EAI Endorsed Transactions
on Energy Web and Information Technologies
Research Article EAI.EU

A Survey of Key Negotiation and Authentication Systems in WSNs

[1]Mohammad Tehseen, [1]Huma Javed, 1Ishtiaq Hussain Shah, [2]Sheeraz Ahmed

1Department of Computer Science, University of Peshawar, 2Department of Electrical Engineering
Gomal University, D. I. Khan to_tsn@yahoo.com, humajaved15@upesh.edu.pk, ishtiaquop@yahoo.com, sheerazahmed306@gmail.com

Abstract

Wireless Sensor Networks (WSNs) is a type of adhoc network that is use to sense some phenomena with the help of sensor nodes. The nodes have scarce resources like power, storage, processing power, sensing and communication. Now a day WSNs are helping as a main constituting component for variety of applications like intelligence gathering, battle field monitoring, pollution mapping, smart cities, smart homes and health care monitoring systems etc. To make such system a reality and work with reliability, data security needs a lot of attention to be handled properly. Due to scarce resources in WSNs, implementation of proper security technique is not quite simple rather it is a challenging task to accomplish. Huge number of security algorithms have been proposed for WSNs, but among them network wide master key based security systems are more appropriate due to less overhead in establishing a secure channel. In this survey different security solution such as LEAP, BROSK, Spins, C & R, Light Weight Authentication Systems and ECC are investigated to study the impact of physical attack on them.

Keywords: Wireless sensor networks, Elliptic Curve Cryptography, Symmetric and Asymmetric Cryptography,

Hashes. Received on 12 September 2017, accepted on 08 January 2018, published on 10 April 2018

doi: 10.4108/eai.10-4-2018.154445

1. Introduction

WSNs are adhoc networks, as like any other adhoc network, these networks lack administrative infrastructure [1]. Because of this special feature, these networks can easily be established and utilized in catastrophically destroyed areas or in the region, where there is no communication infrastructure was present or destroyed completely. Under normal circumstances these networks gather information with the help of sensing unit present at individual node and transfer this data to a sink node or base station where this information is utilized accordingly. For communicating the sensed data, nodes normally are equipped with RF based communication unit and have limited resources like processing power and storage capability [2]. During the communication of data, security becomes very crucial more specifically in the applications like battle field monitoring, enemy tracking and targeting etc. Due to the scarce resources at sensor nodes, it becomes even more challenging to develop and deploy proper security algorithms for data communication in WSNs. The rest of the paper is organized as, section 2 gives an over view of the security challenges related to WSNs. Section 3 provides an overview on security requirements and some constraints regarding sensor nodes. Section 4 contains survey of the security protocols and section 5 provides future directions and concludes the paper.

2. Security Challenges

This section provides an overview of the security challenges present in WSNs implementations pointed out in other literature.

2.1 Wireless Communication

Sensor nodes require wireless medium to communicate their data and normally contain RF unit [3], in wireless communication data is broad casted and thus it is more easily be picked by the eavesdropper present in the communication range. Therefore proper measures are required to protect the data before communication.

2.2 Limited resources

Sensor nodes have scarce resources like operating and processing power, therefore there is a need of light weight security mechanism having less computational cost and storage. Thus computationally intensive algorithms like asymmetric key based algorithm have become impractical to utilize [3] whereas symmetric key based algorithms is the only choice left for prolonging the life of wide range networks.

2.3 Physical Attacks

When WSN is deployed its sensor nodes operate unattended [3], therefore nodes can very easily be captured physically and all the data present in its memory can be retrieved which may contain the security keys and other security information.

2.4 Lack of Fixed Infrastructure

As WSNs lack fixed infra structure so there is a requirement for each and every node to make itself secure by employing security mechanisms from any type of external and internal intrusion and hence security requirements needs to be implemented on individual node basis [3]. Nowadays WSNs are employed as a monitoring and controlling system in variety of domains like Military or Border Surveillance Applications [2], Environmental Applications, Health Care Applications, Intelligent Agriculture, Structural Monitoring [4], Smart Cities, Smart Offices [4, 31], Intelligent Agriculture and Farming [5], Home Intelligence [6], Infant Monitoring Systems [7], Community Based ECG Monitoring System [8], Radio Active Rays Monitoring [9], etc. In all of the above mentioned applications implementation of data security is imminent to make these applications work reliably and successfully. Information should be made secure for communication at the level of individual nodes because nodes are easy targets for attacking. Thus in these type of applications data security should be handled in each and every aspect of development of WSNs [10].

3 Requirements and Constraints in WSNs

This section high lights the main requirements and constraints in security of WSNs.

3.1Security Requirements in WSNs

3.1.1 Data Confidentiality

Data belongs to one node should not be exposed to any other node of the same network and also to the nodes of other networks [2], only the intended node should be able to use the data. To fulfill this requirement proper encryption from the source node and decryption at destination node is required. Hence secure link needs to be established among all the nodes of the network.

3.1.2 Data Authentication

Every node on the network should be able to verify the authenticity of the received data; nodes requires some mechanism to conclude that the sender of the received data is an authentic node of a network; this is known as data authentication [2]. Data authentication is necessary because any eavesdropper can inject the fake messages because of the broadcasting nature of communication. To fulfill this requirement hashing or MAC algorithms can be utilized to avoid the asymmetric key based algorithms because of their high computational cost.

3.1.3 Data Integrity

During the transmission, data can be modified intentionally or unintentionally [2]. Nodes in the network should have some way to figure out any type of modifications in the message that occurs on the way from source to destination. To achieve integrity of data same hashing or MAC algorithms can be used that are devised for data authentication.

3.1.4 Data Freshness

Nodes in the network should be able to distinguish between the fresh chunk of data and old one in order to avoid the replay attacks. As sensors sense data and sends it after some fix interval of time so there should be some mechanism as a part of security system that verify whether the data received is a fresh copy of data or is the one that is already received. Data freshness can be achieved by utilizing the sequence of nonces with proper request response mechanism [2].

3.2 Security Constraints in WSNs

Apart from security requirements there are some constraints that needs to be consider and addressed properly to make a reliable security system for WSNs

3.2.1 Power Consumption Constraints

Limited power of the sensor nodes, both in terms of battery and processing, is one of the main constraint that cause hindrances in implementation of proper security systems in WSNs [3]. Due to these reason security systems needs to be light weight in terms of computational cost. As asymmetric key based algorithms are computationally expensive, the use of public key

based crypto systems was considered impractical in WSN security [11,12] but with the development in the technology nodes are now able to utilize public key based crypto systems as well [13,14]. However the symmetric key based crypto systems are still considered as a better choice due to involvement of less computational complexity especially in large scale WSNs.

3.2.2 Key Management Constraints

Establishing secure channels between the nodes (Key distribution) and management of these channels can become another problem due to limited storage space at the level of nodes. In large scale WSNs key predistribution schemes [15,16] are still considered as smart choice because no extra over head is involved for the exchange of keys. It also saves battery power of the nodes as 80 percent battery power is drained by the sending and receiving messages [16]. Such schemes requires installation of keys in pre deployment phase, two approached exists here, in first approach one master key Key-M is generated and installed in all the nodes at the time of manufacturing. In second approach pair wise keys for individual pair of nodes are generated and installed to be use in pair. Pair wise key approach needs total of (n-1) keys installed at every node for a network of N nodes, where as master key based approach requires single master key to be installed at every node. In terms of storage master key based approach is much better but in terms of security pair wise key approach is more reliable [12].

4 Master Key Based Algorithms

This section provides insight to the master key based and a public key based state of the art security solutions. Some notations are introduced which will be followed in the rest of the paper and will help in understanding the existing solutions.

4.1 Notations

Key-M : Network Wide Master Key.

$E(M)_K$: Encryption of Message 'M' using Key 'K'.

$H(M)_K$: Hash of Message 'M' Using Key 'K'.

$H(M)^i_K$: Message 'M' is Hashed 'i' Times Using Key 'K'.

4.2 Spins

Spins [2], this master key based algorithm works in two main parts SNEP (Secure Network Encryption Protocol) and µTESLA (Micro TESLA). SNEP deals with freshness, integrity, authentication and confidentiality of data while µTESLA (modified version of TESLA [17,18]) provides broadcasting services with authentication. Spins utilizes third party called Key Distribution Center (KDC) for establishing a secure channel between the nodes after authenticating them. In normal situation Base station serves as KDC between the two nodes but it is not necessary, nodes can also select KDC among the other nodes as well. This algorithm proceeds as, master keys (Key-M) are generated carefully for each node and stored in the memory of the individual node in pre deployment phase of a network, however all these keys are made shared with the KDC to authenticate the nodes in deployment and network establishment phase. Let's two nodes A and B wanted to establish a secure link through KDC, Key-MA is a master key of node A and Key-MB is a master key of node B, both the keys are shared with KDC to authenticate node A and B. Then algorithm proceeds as.

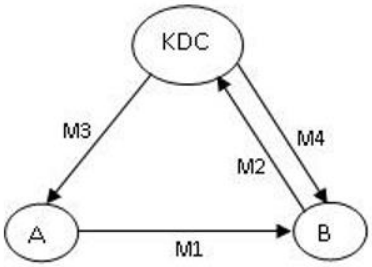

Fig. 1. Session Key Exchange Protocol (Spins[2])

Fig. 2. Challenge And Response Key Exchange [19]

Given below are the exchanged messages.

1. (A -> B) : $Non_A \mid Iden_A$
2. (B -> KDC) : $Non_A \mid Non_B \mid Iden_A \mid Iden_B \mid H(Non_A \mid Non_B \mid Iden_A \mid Iden_B)_{Key\text{-}MB}$
3. (KDC -> A) : $E(SK_{AB})_{Key\text{-}MA} \mid H(Non_A \mid Iden_B \mid E(SK_{AB})_{Key\text{-}MA})_{Key\text{-}MA}$
4. (KDC -> B) : $E(SK_{AB})_{Key\text{-}MB} \mid H(Non_B \mid Iden_A \mid E(SK_{AB})_{Key\text{-}MB})_{Key\text{-}MB}$

Where ("Non" is short form of Nonce and "iden" is short form of Identity) as depicted in figure 1, spins algorithm running at node A wanted to establish a session key SKAB with node B. Node A will send a message M1 to node B. In a response node B will send a message M2 to KDC. KDC then generate a session key SKAB and forwarded it to node A and B in messages M3 and M4 respectively. Now both the nodes have a session key send by the KDC, so a secure channel is established and can be utilize for future communications.

4.4 BROSK (BROadcast Session Key)

BROSK algorithm [20] is a master key (Key-M) based algorithm, to establish a secure channel among the nodes of a network. In this algorithm individual node generates a nonce and attaches its ID with it and broadcast it to all the neighboring nodes in a message M1 as shown in Fig 3.

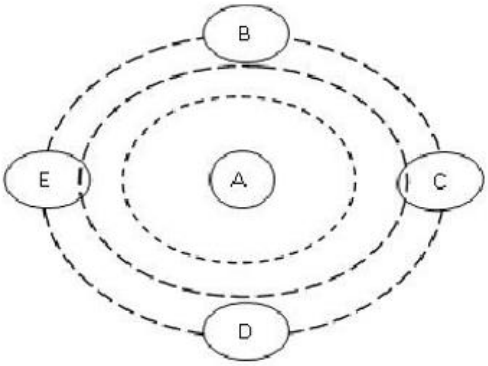

Fig. 3. BROSK [20]

$M1\ (A \rightarrow *) : Non_A \mid Iden_A \mid H(Iden_A \mid Non_A)_{Key\text{-}M}$
$M2\ (B \rightarrow *) : Non_B \mid Iden_B \mid H(Iden_B \mid Non_B)_{Key\text{-}M}$
$SK_{AB} : H(Non_A \mid Non_B)_{Key\text{-}M}$

In response every node will broadcast a message M2 containing its nonce and ID. As a result each node will have the nonces and IDs of all the nodes present on the network. After authentication each node can generate the pair wise session keys for every other node present on the network by utilizing the equation 1 given below. Consider node B has received the message M1 sent by node A. after receiving M1, B will send a message M2. As a result both A and B has received the nonces and IDs of one another and can generate the session key SKAB as shown in equation 1.

$SK_{AB} : H(Non_A \mid Non_B)_{Key\text{-}M}$

In this algorithm every node establishes a session key directly with every other node present on the network for secure communication.

4.5 LEAP (Localized Encryption and Authentication Protocol)

LEAP algorithm uses more than one key for uni-casting, multicasting and broadcasting securely [21]. It utilize pairwise key for unicasting and considers a cluster as multicast group and uses cluster key for multicasting purposes. Whereas whole network is considered as broad cast group and if there is any data that needs to be broadcasted then algorithm uses group key. Given below are the keys use to provide security.

(a) Individual Key All
the nodes on the network will have a unique key called individual key for authentication purpose only. Base station will also have the same keys to authenticate the nodes when they contact base station. Individual key in every node will be installed in the pre deployment phase.

(b) Pair Wise Key Two nodes that wanted to communicate with each other will have to exchange this key. Pair wise key is established when a network is deployed.
(c) Cluster Key
If a network will be divided in to the clusters so a key is established among the nodes of the clusters for secure communication within the cluster this key is called cluster key.
(d) Group Key The whole network is considered as a group so a different key is required to be established called group key and is used in a case where base station wanted to communicate a message with whole of the network.

4.5.1 Mechanisms for Exchanging Keys

This section gives overview for exchanging each type of key.

(a) Individual Node Keys
During pre deployment phase a single master key (Key-M) is generated and stored in every node along with the base station. When the network is deployed every node generates its individual key by using the equation 2. For instance node A will generate individual key KA as follows.

$$K_A = F(Iden_A)_{Key\text{-}M}$$

In the equation Key-M is the master key, IdenA is a unique number serve as identity of node A on a network and F is pseudorandom function [22].

(b) Sharing Pair Wise Key(b) Sharing Pair Wise Key
When the individual key is generated after that nodes will share pair wise key with neighbors. If any node wanted to communicate with multiple hops away node, then scheme called a probabilistic key sharing [23,24,25,26] can be employed. Let's node A needs to communicate using a pair wise key with a node B, then given below steps will be followed.
1/ Node A should have generated its individual key K_A and node B has its individual key K_B.
2. (B -> A): $Iden_B \mid H(Iden_A \mid Iden_B)_{KB}$

Node A after receiving this message can authenticate B by computing KB. KB = F (IdenB) Key-M
3. When authentication is done pair wise key can be generated using the equation given below

SKAB = F (IdenA) KB Node A will utilize the same procedure with all neighboring nodes, in order to establish a secure channel for communication.

(c) Sharing Cluster Key

After pair wise key is established and there is a requirement to make a cluster, then a cluster key has to be establishing among the cluster members for broad casting a message with in the cluster. Node A, B, C, D and E wanted to make cluster, they needs a cluster key to communicate securely as shown in figure 4.

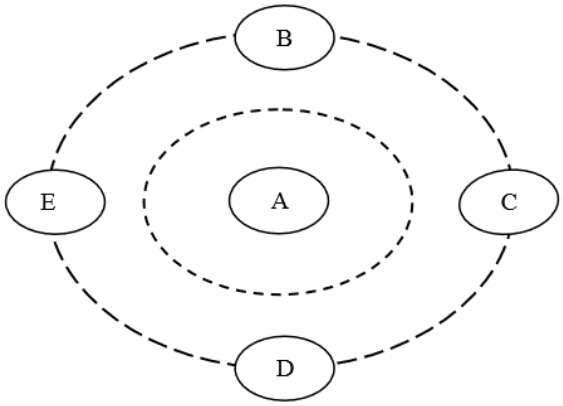

Fig. 4. Five Nodes Cluster [21]

Node A will communicate a cluster key CKA after generating it with all the nodes wanted to be a part of clusters after encrypting it with their respective pair wise keys. Each node then decrypts the key and stores it as cluster key of node A.

(iv) Sharing Group Key This key will be used to authenticate the broad casted messages from the base station, authentication is required to avoid any other node impersonating as base stations. Easiest way to establish group key is to store this key in the memory of every node in pre deployment phase. Any new node can enter the group after authentication from the base station and then base station will generate a new group key to be shared with all the nodes using a µTESLA [2] protocol.

4.6 A Light Weight Authentication Scheme (Delgado-Mohatar)

This algorithm works in three main phases [3].

4.6.1 Pre-Distribution Phase

In this phase a master key Key-M is selected very carefully according to the NIST [29] recommendation and stored in all the nodes, along with the initial authenticator (µi) known as ith cycle authenticator. Purpose of authenticator is to authenticate the nodes, where i denote the current cycle of authenticator. Rows of random numbers ri and their computed hashes from current authentication key are actually stored in the authenticator.

For the first cycle of authentication master key Key-M is used as AK0. The rows present in the authenticator are given in the form of equation 3.

$$\mu^0 = \{(Ran_i, [Ran_i]Key\text{-}M)\} \quad i = 0,.....,n\text{-}1 \qquad (3)$$

Ran_i is random number for ith round. Authentication key for the nth round can be derived as $AK_N = [Key\text{-}M]^N$ and the set of random values will be.

$$\mu^N = \{(Ran_i, [Ran_i]AK_N)\} \quad i = 0,.....,n\text{-}1 \qquad (4)$$

Authenticator changes states from one to another. Each node after deployment will contain Key-M, initial authenticator μ^0 and AK_0 for initial stage $AK_0 = Key\text{-}M$.

4.6.2 Network Initialization Phase

When the nodes are deployed, this phase actually starts and works as follow:

1. Individual node will generate a unique symmetric key EKi for encryption. For key generation random number Rani will be used as depicted in given equation $EK_i = H (r_i)_{Key\text{-}M}$.
2. Nodes will send their Rani for very small period usually in seconds [30]. Every other node after receiving the neighbors Rani will generate the encryption keys for neighboring nodes.
3. Every node will now produce the authentication key regarding forthcoming stage as. $AK_1 = H (Key\text{-}M)^1$ Up to the end of this step, nodes will have encryption key, neighboring nodes encryption keys, authentication key AK1 for the next cycle and authenticator for the current cycle.

4.6.3 Authentication Protocol

This phase will be activated every time when new node needs authentication to enter into the network. Let's a fresh node A wanted to join the network. A's authenticator operator will be in a initial cycle µ0. Node B will serve as an authenticator node and its authenticator will be in arbitrary jth cycle µj, rest of the protocol is shown in figure 5

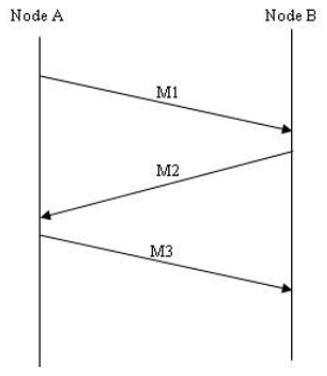

Fig. 5. Authentication Protocol [3]

Following is the sequence of messages that will exchange during this phase.

1. (A -> B): Ran_A
2. (B -> A): Ran_B | H (Ran_A)AK_{j-1} | E (EK_B)AK_j | J
3. (A -> B): H (Ran_B)AK_{j-1} | E (EK_A)AK_j

In the start A sends a message M1 to B containing the random number RanA. In a response node B will send a message M2 and after exchanging the message M3, both the nodes A and B will have the encryption keys for secure communication with each other.

4.7 Short Elliptic Curve Cryptography Scheme

In this scheme asymmetric algorithm is proposed that is based on a Elliptic Curve Cryptography (ECC), main motivation was that the level of security provided by the ECC based systems is same as provided by the public key algorithms based on modular arithmetic with much smaller size of keys [32]. In order to make ECC light weight reduction in the size of key is proposed. In standard ECC according to NIST recommendation 224 bit key lengths provides the same security level as provided by the RSA with 2048 bit key sizes [32]. In short ECC to make it more light weight the reduction in the key size up to 32 to 64 bit is recommended but within a constraint environment [32], that is after dividing the WSN into small closed groups. This scheme reduces the computational load by reducing the size of key with same level of security as provided by the standard ECC. Short ECC algorithm is the same for key generation scheme just reduces the size to make it more usable on WSNs because of scarce resources. Scheme recommended El-Gamal standard for confidentiality requirements and ECDSA for authentication and data integrity purposes [32]. ECC works as follow, let's node A amd B needs to share a session key, A selects Eq (a, b) and G (where Eq (a, b) is an elliptic curve with parameters a,b and prime number q. G is a point on Eq (a, b)). After that node A will select a private key PRA where PRA < N, after selecting PRA node A will select a public key PUA as follow.

PUA = PRA x G
PUB = PRB x G
At node A: SKAB = PRA x PUB
At node B: SKAB = PRB x PUA

After following the same procedure node B will also generate the public and private key pair let's denoted by PUB and PRB. Both the nodes now will share their public keys with one another. When the public keys are shared session key SKAB will be generated at both the ends.

5 Conclusions

This paper discussed different key negotiation schemes that can be used for establishing a secure link among the nodes of WSNs, whether it is a network wide master key based schemes among the symmetric systems or asymmetric public key based scheme. Master key based schemes as compared to asymmetric key schemes are much better in terms of low overhead needed to establish a secure channel whether it is in terms of computational cost or communication. All the schemes discussed, provide adequate level of security but there exist a main drawback and that is these schemes lack temper resistance capability. In simple words, if any of the node is captured physically and its keys are extracted from its storage area that can make the whole network compromised. These schemes needs some further improvements in the form of temper resistance and detection capabilities.

References

[1] Stajano, F.: Security for Ubiquitous Computing. John Wiley and Sons (2002)

[2] Perrig, A., Szewczyk, R., Tygar, J, D., Wen, V., Culler, D, E.: Spins: security protocols for sensor networks. Wireless Networks 8 (5) 521–534. (2002)

[3] Delgado-Mohatar, O., Fúster-Sabater, A., Sierra, J, M.: A light-weight authentication scheme for wireless sensor networks. Ad Hoc Networks 9. 727–735. (2011)

[4] Prasanna, S., Rao, S. An overview of wireless sensor networks applications and security. *International Journal of Soft Computing and Engineering (IJSCE)* (2012)

[5] Ojha, T., Misra, S., Raghuwanshi, N. S.: Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. *Computers and Electronics in Agriculture.* Vol. *118.* pp. 66-84 (2015)

[6] Batista, N. C., Melício, R., Matias, J. C. O., Catalão, J. P. S.: Photovoltaic and wind energy systems monitoring and building/home energy management using ZigBee devices within a smart grid. *Energy*, Vol. *49*, pp. 306-315 (2013)

[7] Zhou, H., Goold, B.: A domestic Adaptable Infant Monitoring System using wireless sensor networks. *IEEE 34th International Performance Computing and Communications Conference (IPCCC).* pp. 1-2 (2015)

[8] Lin, B. S., Wong, A. M., Tseng, K. C.: Community-Based ECG Monitoring System for Patients with Cardiovascular Diseases. *Journal of Medical Systems.* Vol. *40*(4). pp. 1-12 (2016)

[9] Gome, A., Magno, M., Lagadec M,F., Benini, L.: Precise, Energy-Efficient Data Acquisition Architecture for Monitoring Radioactivity using Self-Sustainable Wireless Sensor Nodes. IEEE Sensors Journal. (June, 2017)

[10] Perrig, A., Stankovic, J., Wagner, D.: Security in Wireless Sensor Networks. *Communications of the ACM.* 47(6). 53-57. (2004)

[11] Hwang, D, D., Lai, B, C, C., Verbauwhede, I.: Energy-memory-security tradeoffs in distributed sensor networks. ADHOC-NOW. LNCS, vol. 3158. (2004)

[12] Potlapally, N, R., Ravi, S., Raghunathan, A., Jha, N, K.: Analyzing the energy consumption of security protocols, in: ISLPED '03. Proceedings of the 2003 international Symposium on Low Power Electronics and Design. ACM. Korea, pp. 30–35. (2003)

[13] Lopez, J.: Unleashing public-key cryptography in wireless sensor networks. Journal of Computer Security 14 (5) 469–482. (2006)

[14] Wander, A, S., Gura, N., Eberle, H., Gupta, V., Shantz, S, C.: Energy analysis of public-key cryptography for wireless sensor networks. in: PERCOM '05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications. IEEE Computer Society. Washington, DC, USA, pp. 324–328. (2005)

[15] Chan, H., Perrig, A., Song, D.: Random key pre distribution schemes for sensor networks. in: Proceedings of Symposium on Security and Privacy 2003. pp. 197–213. (2003)
[16] Du, W., Deng, J., Han, Y, S., Varshney, P, K.: A pair wise key pre distribution scheme for wireless sensor networks. in: CCS '03: Proceedings of the 10th ACM Conference on Computer and Communications Security. ACM. New York, NY, USA, pp. 42–51. (2003)
[17] Perrig, A., Canetti, R., Song, D., Tygar, J, D.: Ef_cient and secure source authentication for multicast. in: Network and Distributed System Security Symposium. NDSSÕ01. (2001).
[18] Perrig, A., Canetti, R., Tygar, J., Song, D.: Ef_cient authentication and signing of multicast streams over lossy channels. in: IEEE Symposium on Security and Privacy. (2000)
[19] Menezes, A, Z., van Oorschot, P, C., Varstone,S,A.: *Handbook of Applied Cryptography*. CRC Press. (1997)
[20] Lai, B,C., Hwang, D,D., Kim,S,P., Verbauwhede, I.: Reducing radio energy consumption of key management protocols for wireless sensor networks. in: ISLPED '04: Proceedings of the 2004 International Symposium on Low Power Electronics and Design. ACM. California, USA, pp. 351–356.(2004)
[21] Zhu, S., Setia, S., Jajodia, S.: LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks. *CCS '03*. Washington D.C., USA, New York, USA. ACM Press. 62-72. (2003)
[22] Goldreich, O., Goldwasser, S., Micali, S.: How to Construct Random Functions. Journal of the ACM. Vol. 33. No. 4. pp 210-217. (1986)
[23] Zhu, S., Setia, S., Jajodia. S.: Leap: Efficient security mechanisms for large-scale distributed sensor networks. In Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03). 62–72. (2003)
[24] Du, W., Deng, J., Han, Y., Varshney, P.: A pairwise key pre-distribution scheme for wireless sensor networks. In Proc. of the 10th ACM Conference on Computer and Communications Security (CCS'03). 42–51. (2003)
[25] Liu,D., Ning, P.: Establishing pair wise keys in distributed sensor networks. In Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03). 52-61. (2003)
[26] Zhu, S., Xu, S., Setia, S., Jajodia. S.: Establishing Pair-wise Keys For Secure Communication in Ad Hoc Networks: A Probabilistic Approach. In Proc. of the 11th IEEE International Conference on Network Protocols (ICNP'03). (2003)
[27] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., Pister, K.: System architecture directions for networked sensors. In Proc. of ASPLOS IX. (2000)
[28] Karlof, C., Wagner, D.: Secure Routing in Sensor Networks: Attacks and Countermeasures. To appear in Proc. of First IEEE Workshop on Sensor Network Protocols and Applications. (2003)
[29] NIST. Recommendation for Key Management. Part 1: General Guideline. Special Publication 800-57, p. 63. (2007)
[30] Anderson, A., Chan, H., Perrig, A.: Key infection: smart trust for smart dust. in: Proceedings of ICNP'04. (2004)
[31] Kabalci, Y.: Communication Methods for Smart Buildings and Nearly Zero-Energy Buildings. InEnergy Harvesting and Energy Efficiency. Springer International Publishing. pp. 459-489. (2017)
[32] Sojka-Piotrowska, A. Langendoerfer, P.: Shortening the security parameters in lightweight WSN applications for IoT-lessons learned. InPervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference. 13 pp. 636-641. (2017)