Security in Wireless Sensor Networks

Assignment II in the subject Research Methods and Project Management

Georgia-Eirini Trouli
School of Engineering
Informatics Engineering
Heraklion, Greece
tp174@edu.teicrete.gr

Ladislav Šulák
School of Engineering
Informatics Engineering
Heraklion, Greece
laco.sulak@gmail.com

***Abstract*— Network security in general is a very changeable and complex topic. This review is focused on a security of wireless sensor networks, which is also consisted of many things to be aware of. It brings new types of problems also in the field of security because of limited resources of sensor devices in a wireless network, which may include a great number of nodes. This paper aims on a review, ideas, problems and technical approaches of a given topic via investigation of significant papers and studies did in the past.**

Keywords—wireless sensor networks, sensor nodes, security in WSNs, restrictions of sensor nodes, wireless cryptography

I. Introduction

Wireless sensor networks (WSNs) have become a very attractive and popular topic over the last decade. It is a network which may consist of hundreds or in some occasions even thousands of small devices of various purposes. There is typically a requirement to be a low cost and each of such devices typically has many constraints like small computing power, small amount of memory and also energy. Additionally, they can be deployed in remote and unavailable places, so they should be equipped with security mechanisms to defeat against various threats. The applications can be very different and they number is still growing. WSNs are being deployed to various scenarios which could be indoor like at the home, office or hospital, but also outdoor like in tactical battleground for military. From that it can be seen that some types of applications could be very critical and therefore a security is a very important question in some of them, which means that the balance between low power consumption and security can significantly differ according to the application. The design and the implementation of secure WSNs itself is a challenging task. This review serves as a brief summary and introduction to the security of wireless sensor networks and it brings to the reader the most important principles and problems regarding it.

This paper is structured as follows. In Section 2 there are various constraints of WSNs being discussed. Section 3 deals with a security requirements and Section 4 aims at various attacks on WSNs and their defenses. Section 5 details security mechanisms for WSN which are either used in real-world scenarios or were used just in laboratory conditions during previous research. Final Section 6 concludes this review and highlights some future directions or the research in WSN security as well.

II. Constraints of Wireless Sensor Networks

WSN typically contains of a big number of sensor nodes which have limited resources [2]. It is caused mainly by a small physical size and limited energy. Because of that, it is more difficult to implement a security solution for WSN and conventional methods are not always suitable for such nodes. It is necessary to be aware of the constraints of WSNs for adaptation and optimization of security approaches for such network. Major constraints are briefly described below:

1) *Energy constraints:* energy is needed for sensor transducer, communication and microprocessor computation. It has been found that communication is much more expensive than computation in those systems. That means that secured communication requires extra energy because messages are being expanded by cryptography functions.
2) *Memory limitations:* it usually contains flash memory (application code) and RAM (application programs and data) of a small physical size. One the operating system and application code are loaded, it has no place for running complicated algorithms. It should be noted that we are talking about few (or less than few dozens) of kilobytes of free space and also there is a requirement of a small cost.
3) *Transmission range*: transceivers in sensor nodes have limited transmission range and also they can be deployed in larger area and the topology can change dynamically. Once a node receives data, it first checks its header for the sequence number for checking if the data received is a new or it's a duplicate [3].
4) *Unreliable communication:* main concerns here are that packets can be dropped or damaged on the way which both leads to much higher overhead for robust error handling schemes. Also, they can collide in transit and may need retransmission.

III. Security Requirements in Wireless Sensor Networks

A WSN is a special type of network so the security requirements are also slightly different in comparison to conventional wireless networks. They are mostly oriented on protecting communication messages and the resources of attacks as well as misbehavior of nodes. Except those, there are also some other requirements (so called secondary requirements) which are following: source localization, data freshness and self-organization. They provide protection against attacks on the information which is being transmitted over WSN [1], [4], [5] and [6]:

1) *Data confidentiality*: (a) only authorized nodes are allowed to access a node reading, (b) mechanism of a key distribution should be extremely robust and (c) protection against analysis of the attacks aiming at probing public information like public keys, identities or routing data. As a defense, messages need to be encrypted with a secret key.

2) *Data integrity*: messages are not altered by other entity on their way. It could be utilized by message authentication codes or cyclic codes.

3) *Availability*: services of WSN must be always available even during the attacks like denial of service. Special detection and defense units are being used for this purpose.

4) *Time synchronization*: there exist more secure synchronization protocols for WSN which is required for many security mechanisms in WSN.

5) *Authentication*: it is essential for a receiver device to have a mechanism which would verify that receiving communication come from a sender node which claims to be. Authentication in WSN can be achieved via symmetric cryptography.

6) *Data freshness*: no adversary can replay old messages, like ones containing shared keys for message communication. Usually, a counter is being added to the message itself or a random number can be used during message encryption.

7) *Self-organization*: each node in WSN has to be self-organizing and self-healing. It is regarded to key pre-distribution schemes in symmetric encryption. It is much needed that the nodes in WSN are self-organized among each other, not only for multi-hop routing, but also for handling key management and for developing trust relations.

8) *Secure localization*: location information must be secured properly because potential attacker can manipulate with this information for his own benefit. There are more techniques to achieve protection. One of them uses computation of device position by series of known reference points and authentication. The other one uses a technique, which takes a benefit from computing a sensor's position by listening to multiple encrypted messages from trustworthy locators and the computation is based on majority vote scheme.

IV. Security, Attacks and Defenses in Wireless Sensor Networks

There are various types of attacks which are possible to perform and they can be categorized into 4 groups described in the next sections. For some attacks there exist no known defenses yet and for the other ones the protection mechanism is always briefly described.

1) *Attacks on network availability* are basically Denial of Service (DoS) attacks which could target any layer of a sensor network [1], [4].

   a) **Physical layer attacks:** physical layer is responsible for things like carrier frequency generation, frequency selection, signal detection, modulation and also data encryption [4].

   - *Jamming attack* interferes with radio frequencies that the nodes in WSN use for communication. A source for jamming can be either powerful or strategically placed that it could disrupt a communication in the entire network.
     Defense: spread spectrum communication such as frequency hopping spread spectrum (FHSS), which is based on rapid switching a carrier among many frequency channels using pseudo-random sequence known to transmitter and receiver, so the frequency selection sequence is not predictable and therefore almost impossible to jam. Code spreading is another technique, but it requires a great design complexity and energy, so it is not very suitable for WSNs.

   - *Tampering attacks* are very susceptible in WSN since they typically operate outdoors. The adversary may capture a node, tamper with its circuitry and modify the program or replace such node with malicious sensor or extract cryptographic keys.
     Defense: one of the ways is tamper-proofing of a physical package of each node.

   b) **Link layer attacks:** this layer is responsible for data streams error control, multiplexing, medium access control and data frame detection.

   - *Collision attacks*: they occur when 2 nodes are trying to transmit on the same frequency at the same time. If successful, packets are discarded and they need to be retransmitted.
     Defense: usage of error-correcting codes, which however brings additional processing and communication overhead. There is no complete defense mechanism against these attacks since the attacker will always be able to corrupt more than what can be corrected.

   - *Exhaustion attacks*: they are basically repeated collisions which may have serious impact on resources. For example, energy levels of a victim node would be exhausted more quickly.
     Defense: using rate limits in the MAC admission control. That allows that network ignores such requests. Another technique is time-division multiplexing in which each node has allocated always 1-time slot during which it can transmit.

   - *Unfairness attacks*: an attacker is trying to cause that other nodes in the network will miss their transmission deadline in a real-time MAC protocol.
     Defense: some smaller frames could be used so the effect of such attacks is reduced. However, such technique often reduces efficiency and there is still a vulnerability to other types of unfairness for example when an attacker is trying to retransmit packets very quickly instead of randomly delaying them.

   c) **Network layer attacks:** there are more attack scenarios possible, except ones described below, it is possible to attack on the routing protocols in a way of routing table overflow, routing table poisoning, packet replication, routing cache poisoning or rushing attacks and some others, which could cause not only DoS but have many other impacts. For more details about such attacks and defenses please see [2].

   - *Spoofed routing information*: an attacker spoofs, alters or replays routing information for disrupting traffic in the network. It is the most direct attack against routing protocol and it includes routing loops creation, attracting or repelling network traffic from selected nodes, generating fake error messages, extending or shortening source routes and others.
     Defense: authentication and monitoring. A receiver can verify if the message has been spoofed or altered by checking an additionally appended MAC after every message. Furthermore, for defending against replayed information, counters or timestamps may be used in the messages themselves.

   - *Selective forwarding:* compromised node selectively forwards some messages to the other nodes and drops other messages. Or, the malicious node is sending the messages to the wrong path.

Defense: using multiple paths for sending data or detection of malicious node and then searching for a different route.

- *Sinkhole*: compromised node looks more attractive by forging the routing information. Other nodes will send their data through such malicious node as it is chosen to be the next-hop.
  Defense: Redundancy or probing.

- *Sybil attack*: compromised or malicious node takes an identity of multiple nodes in the network and thus routes multiple paths through such node.
  Defense: Authentication, encryption or random key pre-distribution techniques. In the last one, a random set of keys or key-related information are assigned to each sensor nodes. The idea is that each node can find out common keys (shared secret session keys) it shares between its neighbors for ensuring node-to-node secrecy.

- *Wormhole*: an advisory uses malicious node and it eavesdrops a series of packets at 1 point in the network and then tunnels them to another point. After that the attacker replays the packets into the network. The goal is to make a false representation of the distance between the two colluding nodes or to disrupt the routing protocol by misleading the neighbor discovery process.
  Defense: Authentication, probing or a novel technique called packet leashes [2].

- *Blackhole and Grayhole*: during the Blackhole attack a malicious node advertises good paths to the destination node. That could lead to intercepting data packet or hinter the path-finding process. Grayhole is a special type of this attack where malicious node is dropping data packets.

- *HELLO flood*: an attacker transmits HELLO packets with high-powered transmitter and other nodes think that their sender is in the radio range of receiver, which is not true. They are trying to transmit packets to the attacker node, which is not successful because of it is too far away. (transport)
  Defense: Authentication or packet leashes by using geographic temporal information.

- *Byzantine attack*: one or more compromised nodes works in collusion and can have various impacts, like creating routing loops, forwarding packets through non-optimal routes or also selectively dropping packets.

- *Information disclosure*: compromised node can leak some information to unauthorized nodes in the network and the adversary may take an advantage of this information.

- *Resource-depletion attack*: when one malicious node is trying to deplete resources of other nodes in the network like CPU, battery power or bandwidth.

- *Acknowledgment spoofing*: in case that WSN uses such routing algorithms that require transmission of ACK packets, malicious node can overhear packet transmissions from the neighboring nodes and spoofs ACKs for providing false information to the nodes. Malicious node may in this way spread false information about the nodes status, for example ACK message from a node which is not alive.
  Defense: Bidirectional authentication.

d) **Transport layer attacks**

- *Flooding attack:* repeatedly creating a new connection request until the resources are exhausted or reached maximum limit so that no new requests are processed.
  Defense: Client puzzles, where each client is required to solve a puzzle as an evidence of a dedication. An attacker doesn't have infinite resources and it is impossible for him to create a new connection fast enough to cause resource starvation on the serving node.

- *De-synchronization attack*: disruption of an existing connection so that frames of victim node are being retransmitted and in worst case scenario such node is not able to successfully exchange data and it wastes resources as well.
  Defense: authentication of all packets communicated between nodes.

2) Attacks on secrecy and authentication: protection of communication channel against attacks from outside like eavesdropping, packet replay attacks and modification of spoofing of the packets.

a) **Attacks on privacy:** an attacker aims on gathering data from sensors or data which are not so important and marginal, but an adversary may find some sensitive information from them. There exist many ways of defense, but in this review it won't be described later. However, the reader can found more details in [2]. Defenses can be divided into anonymity mechanisms, policy-based approaches and information flooding.

- *Eavesdropping and passive monitoring* is the most common case and if the messages are not encrypted, the attacker could easily read a content of the messages.

- *Traffic analysis*: some sensor nodes may have a special role in WSN and the attacker may take an advantage of that later.
  Defense: the mechanism which is used against these attacks involves 4 strategies, which combination gives an extremely robust protection against any traffic analysis attacks. The author of this mechanism claims that base station is a central point of failure and that once the location of the base station is discovered, an adversary can disable of destroy it so the protection mechanism is considering also that. First, multiple parent routing schemes are introduced which allows that a node can forward a packet to one of the multiple parents. Secondly, packet traffic distribution. A controlled random walk is introduced into the multi-hop path traversed by a packet via WSN towards to the base station. Third strategy introduces random fake paths for confusion of the attacker from tracking a packet. The last strategy uses multiple, random areas of high communication activities so that the true location of the base station is harder to obtain.

- *Camouflage*: compromising a sensor node for later usage along with its masquerading. The goal is that it will look like a normal node in the network. Such node may advertise false routing information and attract packets from other nodes for further forwarding to specific nodes for systematic privacy analysis.

b) **Node replication attack**: an addition of malicious node to the network by replication of the identifier of already existing node. An attacker can disrupt the communication, corrupt packets or forward them to wrong routes, to cause false

sensor readings, gain physical access to the entire network, copy cryptography keys etc.
Defense: randomized multicast and line-selected multicast algorithms, whose details can be found in [2].

3) *Stealthy attacks against service integrity*: the goal of these attacks is that the network will accept a false data values created by an attacker.

4) *Physical attacks* in which there are more attack scenarios possible, except ones described below, it is possible to attack on the routing protocols in a way of routing table overflow, routing table poisoning, packet replication, routing cache poisoning or rushing attacks and some others, which could cause not only DoS but have many other impacts. For more details about such attacks and defenses please see [2].
Defense: the sensor nodes may be protected against tampering by tamper-proofing of the physical packages or tamper-resistant hardware in order to make the memory contents on the sensor chip inaccessible. It is not just hardware, but they can be equipped also by software for detecting physical tampering. Self-termination of sensor nodes is one of way of defending against possible data theft during the physical attack. The basic idea is to destroy all cryptography keys and data stored in the memory. It can be detected by period checking of neighborhood information for each node in the network. Accurate detection of such attack is however an open problem in the case of mobile sensor network.

V. Security Mechanisms for Wireless Sensor Networks

This chapter deals with encryption algorithms, key management protocols and security protocols and at the end the problematic of trust management frameworks, secure data aggregation and intrusion detection systems are all briefly described.

1) *Encryption algorithms*

They can be divided into symmetric and asymmetric cryptography. The first one uses only 1 key for both encryption and decryption and the latter one uses 2 keys for that purpose.

a) **Asymmetric cryptography**

Asymmetric cryptography is usually more robust and provides better security in some cases, but it is also usually much slower and requires more memory.
There are many algorithms in this category, but only a small subset of them was tested and is suitable for microprocessors. However, studies have shown that when using public key cryptography on WSN with the right choose of algorithms, parameters and optimizations, some of them are actually feasible. The most investigated and well-known algorithms in this category are RSA and EEC, briefly described below. Just for the completeness, some studies also discussed and investigated Rabin's Scheme and Ntru-Encrypt [7].

- *RSA (Rivest-Shamir-Adleman)*
  It is well-known public key algorithm which is computationally intensive and one cryptographic operation may contain thousands or millions of multiplication instructions, which could last tens of seconds up to minutes for the encryption and decryption. Furthermore, it also exposes a vulnerability to DoS attacks. Private key operations are very slow and therefore RSA has a limited use in networks like WSN.

- *Elliptic Curve Cryptography (ECC)*
  It has been found that ECC provides equal security for a far smaller key size and therefore communication overhead and processing are reduced. As for an example, RSA with 2048-bit key size provides accepted level of security and it has equivalent strength to ECC with only 224-bit key size.

During a comparison between RSA and ECC it has been observed that operation with private key with RSA is too slow even to the fact that RSA public key operation is slightly faster than operation with ECC. In ECC, both public and private key operations use the same point multiplication operations.

Regarding a key exchange protocol, which is a simplified version of SSL handshake, it involves client (initiating the communication) and server (responding to the initiation) parts. In WSN it is assumed that there is a central unit which administrates the whole network and each sensor has a certificate signed by a private key of such central unit. Key exchange mechanism works faster with ECC in total and for all reasons mentioned above, ECC has been chosen to be more appropriate than RSA in WSN. However, private key operations are still very expensive and slow and in some applications, it may be more suitable to use symmetric cryptography, which works ten or hundred times faster, require lower energy cost. In fact, most of the research studies considering the encryption in WSN are focused on symmetric cryptography.

b) **Symmetric cryptography**

The biggest problem here is to have a secure mechanism for distributing a single secret shared key which is used both for encryption and decryption. In this review it is discussed mainly in two classes: block encryption and bit encryption algorithms.

- *Bit-stream encryption*

Bit-stream encryption takes the input data as a stream of bits one by one. Examples are encryption algorithms RC2, RC4, RC5 and IDEA or hashing algorithms SHA-1 and MD5. According to studies and measurements, hashing algorithms are outperformed by encryption algorithms.

- *Block encryption*

Block encryption takes fixed-length blocks of data from the input text and after the encryption there are blocks of the same length on the output. A description of the most common algorithms is below:

i. Data Encryption Standard (DES, 3DES, DES-X)
DES has been a standard encryption algorithm for almost 25 years and it has been considered as insecure because of short key length. 3DES extended key length, but it seemed to be just a temporary solution. DES-X is a variant of DES which is enhancing the complexity of brute force attack with the usage of key whitening technique. Also, DES-X is faster than 3DES.

ii. Blowfish/Twofish
Blowfish is still considered to be secure, however the author itself recommended using more advanced version, Twofish, instead. Twofish allows making a tradeoff between size and speed. Actually, it was one of five finalists of AES, but it wasn't chosen. NIST chose Rijndael algorithm because of better performance both in software and hardware [8].

iii. Tiny Encryption Algorithm (TEA/XTEA/XXTEA)
The aim of this family of algorithms is to minimize the memory footprint and maximizing the speed. In original TEA there have been found some weaknesses and therefore XTEA and XXTEA were designed.

iv. Rijndael Algorithm (AES)
It is considered as advanced encryption standard selected by NIST in 2000. It is fast in both hardware and software and it is based on substitution permutation network. However, it is different from its predecessor DES, because the author didn't use Feistel network. According to the measurements in previous studies [2], it has been found that this algorithm is one of the best compromises between high security and energy efficiency.

v. *Skipjack Algorithm*
It was developed by NSA and it is one of the simplest and fastest block cipher algorithms, which is critical metric in embedded systems

vi. Scalable Encryption Algorithm (SEA)
It was designed for processors which has limited instruction set. Its design allows to parametrically changing text, key and processor size. This algorithm can be used in application requiring low-cost encryption or authentication.

vii. HIGHT Algorithm
Design of this algorithm allows low-resource hardware implementation which is suitable for computing devices like ones used in WSN. Its encryption algorithm provides a sufficient security even to the fact that it utilizes simple operations.

2) Operation Modes

Except of the selection of a proper algorithm for data encryption, it is needed to choose also operation mode, which many block encryption algorithms provide. They are needed to do safe repetitive usage of a block password under a one key. Data have to be divided into the separate parts for processing variable message lengths [8].

a) ***Electronic codebook (ECB)*** - it uses the same key for each 64-bit long block of plaintext and each block is encoded independently.
Usage: for secure transmission of single values.

b) ***Cipher block chaining (CBC)*** **-** the input to the algorithm is XOR of the next 64-bit block of plaintext and the preceding 64-bit block of already encrypted text.
Usage: general-purpose block-oriented transmission or authentication.

c) ***Cipher feedback (CFB)*** **-** the input is preceding ciphertext and the input processes j bits at one iteration. The final output is a result from the encryption algorithm which is XORed with the plaintext which can be used as a next unit of ciphertext in next iteration.
Usage: general-purpose stream-oriented transmission or authentication.

d) ***Outback feedback (OFB)*** **-** similar to CFB, but the input to the encryption algorithm is the preceding DES output.
Usage: stream-oriented transmission over noisy channel.

e) ***Counter (CTR)*** **–** the output is computed by XORing each block of plaintext always with an encrypted counter. The counter itself is increased for each subsequent block.
Usage: general-purpose block-oriented transmission for high-speed requirements.

f) ***Output codebook block (OCB)*** **-** Each block of plaintext is XORed with NONCE and L values. There is also generated a tag value for privacy.
Usage: authentication and privacy.

3) Key management protocols

Key management is a core mechanism for ensuring a security in WSN applications and it has received maximum attention of the researchers. The goal is to establish keys among all nodes in a secure and reliable way. It also has to deal with node addition and revocation in the network and it has to be extremely lightweight because of constraints of nodes in WSNs. As been told in the previous chapter, symmetric cryptography is less computationally intensive in comparison to public key cryptography techniques and therefore the most key management protocols are based on symmetric cryptography. The approaches to this problem can be divided into 2 categories, based on the network architecture: centralized and distributed.

a) ***Centralized***
In centralized network architecture there is only 1 entity which controls the generation, re-generation and distribution of keys and its called key distribution center (KDC) and the only existing protocol which is based on this is LKHW. The main drawback of this architecture and approach is that if the central controller fails, the entire network with its security is affected.

b) ***Distributed***
Most key management protocols described in the literature falls into this category. In comparison to centralized architecture, these protocols don't have a vulnerability of single point of failure. The most schemes can be grouped into deterministic and probabilistic types, depending on the probability of key sharing between two sensor nodes. Most of the key management protocols for WSNs belong to probabilistic key distribution schemes, but it has to be mentioned that the design of key management protocols is still largely open to research.

The detailed description of each one of them is out of the scope of this review, but at least brief explanation can be found in [2] and the comparison of them is depicted in Table 1 (also taken from [2]).

4) Security protocols

This chapter describes briefly all well-known security protocols which are handling encryption, secure routing, key management and which also provides defenses to many attacks mentioned in the Chapter 4 as a solution to a given WSN instance. Their summary also along with security requirements is in Table 2, taken from [1]. It has to be noted that not all of them were implemented on sensor nodes. According to [1], only TinySec and MiniSec have successful implementation. They both use SkipJack with 80-bit key size, but it has been shown in the past that in SkipJack, at least 128-bits need to be used for key length for data confidentiality. Regarding IEEE 802.15.4 it has been used also for WSN as well as for wireless private networks.

TinySec
Link layer security architecture which has been included in TinyOS. It supports two security modes: encryption with identity authentication or authentication only. They use MAC as identity authentication code and the second mode do not encrypt data. It depends according to a specific application which mode should be used.

Regarding encryption process, it uses Skipjack block encryption with 8-bit initialization vector (IV) and CBC mode with 80-bit key size. In practice there is a single pair of keys; one is used for data encryption and the second one for calculation of MACs. Such pair is selected for the whole network according to a given level of security. In comparison to others, like Zigbee, it provides relatively low security at low power consumption. It cannot provide a defense against message retransmission attacks

MiniSec
MiniSec provides high security at low power consumption: it uses block encryption for privacy and authentication. Also, Initiation Vector is used as a very few bits and there are basic gaps which are used during unicast and broadcast communication. In the unicast mode, the power consumption of radio is reduced by making extra computations and it also uses synchronized counters. Broadcast mode uses bloom filter mechanism.
It uses SkipJack for encryption in OCB mode with 80-bit key size. It should be noted that MiniSec is defenseless against DoS attacks and it cannot guarantee data integrity.

SPINS
SPINS consists of μTESLA protocol which is being used for identity authentication broadcasting, SNEP protocol for confidentiality, identity authentication between 2 nodes (MAC) and data freshness (the counter in MAC) and a routing protocol based on these. SNEP has also lower communication overhead, because the counter is kept on side of receiver and sender and not in the messages. RC5 has been chosen for encryption process.

LISP
LISP (Lightweight security protocol) aims at large-scale wireless networks which have a large number of nodes with limited resources. It is flexible and energy-sensitive protocol. Furthermore, it doesn't work with ACK or other control packages and messages and it is quite resistant to DoS attacks. Additionally, data integrity prevents data tampering of data which is sent and it uses key refreshing which provides protection against such nodes that could jeopardize the network.
It clusters nodes and determines a head for each of them and then creates a key server. To be more particular, it uses a special switching mechanism by using head cluster and key servers, which has following benefits: (i) effective broadcast without the need of sending ACK, (ii) it might recover the lost keys, (iii) it uses check bits which are not part of data message and (iv) refreshing a key without encryption or decryption data. Unfortunately, this protocol so far has not been implemented for WSNs.

LLSP
LLSP provides identity authentication, data integrity and semantic security by using only symmetric cryptography. It includes also a key mechanism which determines key management in WSNs like key distribution, their sharing and updates.

IEEE 802.15.4
This technical standard defines a medium access and physical layers for wireless private area networks (WPANs). It is being used in WSNs because of its low lost, flexibility and it doesn't require great power consumption. It includes Zigbee specification which uses strong encryption via AES-128 and provides freshness, integrity and authentication. Authentication is possible at (i) network level, which is achieved by using public network key and (ii) at device level, which is done by using unique link key between devices. Also encryption could be provided at network and device level. Additionally, Zigbee uses 3 types of keys: (a) master key for providing long term security between two devices, (b) link key for security between two devices and (c) network key which provides security on the network itself. It should be noted, that Zigbee provides high security at high power consumption.

LSec
This is authorization and authentication with simple key exchange and distribution mechanism. LSec uses data confidentiality, identity authentication, data integrity and some other security mechanisms like defense against intruders as well as it takes a benefit on asymmetrical and symmetrical encryption together.

LISA
LISA includes more security mechanisms together:

a) ***semantic security***: more ways of encrypting the same data using counter which is increasing always after each message
b) ***identity authentication****:* insurance that the data is from the node which is supposed to be
c) ***protection against replay attacks****:* mechanism which prevents old messages from being retransmitted again
d) ***weak freshness****:* there is a base station which verifies that a given message is generated after the previous one.

5) Other security mechanisms
Some other security mechanisms are briefly described here, so that the reader can have a better picture about security of WSN from a different point of view:

a) ***Trust management frameworks*** are dealing with high-level of security for protecting against other kinds of attacks. These attacks are beyond the capabilities of the cryptographic security, like judging the reliability and quality of the sensor nodes, data aggregation reliability and correctness of aggregator nodes and others. Such trust-based models and reputation-based frameworks usually require high computational power, which is a challenging task for WSN.

b) ***Secure data aggregation*** is needed because data transmission accounts for more than 70 percent of the energy cost of computation and communication. Some protocols works with special nodes called aggregators, responsible to carry out data aggregation operations. That means that if such node is compromised, an attacker can inject forged data or report false data to base station.

c) ***Intrusion detection systems (IDS)*** are based on rules which monitor a network or host for suspicious activity and they are trying to find abnormal behavior. In WSN, the research is still preliminary, because existing IDS schemes in ad hoc networks may not be adapted to WSNs due to constraints in WSNs. More detailed information is out of the scope of this review, but they can be found in further literature [2].

VI. CONCLUSION

The purpose of this paper was to introduce ideas, approaches and problems regarding security of wireless sensor networks. It was a short review dealing with a brief description of wireless sensor network which was followed by a issues regarding to the securing such network against a various threats. A security part of this paper was focused on encryption algorithms, key management mechanisms and security protocols. Regarding vulnerabilities, attacks and their defenses, it has been detailed following: attacks on network availability, on secrecy and authentication, service integrity, but also

physical attacks. This paper doesn't deal with things in too much detail; rather it provides a short summary which could be one of the first steps in education of individuals about the security of the wireless sensor networks.

It should be noted than during developing a security solution for these networks, the most appropriate one must be selected according to characteristics of the application so there is not one perfect solution for every possible scenario. Unfortunately, many security protocols or architectures have been tested only in simulated environment, so there is a big place for further research and experimentation. We would like to add, that during securing the whole network against all spectrum of various attacks on WSN, the effectivity is lowered and the price and effort are significantly increased. As this paper showed, there is a big variety of attacks on all layers and many defenses solve only a certain problem or a certain category of problems. In some cases, it may be possible that a security solution will open an opportunity to exploit another, new vulnerability.

Also, many security problems are not overcome yet, like exploitation of the availability of private key operations on sensor nodes, securing routing protocols for mobile sensor networks since they are not always stationary, time synchronization issues, defending DoS attacks and QoS with security services, since the performance is generally degraded with security implemented in WSNs. Also, in the future we can expect WSNs which are manipulating with continuous stream events and not just discrete ones like temperature. Those could contain video and image sensors which would produce continuous stream of data and that will bring another security challenge.

REFERENCES

[1] Dener, Murat. (2014). Security Analysis in Wireless Sensor Networks. International Journal of Distributed Sensor Networks. 2014. . 10.1155/2014/303501. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[2] S. Ahmad Salehi, M. A. Razzaque, P. Naraei and A. Farrokhtala, Security in Wireless Sensor Networks: Issues and challanges, 2013 IEEE International Conference on Space Science and Communication (IconSpace), Melaka, 2013, pp. 356-360.

[3] Heejung Byun, Jungmin So, "Node Scheduling Control Inspired by Epidemic Theory for Data Dissemination in Wireless SensorActuator Networks With Delay Constraints", IEEE Transactions on Wireless Communications, Vol.15, Issue: 3, pp. 1794-1807, 2015.

[4] J. Grover and S. Sharma, "Security issues in Wireless Sensor Network — A review," *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, 2016, pp. 397-404.

[5] Vishnu Pratap Singh Kirar, "A Survey of Attacks and Security Requirements in Wireless Sensor Networks", International Journal of Computer, Electrical, Automation, Control and Information Engineering, Vol. 8, number 12, 2014, pp. 91-96.

[6] M. Bhalla, N. Pandey and B. Kumar, "Security protocols for wireless sensor networks," *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, Noida, 2015, pp. 1005-1009. doi: 10.1109/ICGCIoT.2015.7380610

[7] K. A. Shim, "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577-601, Firstquarter 2016. doi: 10.1109/COMST.2015.2459691

[8] Altigani, Abdelrahman, Abdelmagid, Muawia, AND Barry, Bazara. "Analyzing the Performance of the Advanced Encryption Standard Block Cipher Modes of Operation: Highlighting the National Institute of Standards and Technology Recommendations" *Indian Journal of Science and Technology* [Online], Volume 9 Number 28 (26 July 2016)

Prot. Type	Protocol Name	Master Key	Pairwise Key	Path Key	Cluster Key	Scalabi-lity	Robust-ness	Proc. Load	Comm. Load	Storage Load
Deterministic										
	All pairwise	NA	Yes	No	No	Low	Low	Low	Low	High
	LEAP	Yes	Yes	Yes	Yes	Good	Low	Low	Low	Low
	BROSK	Yes	Yes	No	No	Good	Low	Low	Low	Low
	LKHW	Yes	Yes	No	Yes	Fair	Low	Low	Low	Low
	CDTKeying	NA	Yes	No	No	Good	Good	Med	Med	High
	IOS & DMBS	NA	Yes	No	No	Good	Good	Med	Med	High
Probabilistic										
	Basic	NA	Yes	Yes	No	Good	Good	Med	Med	High
	q-composite	NA	Yes	No	No	Good	Good	Med	Med	High
	Polynomial based	NA	Yes	No	No	Good	Good	Med	Med	High
	Blom based	NA	Yes	No	No	Good	Good	Med	Med	High
	Deployment knowledge based	NA	Yes	No	No	Good	Good	Med	Med	High
	Cluster key grouping	NA	Yes	No	No	Good	Good	Med	Med	High
	Location based	NA	Yes	No	No	Good	Good	Med	Med	Med

Table 1: Key Management Protocols

Security requirements/protocols	TinySec	SPINS	MiniSEC	LSec	LLSP	LISA	IEEE 802.15.4	LISP
Data confidentiality	+	+	+	+	+	+	+	+
Data integrity	+	+	–	–	+	+	+	+
Data authentication	+	+	+	+	+	+	+	+
Data freshness	–	+	+	–	+	+	+	–
Data availability	–	–	–	–	–	–	–	+
Implementation	TinyOS (Mica2)	–	TinyOS (TelosB)	–	–	–	TinyOS (MicaZ, TelosB)	–

Table 2: Security protocols