Security Issues in Wireless Sensor Networks: Attacks and Countermeasures

Kahina CHELLI

Abstract—**Wireless sensor networks are one of the most exciting and challenging research domains of our time. They have a great potential to be deployed in wide mission-critical applications, such as military monitoring, health care as well as civilian applications. The highly sensitive nature of collected information makes security in these special networks a crucial concern. Owing to the hostile nature of their deployment environments, the wireless medium and the constrained nature of resources on the tiny sensor devices used in such networks, security poses more severe challenges compared to the traditional networks. As attacks to any part of the hardware or software may gives significant damages to these networks. Indeed, the development of effective and efficient defense mechanisms to those attacks must be addressed at every stage of the system design.**

This paper tends to outline the major aspects of wireless sensor networks security. We discuss some security attacks and their classification mechanisms. Some related works and proposed schemes concerning security in these networks are also discussed. And finally we conclude the paper delineating the research challenges and future trends toward the research in wireless sensor network security.

Index Terms—**wireless sensor networks, network attacks, security design challenges, symmetric and asymmetric cryptography.**

I. Introduction

Wireless sensors networks have emerged as modern day technology under the push of recent technological advances in Micro Electro-Mechanical Systems (MEMS) technology, wireless communications and digital electronics [1]. Sensor node is a smart, tiny, self-organizing low cost multi-functional device, equipped with battery, radio communication, microcontroller and sensors. It has very limited processing capability, battery power, and memory and also a restricted field of sensing [2] [3] [4]. A wireless sensor network (WSN) is application-specific, designed to monitor and control physical environments from remote locations with better accuracy. Therefore, multiple spatially distributed sensors nodes collaborate and in-network process collected information. They are connected to each other through short range wireless links, used as an infrastructure to forward the collected report to an authorized user-end over base station [1] [5] [6] [7].

Indeed, WSNs gaining rapid worldwide attention because of their potentially low cost solutions to a variety of real-world challenges. Many other favoring factors of WSNs use are self-organizing, self-healing, having dynamic network topology to cope with node malfunctioning and failures, mobility of deployed nodes, unattended operation, ability to withstand bad environmental conditions, heterogeneity of nodes, scalability, at the time of deployment and after deployment, as well easy use [2] [6]. WSNs have the potential to be deployed in mission-critical applications such as military surveillance, or medical applications, e.g., Body Area Network (BAN) [8], where several low-cost nodes are attached to the human body to collect data and is periodically transferred to a sink node for further processing. Sink nodes are also often designed to work as gateways to transfer data to eHealth systems residing in the cloud. These BANs could be deployed in hospitals or at homes for ambient and assisted living monitoring elderly. Patient data is often categorized as high sensitive information that must be transferred in an encrypted form and nobody can inject faked data as this can have serious impacts. Indeed, securing WSNs is of paramount importance in order to protect the sensitive data involved. This necessity of effective and efficient security techniques to secure sensor networks has attracted a great deal in the recent years.

The rest of the paper is organized as follows. In section II we summarize the major design obstacles for the sensor networks security. In section III the requirements of WSNs security are listed. The major threats and attacks against these networks are categorized in section IV, and we outline the corresponding defensive measures in section V. Finally, section VI points out our future observation and concludes the paper.

II. Major Design Challenges

WSNs have many constraints from which new challenges stand out. The extreme resource limitations of sensor nodes and unreliable communication medium in unattended environments make it very difficult to directly employ the existing security approaches on a sensor platform due to the complexity of the algorithms [2] [4] [6] [8]. Indeed, the understanding of these challenges within WSNs provides a basis for further works on sensor networks security.

A. Very Limited Resources

WSNs pose unique challenges because of the strict resource constraints on each individual sensor. Embedded devices with very limited resource must implement complex, distributed, ad-hoc networking protocols. Size reduction of sensor nodes is essential to cut costs and create more

Manuscript received March 23, 2015; revised April 12, 2015.
Kahina CHELLI, University of Mouloud MAMMERI Tizi-Ouzou 15000 Algeria; e-mail kahinachelli@gmail.com

applications. As physical size decreases, so does energy capacity. The underlying energy constraints end up creating computational and storage limitations that lead to a new set of design issues. For example, Zigbex sensor type HBE has an 8-bit, 7.372 MHz ATmega128L RISC MCU with only 4 Kb SRAM, 128 Kb flash memories and 512 Kb flash storage [5]. With such limitations, the software built for the sensor must also be quite small.

B. Unreliable Communication

Due to the wireless medium that is inherently broadcast in nature, packets may get damaged due to channel errors and conflict will occur, or dropped at highly congested nodes in the network. As well, an attacker can launch Denial-of-Service (DoS) attacks without much effort, etc. Furthermore, the multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution.

C. Unattended Operations

Sensors nodes interact closely with their physical environments, process and fuse data, and eventually create new knowledge that must be presented to an end-user. These tiny nodes are often deployed in open, large-scale and even hostile areas. Potential issues range from accidental node failure to physical capture. Getting secure data in harsh environment from physical wireless sensors to an end-user is not a simple task due to these severe constraints.

III. WSN SECURITY GOALS

In this section, the main security goals for WSNs are summarized [4] [6] [9] [10] [11].

A. Data Confidentiality

It is the ability to hide message from a passive attacker and is the most important issue in network security. Sensor nodes may communicate highly sensitive data, such as key distribution, so it is extremely important to build a secure channel in a WSN. Moreover, sensor identities and public keys should also be encrypted to some extent to protect against traffic analysis attack.

B. Data Integrity and Authentication

Integrity refers to the ability to confirm the message has not been tampered or altered while it was on the network. An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. Indeed, data authentication allows a receiver to verify that the data really is sent by the claimed sender.

C. Data Availability

Availability is of importance for maintaining an operational network. It is the ability of a node to utilize the resources and the network is available for the message to move on.

D. Data Freshness

It ensures that data contents are recent and there no replay of any old content. This requirement is especially important when there are shared-key strategies employed in the design and need to be changed over time.

E. Self-Organization

WSN is typically an ad-hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the network management, so nodes must their selves adapt the topology and deployment strategy.

F. Time Synchronization

Many WSN applications demand some form of time synchronization for execution. A more collaborative sensor network may require group synchronization for tracking applications.

G. Secure Localization

Sensors may get displaced while deploying them or after a time interval or even after some critical displacement incident. The utility of a WSN will rely on its ability to accurately and automatically locate each sensor in the network.

IV. THREATS AND ATTACKS IN WSNS

An attacker in WSNs can be categorized as illustrate in Fig 1, based on the following characteristics: goals, performer, and layer wise.

A. Goal-Oriented Attacks

We distinguish passive and active attacks [10] [11] [12].

Passive Attacks

These attacks are mainly against data confidentiality. An attacker monitors unencrypted traffic and looks for sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring communications, decrypting weakly encrypted traffic, and capturing authentication information. Passive interception of network operations enables adversaries to see upcoming actions. Such attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attacks

In active attacks, the attacker is no longer passive but takes active measures to achieve control over the network. Some examples of active attacks are DoS, modification of data, black hole, replay, sinkhole, spoofing, flooding, jamming, overwhelm, wormhole, fabrication, Hello flood, node subversion, lack of cooperation, modification, node subversion, man-in-middle attack, selective forwarding and false node.

B. Performer-Oriented Attacks

Another category in attacks on WSNs can be either outside or inside attacks [13] [14] [15].

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Outside Attacks

Outside attacks may cause passive eavesdropping on data transmissions, as well as can extend to injecting bogus data into the network to consume network resources and raise Denial of Service attacks.

Inside Attacks

Inside attackers can damage the network stealthily since they can avoid our authentication and authorization because they are legitimate nodes of the native network and have access to the network information, and it is not easy to expect their attack patterns. Inside attackers can launch various types of attacks, such as modification, misrouting, eavesdropping or packet drop. This last attack is tricky to counter, because for a particular packet drop, we cannot distinguish whether it is dropped by an attacker or a result from collision or noise. This attack suppresses the important information reaching the base station which significantly degrades network performance, such as packet delivery rate due to their repeated packet drops. There are several types of packet drop attacks such as blackhole, grayhole and on-off attacks. This is a serious threat for many applications, such as military surveillance system that monitors the battlefield and other critical infrastructures.

C. Layer-Oriented Attacks

WSNs are organized in layered form. This layered architecture makes these networks vulnerable to various kinds of attacks.

Physical Layer Attacks

Physical attacks on WSNs range from node capturing to the jamming of the radio channel [16] [17] [18]. Physical attacks on WSNs availability are even more difficult to prevent than software attacks, because of the lack of physical control over the individual nodes. Jamming is one of the most important attacks at physical layer, aiming at interfering with normal operations. An attacker may continuously transmit radio signals on a wireless channel. An attacker can send high-energy signals in order to effectively block wireless medium and to prevent sensor nodes from communicating. This can lead to Denial-of-Service attacks at this layer.

Data Link Layer Attacks

The functionality of link layer protocols is to coordinate neighboring nodes to access shared wireless channels and to provide link abstraction to upper layers. Attackers can deliberately violate predefined protocol behaviors at link layer. For example, attackers may induce collisions by disrupting a packet, cause drain of sensor node energy by repeated retransmissions, or intercepting and examining messages in order to deduce information from patterns in communication. This can be performed even when the messages are encrypted and cannot be decrypted, or even cause unfairness by abusing a cooperative MAC layer priority scheme [15] [18] [19].

Network Layer Attacks

The network layer of WSNs is vulnerable to the different types of attacks, such as DoS attacks that are aimed at complete disruption of routing information, and therefore the whole operation of ad-hoc network. A sinkhole attack tries to lure almost all the traffic toward the compromised node, creating a metaphorical sinkhole with the adversary at the centre. Also if an attacker captures a single node, it is sufficient for him to get hold of the entire network. Malicious or attacking nodes can however refuse to route certain messages and drop them [13] [17] [21].

Spoofed, Altered, or Replayed Routing Information are the most direct attacks against a routing protocol in any network, are to target the routing information itself while it is being exchanged between nodes. An attacker may spoof, alter, or replay routing information in order to disrupt traffic in the network.

Transport Layer Attacks

An attacker may repeatedly make new connection request until the resources required by each connection are exhausted, or reach a maximum limit. It produces severe resource constraints for legitimate nodes [14] [21].

Application Layer Attacks

Different type of attacks can be carried out in this layer, such as overwhelm, repudiation, data corruption and malicious code. In overwhelm attack, an attacker might overwhelm network nodes, causing network to forward large volumes of traffic to a base station. This attack consumes network bandwidth and drains nodes energy [19] [22].

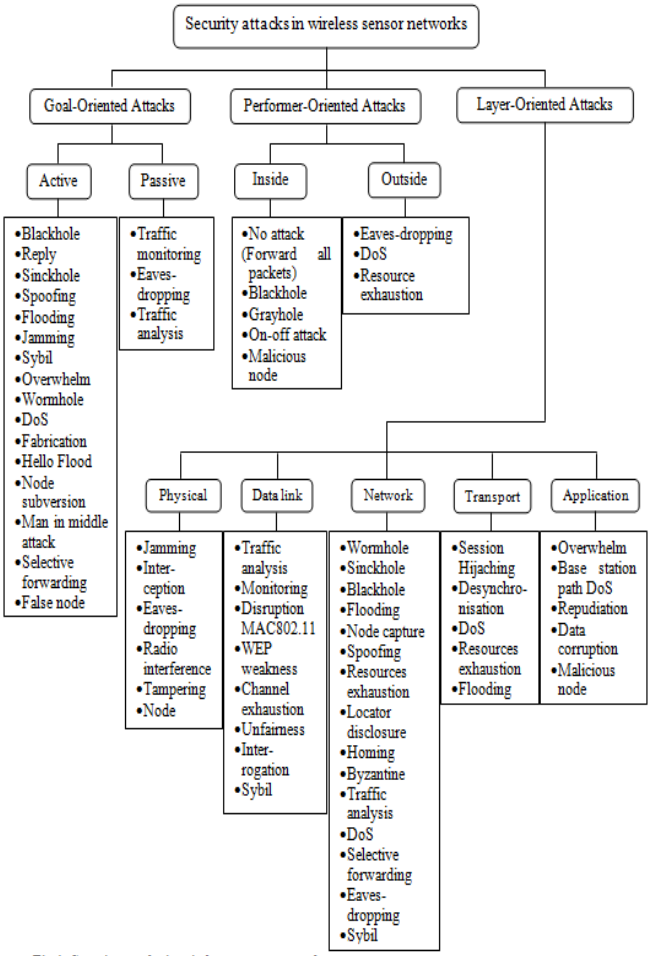

Fig.1. Security attacks in wireless sensor networks

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

V. BASIC SECURITY SCHEMES IN WSNS

To address the kernel security issues in WSNs, we talk about cryptography and its applicability. Basically, the major challenge for employing any efficient security scheme in WSNs is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensor nodes, as well as the limited communication capacity [12] [23]. For secure transmission of various types of information over sensor networks, several cryptographic techniques are used: symmetric key ciphers and asymmetric key ciphers. The security of asymmetric cryptography depends on the difficulty of a mathematical problem and the resulting algorithm consumes considerably more energy than symmetric key ciphers, which are constructed by iteratively applying simple cryptographic operations.

There is currently enormous research in the field of WSNs security. Many researchers have provided security solutions by using symmetric key cryptography. We give some of the commonly used to achieve security goals.

A. Symmetric Cryptography in WSNs

The idea of the symmetric cryptography is to load secret information in the sensor nodes before their deployment in the network. This secret information may be the secret key itself or auxiliary information that helps the sensor nodes to derive the real secret key. With this secret key, nodes can securely communicate [23]. The main disadvantage of this solution is that compromising one node (access to the pre-loaded key) might lead to compromise the entire network. To overcome this limitation, several researchers propose schemes that establish pairwise keys rather than a unique global key.

Perrig et al. propose SPINS, a key management protocol that relies on a trusted base station to distribute keys. SPINS contains two parts: SNEP (Secure Network Encryption Protocol) and μTESLA (micro time efficient streaming loss tolerant authentication). This protocol offers many security properties like semantic security, data authentication, replay protection, data freshness, and low communication overhead, and it is optimized for resource constrained and wireless communication [24]. SPINS which is a three-part approach providing for an authentication routing protocol as well as a three-part approach providing authenticated streaming broadcasts as well as two-party data authentication, data confidentiality, and freshness [25].

In [24] TinySec (Link Layer Security Architecture), TinySec provides authentication service and it is lightweight security package. It is included into the official TinyOS release. TinySec supports two special security options: authenticated encryption (TinySecAE) and authentication only (TinySecAuth).

In [26], the authors propose LEAP (Localized Encryption and Authentication Protocol); a key management protocol intended to support a several communication patterns. In this protocol, each node stores four types of keys: individual, pairwise, cluster, and group. An individual key is a key shared between a node and the base station.

A pairwise key is shared between a node and each of its neighbors. A cluster key is a key shared between a node and all neighboring nodes. A group key is a key common to the entire network. The individual key is preloaded. After deployment, neighboring nodes establish pairwise keys. They authenticate themselves using a pre-deployed key which is erased as soon as pairwise keys are established. To establish cluster keys and the group key, nodes use broadcasts and message relaying. The protocol uses μTesla [24] to authenticate broadcasts.

In [27], the authors propose BROSK (BROadcast Session Key negotiation protocol). With BROSK every node broadcasts a message containing its nonce. So, every two neighbouring nodes that hear each other can compute a common key which is a function of their two nonces. Neighbouring nodes authenticate themselves with a pre-deployed key which is supposed to be unreachable in the case the node is captured.

In [28], Blon describes an optimal class of symmetric key generation systems solution. In this solution, some of the possible link keys in a network of size N are represented as a $(\lambda+1) \times N$ key matrix. The scheme stores small amount of information in each sensor node, so that some pair of nodes can calculate corresponding field of the matrix, and uses it as the link key. This solution is λ-secure, meaning that keys are secure if no more than λ nodes are compromised. Another λ-secure solution is presented in [29] and called Polynomial-based key pre distribution scheme. This scheme distributes a polynomial share to each sensor. So, each sensor node stores a polynomial with (λ+1) coefficients and every pair of sensor nodes can establish a key using the property of symmetry of polynomials. The solution is λ-secure, meaning that coalition of less than λ+1 sensor nodes, knows nothing about pairwise keys of others.

Liu et al. propose in [30] LBKs (location-based keys) that relies on location information to achieve key management. The keys are established according to the geographical location of sensor nodes. However, knowing the geographical location of nodes is not guaranteed with random deployment.

Eschenauer and Gligor [31] propose a scheme based on a random key pre-distribution. In this scheme, each sensor randomly picks a set of keys and their identifiers from a key pool before deployment. Then, a shared-key discovery phase is launched where two neighbors exchange and compare list of identities of keys in their key chains. Basically, each sensor node broadcasts one message and receives one message from each node within its radio range where messages carry key ID lists. So, any pair of nodes has a certain probability to share at least one common key. The challenge of this scheme is to find a good trade-off between the size of the key pool and the number of keys stored by nodes to achieve the best probability. The main drawback of this approach is that if the number of compromised nodes increases, the fraction of affected links also increases.

In [32], the authors focus on developing cost-saving mechanisms while weakening the threat model. They propose Key Infection, a lightweight security protocol suitable for use in noncritical commodity sensor networks where an attacker can monitor only a fixed percentage of communication channels.

In general, existing symmetric cryptographic solutions for WSNs focus particularly on the efficiency of key

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

establishment after the deployment of the network. However, they do not deal with key refresh which makes key management dynamic and adds a further difficulty to the task of attackers. Furthermore, symmetric solutions do not scale well when the number of sensor nodes increases, and neglect the effect of captured node attacks. Using symmetric cryptographies in software implementation are challenging. Because they are not providing a perfect trade-off between resilience and performance, and hostile nature environments where sensor nodes are deployed makes it vulnerable to various attacks.

In the context of public-key cryptography, with thousands and millions of multiplications involved, it has become a major research branch to adapt and optimize advanced cryptosystems to small systems, such as sensor devices. Many works focused on the lightweight adaption of asymmetric cryptographic algorithms.

B. Asymmetric Cryptography in WSNs

Public-key cryptosystems are considered to be too heavy to use in WSNs. However, recent works show successful implementation examples of public-key cryptography in constrained sensors devices.

In [33], Gura et al. report that both RSA and elliptic curve cryptography are possible for small devices without hardware acceleration. With 8-bit CPUs, ECC shows a performance advantage over RSA. Another advantage is that ECC's 160-bit keys result in shorter messages during transmission compared to the 1024-bit RSA keys. In particular, Gura et al. demonstrate that ECC point multiplication on small devices is comparable in performance to RSA public-key operations and an order of magnitude faster than RSA private-key operations.

In [34], Watro et al. show that part of the RSA cryptosystem can be successfully applied to actual wireless sensors. The TinyPK system described by [34] is designed to allow authentication and key agreement between resource-constrained sensors. The protocol is used together with the existing symmetric encryption service for node networks, such as, TinySec. In particular, they implemented the RSA public operations on the sensors and the RSA private operations to an external party, such as a laptop.

In [35], Malan et al. demonstrate a working implementation of Diffie-Hellman based on the Elliptic Curve Discrete Logarithm Problem. In addition, they show that public keys can be generated within 34 seconds, and that shared secrets can be distributed among nodes in a sensor network within the same, using just over 1 kilobyte of SRAM and 34 kilobytes of ROM. So, public-key infrastructure is viable on the MICA2 for infrequent distribution of shared secrets.

Wang et al. in [36], proposes a public-key scheme for WSNs. They built an ECC-based access, which consists of pairwise key establishment, local access control, and remote access control. They have performed a comparison test by implementing both symmetric-key and public-key primitives on MICAz nodes and HP iPAQ. Their case study shows that the public-key scheme is more advantageous than symmetric key in terms of the memory usage, message complexity, and security resilience.

In [37], a very efficient ECC implementation called WM ECC, which is based on prime field operations, is reported. In [38], TinyPEDS is an approach for asynchronous WSNs, which allows confidential, memory-efficient, and distributed storage of sensed data on resource constrained devices. In [39] TinyPBC is presented. It is an efficient implementation of Pairing-based Cryptography (PBC) primitives for an 8-bit processor. TinyPBC takes less amount of time, only 5.45s to compute pairings on ATmega128L.

These solutions differ on the implementation algorithms, the optimizations performed, the functional completeness and platforms.

VI. Conclusion

The wireless sensor networks continue to grow and become widely used in many mission-critical applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, as well as unreliable communication and unattended operation, etc. There are many ways to provide security, and the main one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide appropriate security services in WSNs. Public-key cryptosystems are considered to be too heavy for resource-constrained sensor nodes. However, several studies have shown that it is feasible to apply public key cryptography to sensor networks by using the right selection of algorithms and associated parameters, optimization, and low power techniques. These cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches, and lead to more performance.

Both RSA and Diffie-Hellman based on the elliptic curve cryptography are possible for tiny sensor nodes, and the results show that it is possible to achieve good results with smaller keys. It reduces computation time and also the amount of data transmitted and stored. Asymmetric approaches with public key cryptosystems, specifically elliptic curve cryptography are promising approach for meeting security requirements in WSNs.

In this article, we aimed to provide a general overview of the major aspects of wireless sensor networks security: challenges, goals, and attacks; as well as some of commonly used defenses approaches.

References

[1] I.F.Akyildiz et al., "A Survey on Sensor Networks", IEEE Commun.Mag.,Vol. 40, No. 8, pp.102-114, Aug. 2002.
[2] E.Shi and A.Perrig, "Designing Secure Sensor Networks", Wireless Commun. Mag., Vol. 11, No. 6, pp.38-43, Dec 2004.
[3] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, pp. 30-33, Jun. 2004.
[4] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Sean Hong, "Security in Wireless Sensor Networks: Issues and Challenges", Proc. ICACT 2006, Volume 1, 20-22, pp. 1043-1048, Feb. 2006.
[5] HBE-Zigbex. Ubiquitous sensor network. Zigbex Manual [Online]. Available: http://www.hanback.co.kr
[6] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.
[7] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, 47(6):53–57, Jun. 2004.

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[8] Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo, “on the Security Issues in Wireless Body Area Networks”, International Journal of Digital Content Technology and its Applications Vol. 3, No. 3, Sep. 2009.
[9] Kalpana Sharma. M K Ghose, “Wireless Sensor Networks: An Overview on its Security Threats”, IJCA Special Issue on Mobile Ad-hoc Networks 2010.
[10] David Martins, and Herve Guyennet, “Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey”, 2010 IEEE.
[11] Anitha S.Sastry, Shazia Sulthana and Dr.S Vagdevi, “Security Threats in Wireless Sensor Networks in Each Layer”, International Journal of Advanced Networking and Applications, Vol. 04 Issue 04, pp. 1657-1661, 2013.
[12] Kaplantzis, S., “Security Models for Wireless Sensor Networks”, 2006, http://members.iinet.com.au/~souvla/transferfinal-rev.pdf
[13] Chris Karlof and David Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Ad Hoc Networks Journal, Vol.1, Issue 2-3, pp. 293-315, 2003.
[14] Yan Sun, Zhu Han, and K. J. Ray Liu, “Defense of Trust Management Vulnerabilities in Distributed Networks,” IEEE Communications Magazine, Vol 46, Issue 2, pp.112-119, 2008.
[15] Yanli Yu, Keqiu Li, Wanlei Zhou, and Ping Li, “Trust mechanisms in wireless sensor networks: attack analysis and countermeasures,” Journal of Network and Computer Applications, Elsevier, 2011.
[16] W. Xu et al., “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” MobiHoc ’05: Proc. 6th ACM Int. Symp. Mobile Ad Hoc Net. and Comp., pp. 46–57, 2005.
[17] W. Xu, W. Trappe, and Y. Zhang, “Channel Surfing: Defending Wireless Sensor Networks from Interference”, in Proc. Of Information Processing in Sensor Networks, 2007.
[18] Shih, E., Cho, S., Ickes, N., Min, R., Sinha, A., Wang, A. & Chandrakasan, A., “Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks”, Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, Rome, Italy, pp. 272-287.
[19] Woo, A. and Culler, D., “A Transmission Control Scheme for Media Access in Sensor Networks”, Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom, Rome, Italy, 2001.
[20] Sohrabi, K., Gao, J., Ailawadhi, V., and Pottie, G. J., “Protocols for Self-Organization of a Wireless Sensor Network”, IEEE Personal Communications, pp. 16-27, 2000.
[21] David R. Raymond and Scott F. Midkiff, “Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses”, IEEE Pervasive Computing, Vol. 7, No. 1, pp. 74-81, 2008.
[22] Parno, B., Perrig, A. and Gligor V., “Distributed Detection of Node Replication Attacks in Sensor Networks”, Proceedings of the IEEE Symposium on Security and Privacy (S&P’05), 2005.
[23] Y Xiao, VK Rayi, B Sun, X Du, F Hu, M Galloway, “A survey of key management schemes in wireless sensor networks”, Computer Communications 30(11-12), 2314–2341, 2007.
[24] Abhishek Jain, Kamal Kant and M. R. Tripathy ,“Security Solutions for Wireless Sensor Networks”, Second International Conference on Advanced Computing & Communication Technologies, 2012.
[25] Daniel E. Burgner , Luay A, “Wahsheh "Security of Wireless Sensor Networks”, Eighth International Conference on Information Technology: New Generations, 2011.
[26] S Zhu, S Setia, S Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks”, Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03), 62–72, Oct. 2003.
[27] B Lai, S Kim, I Verbauwhede, “Scalable session key construction protocol for wireless sensor networks”, Proceedings of the IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES '02), 2002.
[28] R Blom, “An optimal class of symmetric key generation systems”, Proceedings of the Eurocrypt 84 Workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques, (Springer), pp. 335–338, 1985.
[29] C Blundo, AD Santix, A Herzberg, S Kutten, U Vaccaro, M Yung, “Perfectly-secure key distribution for dynamic conferences”, Proceedings of the 12th Annual International Cryptology Conference on Advances in Crypto-logy, Berlin, Germany (Spring), pp. 471–486, 1992.
[30] D Liu, P Ning, “Location-based pairwise key establishments for static sensor networks”, Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (CCS '03), 72–82, Oct. 2003.
[31] L Eschenauer, VD Gligor, “A key-management scheme for distributed sensor networks”, Proceedings of the 9th ACM Conference on Computer and Communications Security, 41–47, Nov. 2002.
[32] R Anderson, H Chan, A Perrig, “Key infection: Smart trust for smart dust”, Proceedings of the 12thIEEE International IEEE International Conference on Network Protocols (ICNP '04), 206–215, October 2004.
[33] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz, “Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs”, Sun Microsystems Laboratories, http://www.research.sun.com/projects/crypto.
[34] Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn and Peter Kruus, “TinyPK: Securing Sensor Networks with Public Key Technology”, Proceedings of the 2nd ACM workshop on security of ad hoc and sensor networks SASN’04, pp. 59-64, Oct.2004
[35] David J. Malan, Matt Welsh, Michael D. Smith, “A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography”, Division of Engineering and Applied Sciences, Harvard University, Dec 2007.
[36] Haodong Wang, Bo Sheng, Chiu C. Tan, Qun Li, “Comparing Symmetric-key and Public-key based Security Schemes in Sensor Networks: A Case Study of User Access Control”, College of William and Mary Williamsburg, VA 23187-8795, USA.
[37] H. Wang and Q. Li, “Efficient implementation of public key cryptosystems on mote sensors”, in Proceedings of the International Conference on Information and Communication Security (ICICS ’06), pp. 519–528, December 2006.
[38] J. Girao, D. Westhoff, E. Mykletun, and T. Araki, “TinyPEDS: Tiny Persistent Encrypted Data Storage in Asynchronous Wireless Sensor Networks”. Elsevier Ad Hoc Journal, 5(7):1073–1089, September 2007.
[39] Leonardo B. Oliveira, Michael Scott, Julio Lopez, Ricardo Dahab, “TinyPBC: Pairings for Authenticated Identity Based Non-Interactive Key Distribution in Sensor Networks”, CAPES (BrazilianMinistry of Education) grant 4630/06-8 and FAPESP grant 2005/00557-9.

ISBN: 978-988-19253-4-3
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)