible due to topology changes, interferences brought on by environmental factors or enemies, node failures, or dwindling energy resources.

A complete network failure can be prevented by routing packets around crucial locations using the most recent routing information. Additionally, the routing algorithm should consider load balancing to prevent overloading of certain nodes and lower the possibility of network segmentation, which could result in missing paths between the source and the destination. Furthermore, in order to decrease repeated transmissions of the same data, the fusion of sensed data must be taken into account in WSN routing protocols. Although data packet routing in WSNs is a crucial service that enables communication in the first place, security concerns in the routing domain have largely gone unaddressed. Instead, the majority of the existing routing protocols focus on energy conservation, robustness, responsiveness, and reliability. However, failing to take into account potential security concerns in the routing space could prove catastrophic because practically all application areas where WSNs are employed, As a result of their placement in hostile or unmanaged surroundings, sensor nodes are vulnerable to some types of attacks from enemies. A major issue is the capture and compromise of nodes, in particular, because it is simple for attackers to physically access the sensors. In this study, security issues of WSNs will be explored with a special emphasis on the network layer, in contrast to several prior studies that dealt with broad security issues of WSNs, among other things; see, for example, [8, 10].

The remainder of the essay is structured as follows: Section 2 discusses the unique traits of WSNs. Following the presentation of the fundamental requirements for safe WSNs in Section 3, several methods of attacks on WSNs are next examined in Section 4, with a particular emphasis on the network layer. In Section 5, mechanisms for secure routing in WSNs are covered, taking into account solutions put forth by previous researchers in this field. Topics covered include cryptography, key establishment, trust &

reputation, and secure localisation. After discussing the prospects for these security measures in the future, judgements will be made.

I. Characteristics of wireless sensor networks

Wireless Sensor Networks (WSNs) differ from conventional wired or even modern wireless networks in a number of ways, including the features they offer and the targets they present for attackers. As a result, the next section emphasises the technical and architectural features of WSNs, including both the restrictions of individual sensor nodes and the constraints of the overall WSN topology. In light of these characteristics, security issues for the network layer in WSNs are examined in conclusion. (see, e.g. [4, 65, 68])

Sensor node constraints

Memory limitation

A sensor node typically has a minimal amount of memory (a few KB). However, the operating system for the sensor typically uses around half of the RAM. TinyOS [63], Contiki [62], MANTIS [48], THINK [51], microC/OS-II [49], and nano-RK [16] are some of the most popular OS for WSNs. The remaining RAM must accommodate everything else, including executable programme code, buffered communications, routing tables, etc.

Computational limitation

Due to cost and energy-saving concerns, the processing power of the sensor nodes is also severely constrained. Because of this, the majority of sensor nodes employ subpar processors with a 4–8 MHz clock-rate, such as the Atmega128L [9] or MSP430 [13]. To the detriment of the nodes' longer lifespan, sensor nodes may use stronger processors with a few hundred MHz, such as StrongARM [69] or SH4 [6, depending on the application area. entry point or hostile setting. The sensor unit, the communication unit, and the compute unit are the three primary energy consumers for a sensor node. Energy is frequently one of the key criteria in WSNs routing algorithms because to the limited energy reserves [3]. Numerous WSN operating systems have specific functions to conserve energy [31].

Transmission range

The usage of a very short transmission range by sensor nodes is fairly prevalent in order to reduce the energy required for communication. As a result, it becomes necessary to use many hops to send data across a wide network from a source to a destination node.

Physical accessibility

In contrast to wired networks, where an attacker must get past many physical defences like firewalls or gateways, nodes in WSNs can be easily attacked by an adversary because they are typically put in an unprotected environment. The network may be troubled by extra physical dangers as well, such as weather and radiation.

Network constraints

Deployment uncertainty

Sensor nodes are often distributed randomly and dynamically, meaning that neither the location of the nodes after deployment nor which nodes will be next to which other nodes are known in advance. The sensor nodes should, however, be capable of organising themselves and configuring themselves without additional assistance from operators once they have been deployed.

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. Further- more, 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 causes the latency to increase because of network congestion and the additional processing time needed. Additionally, the routing procedure in WSNs frequently results in delays: for instance, if a routing algorithm divides the energy load among many paths between a source and a destination, the quickest path is not always taken, resulting in extra predictable delays.

Remote management

The sensor nodes must be managed remotely after deployment due to the application area of sensor nodes in unattended environments. As an illustration, in a military After deployment, there will be no direct access available in the scenario when the sensor nodes are positioned behind enemy lines for reconnaissance.

Network partitions

It is possible for a randomly distributed WSN to be separated into multiple sub-networks, or "network partitions," that are unable to communicate with one another. This problem can still persist after the deployment if certain nodes are destroyed, lose power, or move out of range.

Lack of a central management

There is typically no special central facility in charge of managing WSNs; instead, complete WSNs operate in a

dispersed, self-organizing, and self-configuring peer-to-peer fashion. On the one hand, this results in a very resilient infrastructure with some sort of self-healing qualities, but on the other, new difficulties appear.

Scalability

In order to monitor specific areas, a lot of sensor network nodes are typically deployed. Scalability must therefore be taken into account in the network protocols. No matter how many sensor nodes there are—a few or many—it must be verified that the established mechanisms function uniformly.

Data aggregation

The sensor nodes need not be taken into account individually in order to get usable results from a WSN; instead, the monitored data should be aggregated in order to get more reliable findings and, at the same time, save energy throughout the routing process.

Topology changes

Although the sensor nodes are stationary in the majority of WSN cases, the topology of the WSN might change as a result of node failures brought on by hardware malfunctions, battery drain, and other external factors like attacks or interference from the environment.

Considering security at the network layer The limitations of each individual sensor node as well as the limitations of the network do affect the security considerations on the network layer and must thus be taken into account**:**

Prior to applying specific security algorithms on the network layer, it is important to take into account the restricted memory and processing capabilities of the sensor nodes. Due to energy constraints and performance difficulties, the majority of security techniques that are cutting edge on other devices, such as "normal" public key cryptography, cannot be employed on sensor nodes without modifications. Cryptographic algorithms must be specifically optimised for sensor nodes taking into account fewer calculations.

Small key sizes, as well as a limited supply of keys. Because of this, symmetric key cryptography is a common component of the current cryptographic techniques used in WSNs. However, a few recent studies demonstrated the use of public key cryptography in WSNs under specific circumstances (see, for example, Section 5). Hybrid cryptographic methods, which attempt to combine the benefits of both methods, are another choice.
For security procedures in WSNs, the limited energy of the sensor nodes is a critical challenge. Therefore, it is important to minimise any additional computational and communication cost for security mechanisms. From a security perspective, the energy limitations provide attackers another target to aim for: an attacker may purposefully assault the sensors' power sources, for example by continually requesting superfluous routes to deplete the nodes' batteries.
The usage of multiple-hops gives enemies an additional target as a result of the transmission range's limitations, which must be taken into account in WSN routing algorithms. For instance, a hacked node on the route from source to destination gives adversaries the ability to create, copy, or alter data packets.
Additionally, attackers with greater transmission power have a wider range of attack options against the sensor nodes.
The physical accessibility of network nodes in WSNs must also be taken into account. Each sensor node must be able to protect itself from outside attacks due to the absence of a defined line of defence. As a result, it is necessary to safeguard the important programme code, especially the secret keys, from physical intruder attacks. The usage of multiple-hops gives enemies an additional target as a result of the transmission range's limitations, which must be taken into account in WSN routing algorithms. For instance, a hacked node on the route from source to destination gives adversaries the ability to create, copy, or alter data packets.
Additionally, attackers with greater transmission power have a wider range of attack options against the sensor nodes.
The physical accessibility of network nodes in WSNs must also be taken into account. Each sensor node must be able to protect itself from outside attacks due to the absence of a defined line of defence. As a result, it is necessary to safeguard the important programme code, especially the secret keys, from physical intruder attacks. necessary degree of security The degree of security and the latency must be traded off.

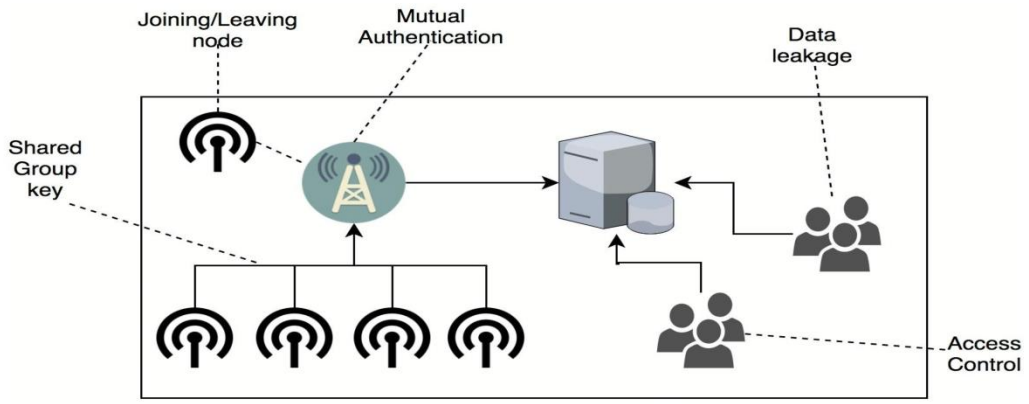


Figure 1: Basic security requirements in WSNs.

A hypothetical network partitioning must be taken into account from a security perspective since the security infrastructure must continue to function even if a single node fails or is no longer reachable.
The implemented security mechanisms should ideally function in a distributed way due to the scattered nature of WSNs. As a result, even a number of failing nodes or a network partitioning shouldn't cause the entire security system to fail. Even while a distributed security solution might be more difficult to implement, the system as a whole would be more reliable because there would be no single point of failure.

Additionally, it's important to consider the routing's scalability and the associated security measures: The distribution of keys inside the network, which serves as the foundation for secure communication and authentication, represents one of the major scalability difficulties for the security of WSNs.
The nodes that are gathering information need to be particularly safe from a security standpoint. Therefore, aggregation must be taken into consideration for safe routing protocols. For instance, if the communication is secured by end-to-end cryptography, aggregating intermediate nodes will find it more challenging to access the data.

II. BASIC SECURITY REQUIREMENTS IN WSNS

There are a number of fundamental security needs that should be considered in order to accomplish secure routing in WSNs (see Figure 1), including

- availability
- resilience
- freshness
- confidentiality
- integrity
- authentication
- authorization/access control
- secrecy

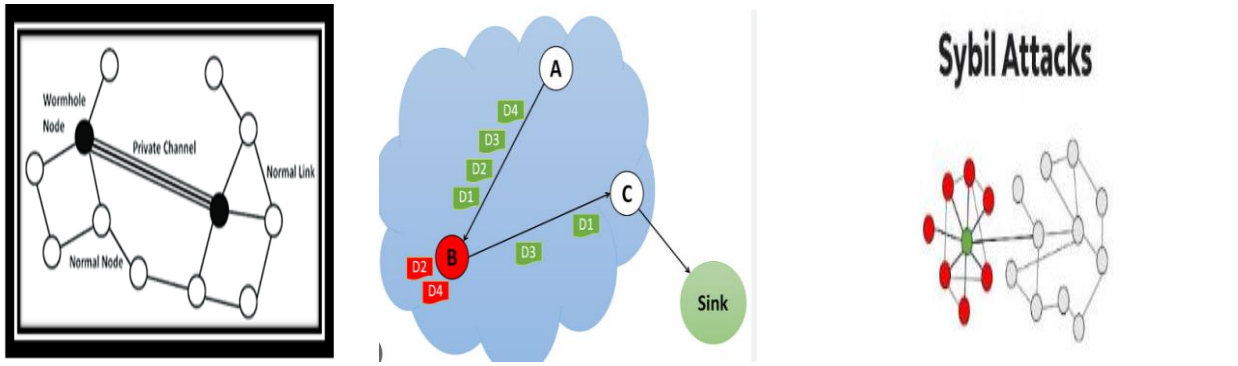
In theory, all criteria should be taken into account, but it is more likely that a subset of those requirements is picked regarding the application area of the network and the level of security that must be adhered to due to latency

problems or energy constraints. See [60, 65, 68] for a more in-depth examination of these fundamental needs.

III. ATTACKS IN WSNS

First, some fundamental attack types that can be launched in WSNs will be covered in the section that follows. Then, a closer examination of WSN network layer attacks will be done.Common WSN attack typesGenerally speaking, attacks against WSNs fall into one or more of the following categories (for examples, see [60, 68]):

- Outsider vs. insider attacks: An outsider attack occurs when a malicious node damages the WSN even if it is not a part of it. In contrast, a malicious node harms the WSN as a (authorised) participant of the WSN in an insider attack.
- Physical vs. remote assault: A physical attack involves an advertiser physically accessing the sensor node that is intended to be damaged and destroying or interfering with the sensor's hardware. A remote attack, in contrast, is carried out from a (far) distance, for instance by interrupting communication by sending out a high-energy signal.
- Passive vs. Active Attack: In a passive attack, the enemy merely listens in on or keeps track of the communication taking place within the WSN. In contrast, the adversary directly affects communication in the WSN during an active attack by altering, falsifying.
- Laptop-class vs. Mote-class assault: A mote-class attack is one that targets a WSN that is implemented from a mote, meaning that the attacking device uses the same type of hardware as the target sensor nodes. Contrarily, in a laptop-class attack, the enemy makes use of a device that has greater computational and transmission capability than the sensor nodes that should be attacked.



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

Figure 2: Attacks on the network layer.

The network layer of WSNs is susceptible to a variety of assaults. As shown in Figure 2, the majority of attacks on the network layer fall into one of the following categories:

- Information disclosure: membership in the WSN, whether passively or actively, results in the revelation of routing information.
- Physical attack: physical intervention to gain unauthorised access to a sensor node.

Energy fatigue is the deliberate squandering of energy resources by enemies, such as when they ask for unneeded routes.

Denial of service involves saturating the network with pointless routing requests.

- Spoofed, altered, or replayed routing information: modifying the routing behaviour by the spoofing, alteration, or replay of routing information.
- Routing table overflow: flooding of the routing database by adding numerous routes that don't already exist.

IV. MEASURES FOR SECURE ROUTING IN WSNS

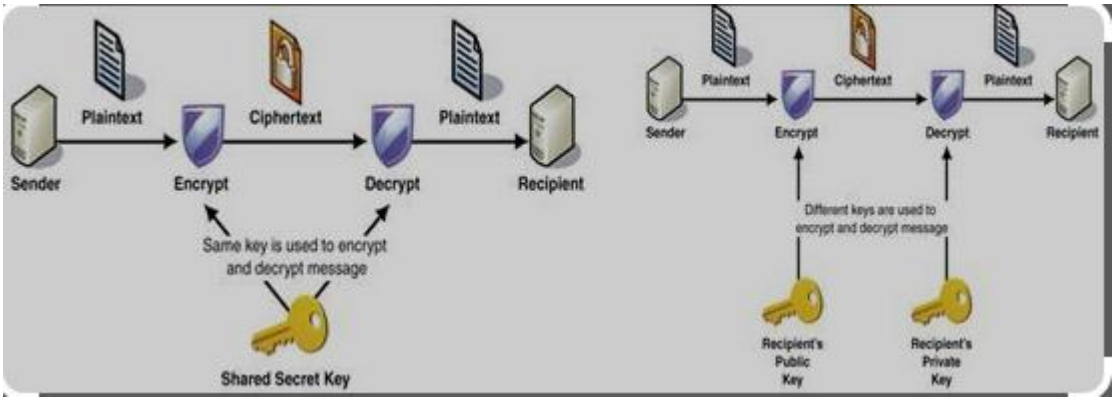
Different security techniques can be used to increase the security of routing protocols in WSNs. Although the majority of the principles are well-known and have been employed in other branches of computer science for many years, they must be applied to WSNs while taking into account their unique features. In addition, it's important to keep in mind the basic security criteria that were highlighted as well as potential WSN attacks.
Based on these factors, a selection of suggested security measures that have recently been debated in the research community and can increase the security of WSN routing protocols are described below.

Cryptography

To achieve the fundamental security needs of confidentiality and integrity in networks, cryptographic techniques are frequently used. However, as previously indicated, sensor nodes have limited processing and memory capacities, making it difficult to directly transfer well-known conventional cryptographic approaches to WSNs without making modifications.

One of the key areas of research for securing WSN communication is cryptography, which has an impact on a number of subtopics like storage-efficiency and energy-efficiency. A brief summary of recent research in the field of WSN cryptography is provided below:

Symmetric cryptography
Since the commencement of the application of cryptography in the context of WSNs, the primary emphasis has been on symmetric cryptography on the grounds that it is believed to be more effective and to consume less energy than public key cryptography (see Figure 3(a)). As a result, there are numerous studies on this subject:
Law et al.'s [38] survey on the evaluation of block cyphers for WSNs is based on authoritative recommendations and current research. The authors search for the most energy- and storage-efficient algorithms in addition to taking into account the algorithms' security features. Benchmark tests are run on the 16-bit RISC-based MSP430F149 with several block cyphers in mind to compare them.



a)Symmetric encryption. (b) Asymmetric encryption.

Figure 3: Types of cryptography

Different operation modes, such as cipher-block chaining (CBC), cipher feedback mode (CFB), output feedback mode (OFB), and counter (CTR); and parameters, such as key length, rounds, and block length. The majority of the

code was adapted from OpenSSL [72] based on a review of various cryptographic libraries, including OpenSSL, Crypto++, Botan, and Catacomb. On the basis of the original papers, ciphers without public implementations were implemented. The MSP430 C Compiler from IAR Systems was used to compile the source code. Based on the available memory and desired security level, the evaluation results of the benchmark tests indicate that the three block ciphers Skipjack, MISTY1, and Rijndael are the most appropriate for WSNs. For pairwise links, i.e., a secured link, "Output Feedback Mode (OFB)" serves as the operating mode.

In their study of survey stream ciphers for WSNs, Fournel et al. The selected stream cipher algorithms (DRAGON, HC-256, HC-128, LEX, Phelix, Py and Pypy, Salsa20, SOSEMANUK) were first submitted to the European Project Ecrypt in the eStream call (Phase 2) and are all intended for software applications. The well-known stream ciphers RC4, SNOWv2, and AES- CTR were taken into consideration for evaluation in order to broaden the choice. The ARM9 core-based ARM922T benchmarks were run to determine the most energy- and storage-efficient stream ciphers for this system. Four performance metrics were taken into account based on the eStream testing framework's methodology [24]: encryption rate for long streams, packet encryption rate, key and IV setup, and agility. On both platforms, speed is comparable. In comparison to the key setup on the conventional PC platform, the key setup for SOSEMANUK was extremely large.
Using MICAz-style motes running TinyOS, Choi and Song [23] investigate the viability of various cryptographic algorithms for their use in WSNs. Experimental analysis was done on how much memory, processing time, and power each cryptographic algorithm used. As a result, it was determined that RC4 and MD5 were the best algorithms for MICAz-type molecules.

The runtime behavior of cryptographic algorithms (including AES) and hash-functions (including MD5 and SHA-1) for WSNs is verified by Passing and Dressler [53] using an experimental setup. Two BTnodes are connected to a Linux-running PC in the experimental setup.

Public key cryptography

Public key cryptography has recently replaced symmetric cryptography in the research community (see Figure 3(b)), which was previously thought to be computationally prohibitive for WSNs. In particular, the developing field of elliptic curve cryptography (ECC) in wireless sensor networks (WSNs) appears to be a promising strategy: compared to common public key approaches, ECC is faster. while also achieving equivalent security with smaller keys. Numerous studies have been conducted on public key cryptography in WSNs, including the following: By proposing a hardware assisted public key approach that is based on optimized algorithms and associated parameters as well as low-power design, Gaubatz et al. [29] challenge the fundamental beliefs about public key cryptography in WSNs. The Rabin's Scheme and NtruEncrypt proof of concept implementations, both of which use a regular ASIC standard cell library, are presented to demonstrate the viability of their strategy in terms of various metrics, including power consumption, throughput, and level of security. The findings demonstrate that public key cryptography can be used for WSNs and has a power consumption of less than 20 W.
For WSNs, Lopez [47] contrasts symmetric and public key cryptography. Lopez emphasizes the symmetry's potential. Public-key cryptography's effectiveness for WSNs and the corresponding issues that must be taken into account are described by Arazi et al. in their article from [7]. ECC is singled out as a suitable technique for WSN because it offers a good balance between key size and security. ECC is one of the most effective forms of public key cryptography in WSNs, according to Liu and Ning [41]. A configurable and flexible library for ECC operations in WSNs, TinyECC, is presented along with its design, implementation, and evaluation processes. The library offers a variety of optimization switches that can be combined to produce various execution times and resource consumptions depending on the developer's requirements for a particular application. Additionally, the TinyECC library was examined on a number of sensor platforms, including MICAz. To find the most computationally and storage-efficient configurations, use Tmote Sky and Imotel.
Gaubatz et al. [29, 30] propose a custom hardware assisted approach to reduce the energy consumption of public key cryptography using special purpose ultra-low power hardware implementations of public key algorithms to make public key cryptography practical for WSNs. The use of public key cryptography, according to the authors, results in less protocol overhead, fewer packet transmissions, and consequently, power savings. Three different public key cryptography implementations for WSNs, including Rabin's Scheme, NtruEncryptor, and ECDSA/ECMV, are also thoroughly compared. The comparison takes into account the cipher text, the message payload, the average power and energy used per message for encryption and decryption, as well as for signing and verification.

Hybrid cryptography

Both strategies, symmetric and asymmetric cryptography, can also be used in conjunction to combine their advantages:
In their paper [56], Pugliese and Santucci discuss a brand-new hybrid cryptographic technique based on vector algebra in GF(q) for the creation of pairwise network topology authenticated keys (TAK) in WSNs. Symmetric cryptography is used for the ciphering and authentication models, and asymmetric cryptography is used for the key generation models.

A unified security framework with three key management schemes—SACK, SACK-P, and SACK-H—is proposed by Riaz et al. in their paper [57]. SACK-H employs a hybrid cryptography strategy, whereas SACK and SACK-P are based on symmetric key cryptography and asymmetric key cryptography, respectively. Asymmetric cryptography is used by SACK-H for intra-cluster communication.

Energy consumption

The energy consumption required for cryptographic methods is another important subject. As a result, numerous studies have been conducted in this area. Wander et al. [66] calculate the energy cost of public key cryptography-based authentication and key exchange on an 8-bit Atmel ATmega128L low-power microcontroller. In order to compare the two public key algorithms RSA and ECC, mutual authentication between two parties is taken into account. The findings demonstrate the viability of software-based public key cryptography on an 8-bit microcontroller platform, but ECC performs noticeably better than RSA in terms of computation time and the amount of data that must be stored and transmitted. ECC therefore uses less energy than RSA.
The power consumption of the most popular RSA and ECC operations, like signature generation and verification, as well as the associated transmissions on popular sensor platforms like MICA2DOT, MICA2, MICAz, and TelosB, is estimated by Piotrowski and Peter [55]. The experiment's findings demonstrate that public key cryptography has little to no impact on the sensors' lifespan, making strong cryptography suitable for WSNs. According to the authors, the transmission power is extremely small in comparison to the computational power. The need to exchange keys should be kept to a minimum, and hardware-accelerated cryptographic computations should be taken into consideration to lower the overall energy consumption in WSNs due to the multiple hop architecture.
a low-cost public transportation system that Batina et al.

Data aggregation
Additionally, as previously mentioned, coordination is required between the interaction of data aggregation and cryptographic techniques. There are studies that concentrate on this subject:
Without decrypting the data, Castelluccia et al.'s[17]main focus is on the effective additive aggregation of encrypted data in WSNs. For the purpose of aggregating cipher text, the authors suggest a homomorphic encryption scheme that enables the efficient aggregation of encrypted data using just a single modular addition.
The indistinguishability property of a pseudo-random function (PRF) is a common cryptographic primitive. In contrast to end-to-end encryption without aggregation, the method offers a high level of security. The new method uses less bandwidth than hop-by-hop aggregation, but it has much higher privacy levels than a naive aggregation method that uses hop-by-hop decryption. Additionally, the nodes' share of the communication load is fairly evenly distributed, which extends the overall network lifetime. In order to defend the integrity of the aggregated data against outsider-only attacks, an end-to-end aggregate authentication scheme is also introduced. This scheme is also based on the indistinguishability property of PRFs.
In order to facilitate efficient and secure data transmission in clustered WSNs, Wang et al. [67] propose a joint data aggregation and encryption scheme. The Slepian-Wolf theorem is applied to the optimal intra-cluster rate allocation problem to minimize the total energy consumed by all cluster nodes to send encoded data. For each cluster, a brand-new encryption method called spatially selective encryption is introduced, which is based on the Slepian-Wolf coding. Each cluster head encrypts its data to protect the data of the members, which are sent to it by the cluster members unencrypted. The simulation results demonstrate that the new method significantly increases data transmission's energy efficiency while offering a high level of security.
Providing a thorough overview of secure data aggregation in WSNs is Ozdemir and Xiao [52]. A taxonomy of secure data aggregation protocols is presented by the authors based on recent "state-of-the-art" research in this field. For secure data aggregation concepts, open research areas and future research directions are also covered.

Existing secure routing protocols for WSNs

Based on these various security considerations, the research community has developed some comprehensive routing protocols that use encryption to safeguard communication between nodes in WSNs:

SHEER, a secure hierarchical energy-efficient routing protocol is presented by Ibriq and Mahgoub [36] and offers secure communication at the network layer. A probabilistic broadcast mechanism and a three level hierarchical clustering architecture are used to increase the network's energy performance and lifetime. SHEER uses HIKES, a hierarchical key management and authentication scheme, to secure the routing mechanism from the very beginning of the network. According to the simulation results, SHEER is more scalable and energy-efficient than secure LEACH using HIKES.

Based on the curve-based greedy routing (CBGR) algorithm [75] and a suitable encrypting algorithm, Cheng et al. [22] propose a secure routing algorithm for WSNs. A different key is used to encrypt each forwarded packet. The new algorithm's analysis reveals that it is less complex than Direct Diffusion (DD) [37] and LEACH [34] while still providing some degree of security.

By enhancing its security through the use of encryption and packet header authentication, Ali and Fisal [5] enhance the current routing protocol SRTLD [2], which depends on the optimal forwarding decision taking into account the link quality, packet delay time, and the remaining power of next hop sensor nodes. Attacks such as HELLO flooding and selective forwarding are thwarted by the proposed security measures. It was simulated.

Key establishment

A key of some kind is necessary for almost all cryptographic techniques, but in WSNs, how can these keys be efficiently established between randomly placed sensor nodes? Due to the sensor nodes' constrained computational and memory capabilities, well-known key exchange protocols like the Diffie-Hellman key exchange protocol are frequently ineffective. Furthermore, because a WSN typically requires cooperation from hundreds or even thousands of nodes, the scalability of the key establishment protocol must be taken into consideration.

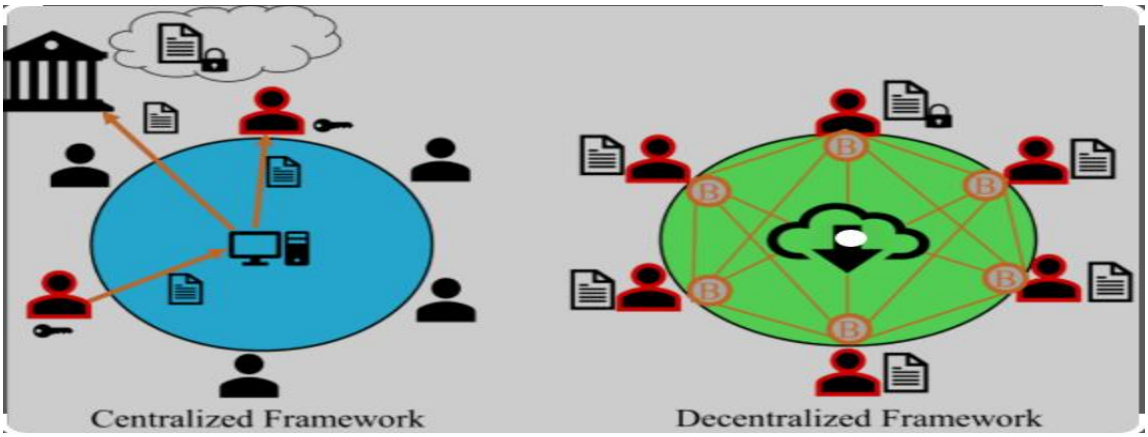
Different approaches can be found in the field of key establishing protocols; in the following, a few examples of recent research are discussed: By introducing "trusted intermediaries for key establishment" (PIKE), a new key-distribution scheme, Chan and Perrig [18] address the incapability of existing symmetric key distribution protocols to scale. Peer sensor nodes are used as trusted intermediaries in PIKE's basic design to create shared keys between nodes. Each node in the network has its own pairwise key that it shares with a specific subset of other nodes. The keys are placed in the network in a special way so that every pair of nodes A and B can locate a node C that has a pairwise key that only it and A and B share. Therefore, node C can be utilized as a secure middleman to create a key between nodes A and B.

The established key is secure as long as C remains secure. To configure the trade-off between communication, memory, and security level, various extensions and parameters can be used. The PIKE- 2D and PIKE-3D configurations were tested by the authors. While PIKE-2D offers greater resilience against node capture, PIKE-3D achieves lower communication and memory overhead while being less resilient against active attacks. The authors demonstrate that PIKE's communication and memory overheads scale (O(n)) sublinearly as a function of the network's node count. Additionally, PIKE establishes keys using a consistent communication pattern, making it more challenging for adversaries to attack. In addition, any two network nodes can establish a key in PIKE, unlike random-key pre-distribution mechanisms.

Bivariate polynomials are used by Liu et al. [44] to create a general framework for creating pairwise keys between sensor nodes. A random subset assignment key pre-distribution scheme and a hypercube-based key pre-distribution scheme are two effective examples of the authors' general framework. Each sensor node is given a subset of the bivariate polynomials generated by the random subset assignment scheme, which creates a pool of random bivariate polynomials. As a result, each pair of sensor nodes has its own unique key. The hypercube-based scheme, in contrast, places polynomials in a hypercube space and gives each sensor node a specific coordinate in that space. Each node can identify the nodes it can directly establish a pairwise key with based on the coordinate in the hypercube.

The sensor nodes are deployed continuously along a line, one by one, according to a new practical deployment model presented by Unlu et al. in [64]. The sensors can be placed over several parallel lines to cover a two-dimensional area. Two key distribution schemes that make use of the deployment knowledge are presented on top of this deployment model. The analysis and simulation results demonstrate that the new key distribution schemes outperform Du et al. [25]'s approach, in which nodes are deployed in groups, in terms of connectivity, resiliency, memory requirements, and communication costs. Zhang et al. [76] propose a novel random perturbation-based

(RPB) scheme. The system ensures that any two nodes can create a pairwise key directly between them without disclosing any information to other nodes. The pairwise keys keep the non-compromised nodes secure even if some nodes in the network are compromised. The system offers minimal computational and communication overhead and adjusts to changes in the network.



A) Centralized trust exchange with a reputation center. (**B**) Decentralized trust exchange by forming a web of trust.

Figure 4: Types of trust exchange.

The RPB scheme's prototype implementation on MICA2 nodes demonstrates its high security, efficiency, and minimal storage requirements. It is therefore appropriate for the current wave of sensor nodes.

Constrained random perturbation vector-based pairwise key establishment (CRPV) and its variant, the CRPV+ scheme, are proposed by Yu et al. [73] for WSNs. The described "versatileness criteria" are all met by the new CRPV+ scheme. The five criteria for a key establishment scheme outlined by Zhang et al. [76] (Resilience to large number of node compromise, guaranteed key establishment, direct key establishment, resilience to network topology, and efficiency) are included in the versatileness criteria, along with the two additional criteria of scalability and independence from hardware that were added by the authors.

For the purpose of designing and analyzing pairwise key establishment schemes for large-scale sensor networks, Huang et al. [35] derive two probability models. The new model examines the key path length hop-by-hop and applies the binomial distribution as well as a modified binomial distribution. The models give designers the ability to examine the connectivity of the key graph and the path length during the pairwise key establishment phase. The results of the two models' systematic validation demonstrate their robustness.

A framework for a group-based deployment model is introduced by Liu et al. [43] to enhance the effectiveness of key pre-distribution in WSNs. In this model, sensor nodes must be placed in groups so that they can communicate with one another.

The accuracy of measurements and routing issues cannot be verified due to compromised sensor nodes or node failures. This issue can be solved by implementing a trust and reputation system, allowing the enormous number of sensor nodes to work cooperatively to determine what is right or wrong in terms of their behaviors. The trust values between the nodes can be transferred using either a centralized or a decentralized trust exchange (see Figure 4). Further choices can be made, like locating better, more reliable routes or isolating misbehaving sensor nodes, based on a trust and reputation system.

Despite the fact that this concept has been taken into consideration in related fields like ad hoc networks and peer-to-peer networks . Distributed reputation-based beacon trust system (DRBTS), which is proposed by Srinivasan et al. [61], is a novel reputation-based scheme for excluding malicious beacon nodes from the network that provide false location information. Every beacon node keeps an eye out for bad behavior from its 1-hop neighbors and updates its reputation table accordingly. Each node publishes its reputation table to its 1-hop neighbors in order to share the

knowledge. The acquired second-hand information is used to update the reputation table if a deviation test is successful. Each node has the option to use or disregard certain beacon nodes' information based on a simple majority scheme. The simulation results demonstrate that the scheme operates reliably in dense networks and that it is adaptable to particular application domains.

For clustered WSNs with backbone, Boukerch et al.'snovelagent-based trust and reputation management scheme (ATRM) is proposed [14]. With a minimum of extra messages and delays, the new system efficiently manages trust and reputation locally. Because a node cannot generate its own trust or reputation values, each node in the network maintains its own trust and reputation information. The process is as follows: Each node has a mobile agent in charge of managing the node's reputation and trust. The mobile agent of the requester is sent to the provider node to obtain a certificate before a transaction between two nodes can occur. A determination is made regarding the transaction's viability based on this certificate. The so-called Reputation-based Framework for Sensor Networks (RFSN), which Ganeriwal et al. [28] investigate, is a generalized and unified approach for providing information about the data accuracy in WSNs. The authors present a middleware for a trust and reputation system for WSNs in which a community of trusted sensor nodes is formed based on reputation metrics. The reputation metrics of each sensor node are kept track of. Each node's reputation is calculated using a Bayesian formulation (beta reputation system), which takes into account both the nodes' historical behavior and any potential future behavior. The middleware was ported to the WSN operating systems TinyOS and SOS and tested in various settings, including simulations using the Avrora network simulator and with actual MICA2 motes in a test-bed. The energy usage of reputation-based trust management strategies is studied by Shaikh et al. The Generic Communication Protocol (GCP), which can be used to exchange trust values, is suggested by the authors. Three cutting-edge reputation-based trust management schemes (GTMS [58], RFSN [28], and PLUS [71]) for WSNs are presented, with analyses of their theoretic energy consumption based on GPC. The findings demonstrate that, in the tested peer recommendation scenario, GTMS uses less energy than PLUS and RFSN.

Zahariadis et al. [74] propose Ambient Trust Sensor Routing (ATSR), a new secure routing protocol that relies on a distributed trust model considering direct and indirect trust, as part of the EU-funded seventh framework (FP7) within the AWISSENET project [11]. The geographic routing principle is modified by ATSR to handle large network dimensions. The remaining energy of each neighbor is considered for the routing decision to improve load balancing and network lifetime. According to the simulation results, significant energy is used for routing and trust functions; as a result, it is important to carefully consider how frequently this information is exchanged.

Secure localization

Secure location-based routing algorithms must ensure the localization of sensor nodes. The security is required for two reasons: first, each sensor node must be able to accurately determine its own location even in hostile conditions; second, compromised nodes must be prevented from broadcasting erroneous location information to the network. Wormhole and Sybil attacks can be defended against with secure location-based routing. In order to protect location discovery services in WSNs, Liu et al. [42] introduce a set of techniques to detect and remove compromised nodes that supply false location information. This research falls under the category of secure localization. To prevent false positives, techniques for detecting replayed beacon signals are investigated along with a straightforward method for detecting malicious beacon signals. Additionally, a technique is offered that enables the base station to deduce the suspect nature of beacon nodes and revoke them appropriately.

Robust Position Estimation (ROPE), a robust localization system proposed by Lazos et al. [40], enables sensors to estimate their own locations independently of a centralized authority. Additionally, ROPE offers a mechanism for location verification that aims to confirm the locations claimed by the sensors before any data is gathered. The suggested method is resistant to attacks like wormhole attacks and node impersonation, among others. The newly introduced "Maximum Spoofing Impact" metric, which is used to assess the impact of potential attacks, when applied to ROPE demonstrates that ROPE limits this metric even for low density reference point deployment. Using a two-tier network architecture, SeRLoc, another method by Lazos and Poovendran [39], proposes a novel distributed range- independent localization algorithm. The algorithm enables sensor nodes to locate themselves passively in an unreliable environment without communicating with other nodes. The likelihood of sensor displacement as a result of security threats, such as wormhole attacks or Sybil attacks, is assessed analytically. The simulation's findings demonstrate that SeRLoc localizes sensors more precisely than other cutting-edge range-independent localization techniques while requiring fewer reference points and less communication overhead. SeRLoc performs better than the other compared schemes as a result. The resistance of positioning techniques to position and distance spoofing attacks is examined by Capkun and Hubaux [15]. The authors then suggest Verifiable Multilateration (VM) as a method for wireless device positioning that is secure. In the presence of attackers, node positions can be computed and verified securely thanks to virtual machines (VM). A system for secure positioning

in a sensor network is proposed with SPINE (Secure Positioning In Sensor NEtworks), which is based on VM. The simulation's findings demonstrate that SPINE is resistant to distance modification attacks from numerous attacker nodes. Two methods to tolerate malicious attacks against range-based location discovery in WSNs are covered in a later work by Liu et al. [45].
The claimer, the witness, and the verifier are three different types of node roles that are defined. While the claimant broadcasts the position message, the witnesses rebroadcast it and give the verifier information on the distance and the lowest hop. Finally, the verifier determines whether or not the claimer accurately reported its location based on a test. The simulation's findings indicate that the probability of claiming a true location is greater than 80%, while the probability of claiming a faked location is typically less than 40%. The investigation of defenses against Sybil attacks is recommended as future work.

For dense sensor networks that are randomly deployed, Ekici et al. [26] propose a secure probabilistic location verification method. The proposed algorithm, known as Probabilistic Location Verification (PLV), takes advantage of the probabilistic dependence between the Euclidean distance between the source and the destination and the number of hops a broadcast packet must travel to reach it. The plausibility of the claimed location is assessed by a small group of verifier nodes and is expressed as a real number between zero and one. Any number of trust levels in the claimed location can be created based on the plausibility metric. The simulation's outcomes demonstrate the high accuracy and efficiency of the suggested algorithm. PLV is therefore a viable option for WSNs as a lightweight location verification system.

Future prospect

The following paragraphs will discuss the potential directions of the examined secure routing research areas:
The symmetric cryptography studies that have been presented support the notion that the sensor platform's unique limitations prevent most well-known symmetric cryptographic algorithms from being directly transferred there.
The following paragraphs will discuss the potential directions of the examined secure routing research areas:
The symmetric cryptography studies that have been presented support the notion that the sensor platform's unique limitations prevent most well-known symmetric cryptographic algorithms from being directly transferred there.
In order to run more effectively on the sensor network platform, either light-weighted sym- metric cryptography algorithms must be created or the current solutions must be modified. Despite this, symmetric cryptography performs well on sensor nodes due to its low memory and computation requirements.

The energy consumption should always be considered when using encryption because it adds to the cost of computation, storage, and transmission. As previously mentioned, in order to achieve maximum efficiency, the algorithms that should be used on a sensor platform must be carefully chosen and optimized with respect to the existing hardware. Always consider the total energy consumption when calculating energy usage; in this case, this includes the energy used for key setup, required. Communication overhead and encryption itself. For both symmetric and public key cryptography, hardware assisted approaches are frequently put forth in an effort to increase efficiency.
A hardware-assisted approach typically results in better performance, efficiency, and consequently, energy savings. However, if more hardware is needed, the price per unit will rise, necessitating the cost-benefit analysis for a sizable number of sensor nodes. Additionally, specialized hardware is typically restricted to specific cryptographic algorithms. However, specialized encryption hardware is a promising strategy that can significantly lower the additional computational costs, making it especially useful for public key cryptography, which has a higher computational cost.

For both symmetric and public key cryptography, hardware assisted approaches are frequently put forth in an effort to increase efficiency. A hardware-assisted approach typically results in better performance, efficiency, and consequently, energy savings. However, if more hardware is needed, the price per unit will rise, necessitating the cost-benefit analysis for a sizable number of sensor nodes. Additionally, specialized hardware is typically restricted to specific cryptographic algorithms. However, specialized encryption hardware is a promising strategy that can significantly lower the additional computational costs, making it especially useful for public key cryptography, which has a higher computational cost.

As a result, the nodes at specific locations are aware of their neighbors beforehand, allowing for the pre-distribution of corresponding keys. However, with such a deployment model, the placement of the sensors becomes rigid

because the grouping and the deployment order of the nodes must be predetermined, the keys must be distributed appropriately, and the deployment must be carried out precisely in accordance with the topology that was previously planned. The subsequent integration of extra nodes into an existing network is also challenging. As a result, only specific application scenarios can be used with this kind of deployment models.
The key establishment based on probabilistic models is one of the most recent and promising research advancements. Because node failures, environmental interferences, and attacks could prevent a proper key establishment between some nodes, the robustness of the key establishment is another crucial consideration. As a result, the key establishment should operate more decentralized and not depend on specific nodes.
The energy of the sensor nodes is limited, so it is important to keep the energy requirements for the key establishment process as low as possible. This will also reduce the amount of extra storage and communication overhead.

Finally, it must be noted that the key establishment is unquestionably closely related to the cryptographic safeguards that the WSN should implement. As a result, the key establishment must be optimized for the cryptographic system. If the system uses second-hand information, such as observations made by other nodes, an effective distribution of this information must be ensured. There are a number of concepts, ranging from using agents to transport trust and reputation information to sharing this information only with the base station or just locally with neighbors. However, as information is shared, adversaries have a new target to attack. For instance, a group of compromised nodes working together can manipulate the system by praising or criticizing one another. Additionally, there are a number of opportunities for the decision-making process, which determines who is trustworthy and who is not, ranging from simple majority schemes to complex statistical.

Reference	**Cryptography**	**Centralized/de centralized**	**Energy consumption**	**Simulation/impl ementation**	**Comments**
23, 27, 32, 38,	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/impl ementation	Comments
[18, 43, 44, 64, 73, 76]		Pre-distributed	Considered	Implemented	—
Reference	Trust and reputation	Centralized/dec entralized	Second hand/first hand	Simulation/imple mentation	Comments
14, 19, 28, 59, 61, 74		Decentralized	First and second hand	Simulated, implemented, implemented, simulated	energy considered, energy considered
Reference	Secure localization	Centralized/dec entralized	Verification/lo calization	Simulation/imple mentation	Comments
15, 26, 39, 40, 42, 45,		Centralized, decentralized	verification	Implemented, simulated	Detect and remove compromised nodes, , passive localization

Table 1: Secure routing mechanisms in WSN.

plans, anything is possible. Additionally, the weighting of the factors as well as the question, "What factors to

consider?" Future research can be done in this area in great numbers.
The best way to handle a misbehaving node is another matter. It is necessary to talk about both preventative measures, like excluding the node, and the mistaken exclusion of nodes because of transient environmental interferences.
How long these various types of systems need to be equilibrated in order to be fully functional after the deployment is another open research question.
However, as already mentioned, the introduction of a trust and reputation system makes the system itself a target, so future studies should also address this type of system's vulnerability.

V. CONCLUSION

Both the military and the civilian sectors have long focused their research on the monitoring of events in particular regions. The development of sensors for WSNs has accelerated recently due to the miniaturization of electronic components, allowing the devices to get smaller and smaller while simultaneously improving both their performance and energy efficiency. The routing protocol is one of the essential services needed in WSNs to enable sensor nodes to cooperate and communicate. Up until this point, the majority of routing protocols created for WSNs have mainly ignored security concerns in favor of common network metrics like throughput, energy conservation, and robustness. While WSNs are frequently deployed in hostile or unattended environments where private data and communication must be secured, ignoring security measures for WSN routing protocols is careless. Because of this, a number of security-related topics that have an impact on WSN routing have been covered in this paper. As was mentioned, conventional security measures cannot be applied to WSNs without adaptation, so new security strategies must be developed that take into account the unique properties of the sensor nodes, the fundamental security requirements of WSNs, as well as potential WSN attacks. The four key related areas of cryptography, key establishment, trust and reputation, and secure localization were identified and discussed as being crucial for secure routing. Several recent studies were presented for each topic, and open issues and potential future studies were highlighted. Table 1 provides a summary of the approaches that were taken into account. Due to the complexity and variety of security solutions offered, it is not possible to recommend "one" solution that addresses all issues. Instead, security measures must be carefully chosen depending on the application area where the WSN should be deployed in order to strike a balance between a high level of security and resource efficiency in order to prolong the lifespan of the sensors.
The other layers, and especially their points of contact, should be kept in mind, even though this paper concentrated specifically on the security of the network layer in WSNs. Future research should take a comprehensive approach to WSN security, keeping in mind both the unique characteristics of each layer and their vulnerabilities. However, the area is secure. Future research must focus on a vast area to find the best solutions that offer high security while consuming the least amount of resources.

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 Communica- tions 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. Ver- bauwhede, *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 applica- tion 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 Communica- tions, 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 wire- less 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 Con-ference 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 Inter-national 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 Con- ference 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 probabilis- tic 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 Ubiq- uitous 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 artin 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 net- work 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 proto- cols for information dissemination in wireless sensor networks*, in Proc. of the 5th Annual ACM/IEEE International Conferenceon 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 microsen- sor 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 predistri- bution 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 sen- sor networks: a comprehensive overview*, Computer Networks, 53 (2009), 2022–2037.

[53] M. Passing and F. Dressler, *Experimental performance evalua- tion 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 authen- ticated 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.

[70] D. Xiao, M. Wei, and Y. Zhou, *Secure-SPIN: secure sensor protocol for information via negotiation for wireless sensor networks*, in

[71] Z. Yao, D. Kim, and Y. Doh, *PLUS:*

[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. Ü nlü, 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 sen- sor 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 Infor- mation Superhighway' Digest of Papers, Santa Clara, CA, 1996,188–191.

Proc. of the 1ST IEEE Conference on Industrial Electronics and Applications, Singapore, 2006, 1–4.

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 Communi- cations (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 3rdInternational 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] Karuturi Satish, K. Ramesh et al., "Intrusion Determent using Dempster-Shafer Theory in MANET Routing", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 6, no. 1, pp. 37-41, 2015.