International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

Research Article

Security Attacks and Countermeasures for Wireless Sensor Networks: Survey

Qusay Idrees Sarhan[a*]

[a]Department of Computer Science, Faculty of Science, University of Duhok, Duhok, Iraq

Accepted 10 June 2013, Available online 15 June 2013, **Vol.3, No.2 (June 2013)**

Abstract

The security topic is a conclusive challenge for Wireless Sensor Networks (WSNs) due to the deployment nature and the resources limitations of wireless sensor devices used in such networks. Wireless Sensor Networks are used sometime in very sensitive applications, such as military, airports, and healthcare. Therefore, we must address the security concerns from the beginning of network design. Due to limited resources and computing constraints security in WSNs poses severe challenges as compare to the conventional wireless networks. There are currently massive studies in the field of sensor networks security. So far no comprehensive survey lists the security attacks which consider unique threats to the WSNs with suitable countermeasures against them. In this study we have addressed well known security threats and have provided the reasonable solutions towards effective countermeasures against the threats posed by this hot field of study.

Keywords: *Security attacks; Countermeasures; Cross-layer approach; Wireless sensor networks.*

1. Introduction

It is predicted that a Wireless Sensor Networks (WSNs) may contain up to thousands of sensor devices in the future, owing to their potentially low cost solutions for a variety of real applications Akyildiz, Weilian, Sankarasubramaniam & Cayirci (2002), the sensor networks are rapidly becoming a popular option. As compared to the conventional desktop computers, securing of a WSN is a rather difficult task. There are many obstacles in securing a WSN, including the limitation of the processing power, storage space, wireless channel bandwidth, and battery energy. Due to the great significance of the security issues, this chapter will address all possible threats and the measures that can be taken to overcome them.

Applications used in the various aspects of our practical lives such as energy management, logistics and inventory management, battlefield, and emergency response information, can now use the sensor networks as a potential option. As the sensor networks have inherent limitations in communication and computing abilities, they create unique security challenges. The sensor networks can be threatened by attacks if they are deployed in an unprotected environment. The adversary may compromise sensor nodes to accept the detrimental nodes as legitimate nodes and thus compromise the entire network. These issues may be solved to some extent by the incorporation of hardware and software enhancements, but in order to properly deal with the issues, it is best to apply strong countermeasures. These measures can be in the form of secure key management schemes, lightweight encryption techniques; secure routing protocols and malicious node detection mechanisms (Kocher, Chee-Onn, Ishii & Zia, 2010).

The threat models and an overview of the security issues are provided by this study. In addition, this study also gives a direction for the future research on methods to deal with the security issues in WSNs. The hindrances, security requirements, attacks and the defensive measures in WSNs are introduced in the following sections.

2. Security constraints and requirements for WSNs

As compared to other networks, the sensor network has many constraints. It is important to understand the constraints for WSNs first as discussed by Carman, Krus & Matt (2000), to develop a useful security mechanism while taking some ideas from the existing security techniques.

2. 1 Security Constraints For WSNs

2.1.1 Limitable Resources

A specific amount of resources such as code storage space, data memory size, and battery energy of the sensor devices are required by all the security techniques for implementing underlying application. In a wireless sensor device, these resources are very limited. Two major limitations will be discussed in this section:

*Corresponding author: Qusay Idrees Sarhan

- Limited storage space: a small amount of storage space is available for a tiny sensor device to apply the code. It is important to limit the size of the security algorithm code, to construct effective security techniques. For instance, Zigbex sensor type HBE has an 8 bits, 7.372 MHz ATmega128L RISC MCU with only 4 Kbytes SRAM, 128 Kbytes flash memories, and 512-Kbytes flash storage (HBE-Zigbex).
- Power limitation: the power energy is another strong constraint to the wireless sensor abilities. The energy must be conserved, once the sensor nodes are deployed in a sensor network to extend the individual life of a sensor node and then the entire network.

2.1.2 Unreliable Wireless Channel

The secure wireless network depends on underlying protocols, which eventually depends on the wireless channel within the entire network (Kocher et al., 2010).

- Unreliable transfer: the packets may get damaged due to channel errors or dropped at highly congested nodes in the network, due to the inherent unreliable wireless routing in sensor network.
- Conflicts: some packets may collide in the middle of transfer, due to the broadcast nature of the wireless network, which will lead to a conflict.
- Latency: the multi-hop routing, congestion, and node processing delay in the sensor network are responsible for latency. It is difficult to achieve real synchronization among sensor nodes within the entire network, because of the latency.

2.1.3 Unattended Environment Operation

Sensor nodes suffer physical attacks in an open environment, as the inherent unattended deployment nature of WSNs in an environment is open to adversary attacks and natural disasters such as bad weather and bushfires.

2.2 Security Requirements for WSNs

The security goals in a sensor network are briefly overviewed by this section. The typical network requirements and the unique requirements suited solely to WSNs are all included in the requirements of the WSNs.

2.2.1 Data Confidentiality

The issue of securing messages must be addressed by any network with security issues and is an important network security issue. This has the potential of hiding messages from passive attackers. The following facts are considered in the confidentiality of the sensor networks:

- The sensor readings must not be leaked to its neighbours.
- It is important to build s secure channel, as the sensor nodes may communicate highly sensitive data such as secret key distribution.
- To add protection against the traffic analysis attack, the sensor's identities and public keys should also be encrypted to an extent.

2.2.2 Data Integrity and Authentication

The ability to confirm that the message has not been tempered with while it was on the network is referred to as integrity. The modification of the data packet is not the only harm an adversary can inflict. By injecting the additional packets, it can also change the whole packet stream. Therefore, it is important to ensure that the data used has originated from the correct source before it is used in the decision -making process.

Verification of the data being sent to the claimed sender is allowed by the data authentication for the receiver. Data authentication can be achieved through a purely symmetric mechanism, in case of a two party communication.

2.2.3 Data Freshness

Ensuring the freshness of each message is also important, concurrent with the goals mentioned in the previous section. Data freshness gives an idea as to whether the data is recent and it also makes sure that the data has not been replayed. When there are shared-key strategies applied in the design and they need to be changed over time, this requirement is especially important.

2.2.4 Availability

The ability to use the resources is verified through availability. In addition, it makes sure that the network is available for the message to move on.

2.2.5 Self-Organization

According to the various environments, every sensor node needs to be independent and flexible enough to be self-organizing and self-healing in a WSN network to work on an ad hoc basis. In a sensor network, no fixed infrastructure is available for the purpose of network management. The WSNs security is also challenged by this inherent feature.

2.2.6 Time Synchronization

Some form of time synchronization is the basis of the sensor network applications. An individual sensor radio may be turned off for some time periods to conserve power. As the packets travel between the two sensors, the sensors may want to calculate the end-to-end delay of packet. Group synchronization may be required by a more collaborative sensor network for tracking the underlying application.

2.2.7 Secure Localization

The network ability to accurately and automatically locate each sensor node in the network will determine the use of sensor network. To pinpoint the location of a fault within the entire network, sensor network requires accurate location data to work effectively.

3. Threats on WSNs

A variety of attack techniques, such as the node takeovers, the DoS attack, attacks on the routing protocols, and attacks on the physical security of a node are present in the sensor networks. Some common attacks such as (Denial of Service (DoS), wormhole, sinkhole, Sybil, traffic analysis, node replication, and physical attacks on WSNs (Kocher and others, 2010; Walters, Liang, Shi, & Chaudhary, 2006) are all discussed subsequently.

3.1 Types of DoS Attacks

Jamming refers to the transmission of a radio signal that interferes with the radio frequencies being used by the sensor network (Wood & Stankovic, 2002). There are two forms of jamming; constant jamming and intermittent jamming. The jamming of the entire network is called constant jamming, while in intermittent jamming, the sensor nodes are able to exchange messages periodically.

- The link layer attacker may intentionally violate the communication protocols such as ZigBee ("Zigbee Specification," 2005) or IEEE 802.11b. To generate collisions, the messages are continuously transmitted. Retransmission process would also be required for any packets lost by collisions.
- A node may take advantage of a multi-hop network at the routing layer by refusing to route messages. As a result, there will be no exchange of messages with any neighbour who tries to route through the malicious node.
- The transport layer is vulnerable to flooding attacks, which refers to the sending of many connections requests to the malicious node. Allocation of resources to address the connection request is required in this case. The sensor nodes will be rendered useless, when the node's resources are exhausted.

3.2 Wormhole Attack

By using a fast (low latency) link, an adversary transmits the received packet from one point of the network to the other point. The transmission range between these points is longer as compared to the actual transmission range of the hop link. For instance, the packets can be relayed by any node without delays between two nodes.

3.3 Sinkhole Attack

In a sinkhole attack case, an adversary attempts to attract the network traffics of a particular area around compromised node. For instance, a high quality link towards the BS may be claimed to be in the possession of the adversary. A powerful device, such as a laptop with communication range more than the actual range, may be used by the adversary to achieve this target. The adversary also convinces the nodes around the malicious node that he/she has the shortest link to the BS.

3.4 The Sybil attack

The Sybil attack is defined by Newsome, Shi, Song & Perrig (2004) as a malicious node illegitimately taking on multiple identities. Kocher et al. (2010) define the notion of Sybil attack in which Sybil node offers multiple identity IDs to neighbors. As there are many distinguishable nodes, the legitimate node will also accept the Sybil node. Originally, this attack was taken as the attack that had the potential of undermining the redundancy mechanisms of the distributed storage systems in peer-to-peer networks.

3.5 Traffic Analysis Attacks

The attacker can simply disable the BS to effectively render the network useless. Two attacks were demonstrated by Deng, Han & Mishra (2004) that can identify the BS in the network without the need to understand the packet contents. The nodes closer to the BS tend to forward more packets as compared to those further away, as is evident from the rate monitoring attack. An attacker generates events and monitors to whom a node sends its packets while in a time correlation attack.

3.6 Node Replication Attacks

An attacker can add a node to an existing sensor network by copying the Node Identity (ID) of an existing node. A sensor's performance can be disrupted and the packets can be corrupted or even misrouted in the presence of a replicated node. A disconnected network and false sensor readings are obtained as a result (Parno, Perrig, & Gligor, 2005).

3.7 Physical Attacks

The small form factor of the nodes, coupled with the unattended and distributed nature of their deployment can make them vulnerable to physical attacks (Wang, Gu, Schosek, Chellappan, & Xuan, 2004). The losses are irreversible as the sensors are permanently damaged by the physical attacks. The cryptographic secrets can be accessed by the attackers. In addition, the attackers can tamper with the associated circuitry, spoof or modify programming in the nodes, and replace them with malicious nodes. The attacker is in complete control of all these operations.

4 Countermeasures for WSNs

The countermeasures for satisfying the requirements and the protection of the sensor network from the attacks are

described in this section. Table 1 summarizes the attacks and countermeasures in a layering model for WSNs (Zia & Zomaya, 2006).

Table (1): Layering approach in WSNs: attacks and countermeasures (Kocher et al., 2010)

Layers	Attack types	Countermeasures
Application Layer	Subversion and Malicious Nodes	Malicious Node Detection and Isolation
Network Layer	Sinkholes, Wormholes, Sybil, Routing Loop	Key Management, Secure Routing
Data Link Layer	Link Layer Jamming	Link Layer Encryption
Physical Layer	DoS and Node capture attacks	Adaptive Antennas, Spread Spectrum

4.1 Defending Against DoS Attacks

The identification of the jammed parts of WSN and effectively routing around them is one strategy of defending against the jamming attacks. Some measures are listed below:

- The nodes might utilize a Medium Access Control (MAC) admission control that is rate limiting in order to handle the jamming at the MAC layer. The requests, that have been designed to exhaust the power reserves of a node, will be ignored by the network. As the network must be able to handle any legal large traffic volume, this process is however not foolproof.
- Aura, Nikander & Leiwo (2001) have recommended the use of client puzzles to overcome the flooding DoS attacks at transport layer. This will allow differentiation between the node's commitments to make the connections by using some of their own resources.

In the new Coremelt attack, the attackers only create traffic between each other and not the victim host, unlike the current DoS attack that is targeted towards a specific victim. The utilization of the puzzles is termed as the best solution to DoS attacks in the current work, which is able to increase the cost for the attacker to consume the victim resources. The attacker will no longer be able to launch a successful attack Studre & Perrig (2009), if the amount of work required to complete the puzzle is sufficiently large.

4.2 Defending Against Attacks on Routing Protocols

To combat against the attacks such as the sinkhole, wormhole and Sybil attacks (Hu, Perrig, & Johnson (2003); Newsome et al. (2004)), there is a great need for both secure and energy efficient routing protocols for the field of WSNs.

An intrusion tolerant routing protocol called INSENS is described by Deng, Han & Mishra (2006). It is designed with the consideration of the route information within the network intrusion and to allow it to limit the scope of an intruder harming the network data. The routing tables are computed on behalf of the individual sensor nodes by a powerful BS. There are three phases of completing this and each phase is vulnerable to the following attacks:

- By sending a bogus request message, the sensor node might deceive the BS.
- When forwarding the requested message to its neighbours, a compromised node might also include a bogus path in the requested messages.
- The requested message may not be requested at all.

They use a scheme similar to µTESLA technique presented by Perrig, Szewczyk, Wen, Culler, & Tygar (2002) in which one-key chains are used to identify a message originating from BS, to overcome these issues as a countermeasure.

The TRANS routing protocol is described by Tanachaiwiwat, Dave, Bhindwale & Helmy (2003). The protocol was designed to be applied in data centric networks. The authors use the loose-time synchronization asymmetric cryptographic scheme to ensure confidentiality of the message. The existing technique, µTESLA, is used in their implementation to ensure the authenticity and confidentiality of the message.

A dangerous threat to WSNs is the Wormholes attack. In this attack, the node eavesdrops on a series of packets and tunnels through the sensor network to another compromised node after which the packets are replayed. The distance between the two colliding nodes is misrepresented. By misleading the neighbour discovery process, the process can also be used to more generally disrupt the routing protocol. This attack has not been dealt with yet.

To assure that a particular identity ID is the only one being held by a given physical node, a mechanism is needed to counter the Sybil attack. Newsome and others.(2004) presents two methods to assure the identities, as follows:

- Direct Validation: whether the node is valid or not is witnessed directly by a trusted node. A radio resource test is included in the direct validation. A different channel is assigned by the sensor node in this test, which is used to communicate. The channel is randomly checked by the node. The node transmitting on the channel is assumed to be a physical node only if there is a transmission on the channel.
- Indirect Validation: the validity of the joining node is allowed to be witnessed by the trustworthy third party node.

4.3 Combating Traffic Analysis Attacks

A random walk forwarding mechanism was applied by Deng et al.(2004) that forwards the packets to the node occasionally other than the parent node. The identification of the clear path would become difficult from the sender to

BS and the rate monitoring attack would be eliminated by its help. The time correlation attack would still affect the system.

A fractal propagation strategy was suggested to deal with the time correlation attack. A forged packet will be generated by the node in this mechanism, when its neighbour is forwarding a packet to the BS. A forged packet can also be generated by another neighbour, to whom the forged packet was also sent. The Time-To-Live (TTL) is used by these packets to decide when the packet should be discarded. The BS is effectively hidden from the time correlation attacks by implementing this approach.

4.4 Key Management Techniques and Protocols

The notion of security becomes essential when the sensor nodes are deployed in a hostile environment. There may be various types of malicious attacks threatening the sensors. The main challenge is the setting up of the pair-wise secret key between the communicating sensor nodes.

Security is regarded as important as performance and energy efficiency for a huge number of applications (Qiu et al., 2009). To solve the key agreement problems in WSNs, key pre-distribution is a good concept. In this case however, the attacker may gain access to the secrets after the node has been compromised. The authors have proposed a new key pre-distribution scheme, based on the KIE-WSNs. No threat remains even after the n-1 nodes are compromised, due to their ability to obtain both a semantic security and optimal KIE-(m-1, m) safety.

Haowen, Perrig & Song (2003) describe the key ring distribution mechanism. Number of keys is randomly selected from a pool of keys generated offline before deployment of the nodes. These keys form the key ring pre-loaded to unique node to be used later for security provision.

A single security requirement may not fit all types of communications in WSNs necessarily, as stated by Zhu, Setia & Jajodia (2003). Depending on what the node is communicating with, a set of four different keys is introduced. The initial key is pre-loaded to each sensor node offline and further set of keys is created post-deployment. To avoid the network from suffering from additional compromised nodes, the initial key should be deleted after the key setup phase in cases when the sensor network is compromised.

A set of secret keys between two nodes can be created through a scheme proposed by Haowen & Perrig (2005), which is based on the common trust of a third node anywhere within the sensor network. Over the network, the nodes and their shared keys are deployed. There is always, for instance, a node C for the two nodes A and B, to share a key with both A and B. Therefore C can be used to route the key establishment protocol between both the A and B nodes. The node C should be a trustworthy node to ensure more safety.

Far less computational power and energy is present in an individual node as compared to Base Station (BS) (Huang, Cukier, Kobayashi, Liu, & Zhang, 2003). Considerable resources are used to perceive the major cryptographic burden on the BS. Owing to the fact that relatively small key sizes are required to provide an expected security level, the elliptic curve cryptography is often used on the side of the node. To create the lawfulness of a public key, this technique also uses certificates. An elliptic curve implicit certificate technique is used as the basis for the certificates. The lawfulness of the nodes before joining the network can be verified through these certificates.

The possibility of the utilization of radio finger-printing to identify the origin of messages in sensor network as done by Bonne Rasmussen & Capkun (2007) is outlined in many recent papers. To create a list of sensor nodes that are authorized members of the network, it is easy to use such mechanisms. Therefore, the presence of the attacker's devices is recognized.

More energy efficient pair-wise key establishment schemes are explained by Kuldeep & Garimella (2009). By communicating with their neighbouring nodes, the nodes can set up their own keys. The division of the network into levels and sectors to restrict the neighbourhood of a particular node is the key idea. It has been proven by authors in the various simulation tests, that there are many benefits of the protocol in terms of energy and storage over existing approaches.

A successful protocol for key establishments in WSNs has been recommended by the current work and must have features of establishing new keys without the requirement of any secret values in both the participating nodes. As long as the attacker is remote, the passive or active attacking nodes cannot perform Man-in-the-Middle (MitM) attacks and will not be able to insert its computationally more powerful nodes into the network; the same idea was used by Seshadri, Luk & Perrig (2008).

Manipulating the messages is required by the attackers in most of the routing attacks such as Sinkhole, Wormhole, and Sybil. An efficient scheme for key management is required to prevent this. The Sinkhole and Wormhole attacks are no longer dealt with by the existing solutions in literature (Sharma, Ghose, Kumar, Kumar, & Pandey, 2010).

To secure the hierarchical clustering based WSNs, my existing work entitled " Novel Secure Key Management (NSKM) " technique was proposed by Gawdan, Chee-Onn, Zia, & Sarhan et al. (2011) as a robust, adaptive and lightweight secure key scheme. Within a specific cluster, the set of post generated keys are created between the neighbouring nodes and updated at each round of the underlying protocol work. With the flavours of cross-layer approach between the various components of the protocol stack of the node, it was able to increase the resistance against the node capture attack.

4.5 Secure Broadcasting and Multicasting

In contrast to the traditional point-to-point communication on the internet network, the major communication pattern of WSNs is broadcasting and multicasting. The secure multicasting and broadcasting pattern is explained in this section:

- Secure multicasting pattern: while considering the benefits of a logical key hierarchy, Di Pietro, Mancini, Law, Etalle & Havinga (2003) proposed a directed diffusion based multicast technique for WSNs. The root of the key hierarchy is the key distribution centre, while the individual sensor nodes make up the leaves. The logical key hierarchy is modified by using this technique to build a directed diffusion based logical key hierarchy. Mechanisms for sensor nodes are provided by this technique by joining and leaving groups where the key hierarchy is used to effectively re-key all the nodes within the leaving node's hierarchy.
- Secure broadcasting pattern: a routing aware based tree was suggested by Lazos & Poovendran (2002) where the leaf nodes are assigned keys based on all forward nodes above them. The routing information is used by this technique and is more energy efficient than the mechanisms that arbitrarily arrange the sensor nodes into the routing tree.

Mechanisms that take advantage of geographic location information through GPS instead of routing information, are explained by Lazos & Poovendran (2003). It is observed that since nodes within a cluster will be able to reach one another within a single hop, the sensor nodes are grouped into clusters. A key hierarchy is constructed as done by Lazos & Poovendran (2002).

4.6 The Malicious Nodes Monitoring Mechanism for WSNs

The functions of such mechanisms are described by Zia (2008). For instance, the node A is a monitoring node. This node will send a message to the node D and then the behaviour of node D will be monitored. Figure 1 shows a message sent by node A. The sent message is secured with the network key K_N. Figure 2 shows an altered message sent by the node D toward the node F.

The impact of most of the known attacks such as Sinkholes, Selective forwarding, Wormholes and Sybil attacks will be mitigated or eliminated by this mechanism. To identify the suspicious behaviour of the neighbouring nodes, this monitoring mechanism can be applied on the basis of the reported data from other monitoring nodes. The node is declared malicious, if the number of suspicious entries concerning a particular node exceeds a set pre-defined threshold value. The neighbours are alarmed and the BS is reached. The malicious node is blacklisted by the Base station (BS) and all the incoming traffic from the node is discarded.

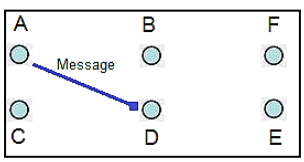

Figure (1): Message sent by sender node A

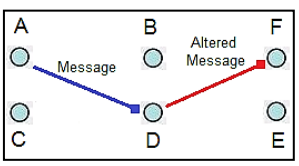

Figure (2): Message forwarded by node D

4.7 Complete Security Framework for WSNs

Sharma, Ghose & Kuldeep (2009) proposed an integrated holistic security framework to provide the security services for WSNs. To analyze the level of security based on cross-layer approach, the authors have added one extra module ISA to the protocol stack of the node. Many components, such as Intrusion Detection System, Key Management Scheme, Trust Framework, and Link Layer Communication Protocol make up the framework. The level of security is associated with the overhead added by this technique, which in turn relies on the underlying application. This framework is incomplete due to the lack of secure routing protocol that incorporate with other modules of the framework to provide multi-level security services for WSNs.

A particular solution is applicable to a single layer itself, since most of the existing security approaches in literature for WSNs are layer wise. Therefore, it is a challenge to integrate these solutions in a unified framework (Gawdan, Chee-Onn, Zia & Gawdan, I. Q , 2011; Kocher et al., 2010).

4.8 Cross-layer Based Selfish Node Detection techniques

To achieve a secure and a robust scheme for most of the current applications, the selfish nodes detection technique is important. Part of the network within the area including that node will eventually go out of service, as an arbitrary node intentionally stops forwarding packets for its neighbours. This issue was addressed through the following approaches (I.S. Gawdan et al., 2011; Mingbo, *Xudong, & Guangsong*, 2006):

- To guarantee that a node has enough interest to forward packets to its neighbours or cluster member nodes, the monitoring mechanisms in the communication protocols are applied.
- The detection of the selfish nodes and their eventual blacklisting is a possibility that can be achieved through the development of the selfish nodes detection techniques for the communication protocols.

To provide multi-levels security services, this study is strongly recommended the creation of a new approach, such as a novel unified framework based on cross-layer idea as a suitable solution for providing security for WSNs after understanding the attack issues against such a network. The network state is the basis for this framework, combined with the cross-layer approach. This approach also eliminates the effects of the attacks and increases the lifetime of the entire network. The cross-layer architecture also mitigates the communication overheads compared with a standard one-layer approach, and gives more robustness against all well-known attacks including the selfish and malicious behaviour nodes (Gawdan, Chee-Onn, Zia & Gawdan, 2011).

5. Conclusions and future direction

5. 1 Conclusions

In many applications, the WSNs have become a promising aspect. A variety of attacks can threaten the sensor networks in the absence of proper security techniques. The four main aspects of WSNs security have been outlined ahead constraints, requirements, attacks, and countermeasures. A number of important subtopics within each category are dealt with in this paper, such as routing, key management, denial of service and others. General overviews of a broad area of wireless sensor network, security issues and threats have been provided in this study. It also provides the main citations that will assist the researchers in their further study of the topic. The need for security in critical applications will increase with more widespread use of WSNs. To provide lightweight countermeasures against attacks in WSNs available nowadays, the current work encourages the idea of cross-layer based security solutions.

5.2 Future Direction

The following are prospects of progressing onwards from this study:

- The security mechanism in routing protocol increases the energy consumption which leads to a reduction in the network lifetime. So, the strength of the security mechanism requires a trade-off with its energy consumption, a fact that can be taken into consideration in future security protocol designs.
- The current symmetric key-based security protocols cannot yet solve the problems of resilience and authentication to prevent physical capture of the nodes for the WSNs. New approaches can be taken to address this issue.
- The security issues at the physical layer of the protocol stack of the sensor node are still open for investigation. Future works can attempt to find ways to prevent attacks at the physical layer.

References

Akyildiz, I., Weilian, S., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks.*IEEE Communications Magazine*, *40*(8), 102-114

Aura, T., Nikander, P., & Leiwo, J. (2001). Dos-Resistant Authentication with Client Puzzles. Paper presented at the 8th *International Workshop on Security Protocols*.

Bonne Rasmussen, K., & Capkun, S. (2007, 17-21 Sept. 2007). Implications of radio fingerprinting on the security of sensor networks. Paper presented at the Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. *Third International Conference on*.

Carman, D. W., Krus, P. S., & Matt, B. J. (2000). Constraints and Approaches for Distributed Sensor Network Security: *NAI Labs,Network Associates*.

Deng, J., Han, R., & Mishra, S. (2004). Countermeasures Against Traffic Analysis in Wireless Sensor Networks: *University of Colorado at Boulder*.

Deng, J., Han, R., & Mishra, S. (2006). INSENS: intrusion-tolerant routing in wireless sensor networks. *Computer Communications*, 29(2), 26-43.

Di Pietro, R., Mancini, L. V., Law, Y. W., Etalle, S., & Havinga, P. (2003). LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. Paper presented at the *International Workshop on Wireless Security and Privacy (WiSPr 03)*.

Gawdan, I. S., Chee-Onn, C., Zia, T. A., & Gawdan, I. Q. (2011). Cross-layer based security solutions for wireless networks. *International Journal of the Physical Sciences* 6(17), 4245-4254.

Gawdan, I. S., Chee-Onn, C., Zia, T. A., & Sarhan, Q. I. (2011, 20-22 Sept. 2011). A Novel Secure Key Management Module for Hierarchical Clustering Wireless Sensor Networks. Paper presented at the 2011 Third *International Conference on. Computational Intelligence, Modelling and Simulation (CIMSim)*,

Haowen, C., & Perrig, A. (2005). PIKE: peer intermediaries for key establishment in sensor networks. Paper presented at the INFOCOM 2005. Proceedings 24th Annual Joint Conference of the *IEEE Computer and Communications Societies*.

Haowen, C., Perrig, A., & Song, D. (2003). Random key predistribution schemes for sensor networks. Paper presented on *proceedings 2003 Symposium at the Security and Privacy*.

HBE-Zigbex. *www.hanback.co.kr*. Ubiquitous Sensor Networks.

Hu, Y. C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. Paper presented at the INFOCOM 2003. Twenty-Second Annual Joint *Conference of the IEEE Computer and Communications*.

Huang, Q., Cukier, J., Kobayashi, H., Liu, B., & Zhang, J. (2003). Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks. Paper presented at the 2nd *ACM International Conference on Wireless Sensor Networks and Applications (ICWSNA 03)*

Kocher, S. I., Chee-Onn, C., Ishii, H., & Zia, T. A. (2010, November 26-28). Threat Models and Security Issues in Wireless Sensor Networks. Paper presented at the *International Conference on Intelligent Network and Computing (ICINC 2010)*, Kuala Lumpur, Malaysia.

Kuldeep, & Garimella, R. (2009, October 28-29). Distributed Key Management For Wireless Sensor Networks.presented at the 5th *ACM symposium on QoS and Security for Wireless and Mobile Networks (QoSWinet 09)*, Tenerife, Canary Islands, Spain.

Lazos, L., & Poovendran, R. (2002). Secure Broadcast in Energy-Aware Wireless Sensor Networks. Paper presented at *the IEEE International Symposium on Advances in Wireless Communications (ISWC 02*), BC,Canada.

Lazos, L., & Poovendran, R. (2003, 6-10 April 2003). Energy-aware secure multicast communication in ad-hoc networks using geographic location information. Paper presented at the Acoustics, Speech, and Signal Processing, 2003. *Proceedings IEEE International Conference (ICASSP '03)*.

Mingbo, X., Xudong, W., & Guangsong, Y. (2006, June 21-23). Cross-Layer Design for the Security of Wireless Sensor Networks. Paper presented at the 6th *World Congress on Intelligent Control and Automation*, Dalian, China.

Newsome, J., Shi, E., Song, D., & Perrig, A. (2004, 26-27 April 2004). The Sybil attack in sensor networks: analysis & defenses. Paper presented at the Third *International Symposium on Information Processing in Sensor Networks, (ISIPSN 04)*, pp. 259–268

Parno, B., Perrig, A., & Gligor, V. (2005, 8-11 May 2005). Distributed detection of node replication attacks in sensor networks. *IEEE Symposium at the Security and Privacy*, 2005.

Perrig, A., Szewczyk, R., Wen, V., Culler, D., & Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5), 521-534.

Qiu, W., Zhou, Y., Zhu, B., Zheng, Y., Wen, M., & Gong, Z. (2009). Key-Insulated Encryption Based Key Pre- Distribution Scheme for WSN Advances in Information Security and Assurance (Vol. 557, pp. 200 209): *Springer* Berlin /Heidelbeg

Seshadri, A., Luk, M., & Perrig, A. (2008, June 2008). SAKE:Software Attestation for Key Establishment in Sensor Networks. Paper presented at the *International Conference on Distributed Computing in Sensor Systems (DCOSS 08)*

Sharma, K., Ghose, M. K., & Kuldeep. (2009). Complete Security Framework for Wireless Sensor Networks. *International Journal of Computer Science and Information Security*, 3(1), 196-202.

Sharma, K., Ghose, M. K., Kumar, D., Kumar, R. P., & Pandey, V. K. (2010). A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks. *International Journal of Advance Science and Technology (IJAST)* 17, 31-44.

Studre, A., & Perrig, A. (2009, September 21-23). The Coremelt Attack. Paper presented at the *European Symposium on Research in Computer Security (ESORICS 09)* Saint-Malo, France.

Tanachaiwiwat, S., Dave, P., Bhindwale, R., & Helmy, A. (2003). Poster Abstract Secure Locations: Routing on Trust and Isolating Compromised Sensors in Locationaware Sensor Networks. Paper presented at the Proc. of the 1st *International Conference on Embedded Networked Sensor Systems (ICENSS 03)*.

Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2006). Wireless Sensor Network Security: A Survey. In Y. Xiao (Ed.), Security in distributed, grid, and pervasive computing*: Publications, CRC Press*

Wang, X., Gu, W., Schosek, K., Chellappan, S., & Xuan, D. (2004). Sensor Network Configuration under Physical Attacks: *The Ohio-State University*.

Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *IEEE Computer*, 35(10), 54-62.

Zhu, S., Setia, S., & Jajodia, S. (2003). Leap: Efficient Security Mechanisms for Largescale Distributed Sensor Networks. Paper presented at the 10th *ACMconference on Computer and Communications Security (CCS 03)*, New York, NY, USA.

Zia, T., & Zomaya, A. (2006, Oct. 2006). Security Issues in Wireless Sensor Networks. Paper presented at the *International Conference on Systems and Networks Communications (ICSNC '06)*.2006.

Zia, T. A. (2008). A Security Framework for Wireless Sensor Networks. PhD thesis submitted to the *University of Sydney*, Australia.

ZigBee Alliance (2005). ZigBee specification. *Technical Report. Document* 053474r06, Version 1.0.