A SURVEY ON WIRELESS SENSOR NETWORKS SECURITY WITH THE INTEGRATION OF CLUSTERING AND KEYING TECHNIQUES

V K Singh[1] and Kalpana Sharma[2]

[1]Department of Computer Science & Engineering, Sikkim Manipal Institute of Technology, East Sikkim, India
vikashsmit2009@gmail.com
[2]Department of Computer Science & Engineering, Sikkim Manipal Institute of Technology, East Sikkim, India
kalpanaiitkgp@yahoo.com

ABSTRACT

Keying technique in Wireless Sensor Networks(WSNs) is one of the most emerging fields of WSN security. In order to provide security on WSN, the role of Key distribution technique is considered to be very significant and thus the key management plays a crucial and fundamental roles in the security service of WSNs. This paper reviews pairwise key establishment technique along with the architecture and the environment of WSN. The cluster based group key agreement protocols for infrastructure base WSN are discussed in this paper. This paper also reviews how the security can be provided to WSNs with the integration of clustering and keying techniques. The survey also provides a more detailed discussion on the comparison between different cluster based group key agreement protocols.

KEYWORDS

Sensor network, security, key establishment, clustering , authentication

1. INTRODUCTION

Wireless Sensor Networks (WSN) consist of hundreds and thousands of tiny nodes having sensing and communication capabilities. In order to accomplish a particular task these sensor nodes are deployed in an area of interest. The most common form of WSN topology consists of the a collection of a large number of sensor nodes and a Base Station (BS). Each sensor nodes are constrained by limited battery power, small memory, low computational ability and limited transmission range [13]. On the other hand the BS has larger memory and processing power. One of the solutions of the re-source constraint nature of WSN is to emphasize on factors like scalability and efficient resource management.

Use of clustering technique, is one of the answers for efficient resource management [16]. In case of a large-scale environment and time critical applications, clustering technique is more suitable [16], [17]. This technique can also be used in one-to-many, many-to-one and even one-to-all communications. The network bandwidth and service discovery can be optimized very easily by

Jan Zizka (Eds) : CCSIT, SIPP, AISC, PDCTA - 2013
pp. 183–191, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3620

using the clustered approach. Details pertaining to the clustering techniques are out of the scope of this paper.

Security is another important issue of WSNs [13]. Since the sensor networks are usually deployed in uncontrollable environments that are not trustworthy, thus WSN is exposed to the common security threats like information disclosure, message injection, and replay attacks etc. [15]. An attacker may capture and compromise a node and thus be able to control some part or even the whole network[18]. One of the security solutions of WSN is to employ and manage the cryptographic keys. This implies that effective key management mechanisms must be employed. There should be a proper mechanism for distribution and management of these keys. This is where 'Key Management Scheme of WSN' comes into play and the significance of Key distribution is felt. Keying technique in WSN is one of the most emerging fields. Various WSN key distribution phases are stated below[17]:

- Deployment phase: Sensor nodes can be deployed into the environment.
- Post-deployment phase: Topology can change after deployment because of irregularities in the environment like obstacles or due to jamming, noise, available energy of the nodes, malfunctioning, etc. [17].
- Redeployment of additional nodes phase: Additional sensor nodes can be redeployed at any time to replace the faulty or compromised sensor nodes.

The process through which cryptographically secure communication links can be established between the sensor nodes is called the bootstrapping process [17]. There are different methods by which the bootstrapping problems can be solved. One of these methods uses the random deployment model which does not use the pre deployment phase to deploy the sensor nodes[16]. On the other hand some keying technique uses all the above three phases to establish a secure communication channel[16],[17]. The selection of the keying technique depends on the application of the sensor networks. The new research direction of WSN stresses on the integration of the clustering schemes and the key management schemes in order to obtain different security schemes for a wide range of applications. J.C. Lee et al. [18], state the use of a group key is necessary for multicast communication, cluster-based group keying schemes are more robust than network-wide keys because the compromise of a node, will lead to the compromise of the cluster, but not the entire group.

The rest of the paper has been organized as follows: section 2 deals with architecture and environment of WSN, section 3 describes the security architecture comprising different interacting phases followed by section 4 which deals with the description of some of the existing cluster based key agreement protocols. Section 5 states the summary of all protocols and Section 6 deals with the conclusion.

2. WIRELESS SENSOR NETWORK ARCHITECTURE AND ENVIRONMENT

The security of the WSN is based on the architecture of its network. To design the security architecture, the basic need is to analyze the characteristics of sensor nodes, the network and the environment which are discussed in subsequent sections.

2.1. Sensor Nodes

Sensor nodes are the resource constraint devices that are small in size and communicate in short distances. These tiny sensor nodes, which consist of sensing, data pro-cessing, and

communicating components, from the sensor networks based on the collaborative effort of a large number of nodes [17]. Details on sensor nodes are found in [15],[17].

2.2. Sensor Network and Environment

A sensor network is composed of a large number of sensor nodes. The position of sensor nodes need not be engineered or pre-determined[15]. The sensor network protocols and algorithms must possess self-organizing capabilities [13]. Instead of send-ing the raw data to the nodes responsible for the fusion, sensor nodes use their pro-cessing abilities to locally carry out simple computations and transmit only the required and partially processed data [17] and this technique is known as 'data aggregation'. The environment of these sensor networks depends on the application of WSN and in most cases it is uncontrollable and not trustworthy. Thus, the need of a security architecture which must be fault tolerant is felt to ensure a certain level of security.

3. SECURITY ARCHITECTURE

Every node of the system is integrated with every other node of the system so that a secure WSN network can be established. The attack may be possible if all components of a network are not implemented with a proper security [14]. Cryptography is one of the methods of defense against such attacks [15]. Varying levels of crypto-graphic protection implies a varying level of overhead in the form of increased packet size, code size, processor usage etc.[8]. Generally, asymmetric as well as symmetric cryptography could be employed to achieve security[18]. The most robust form of WSN security architecture is based on three different interacting phases [13]: a pair-wise key establishment to provide authentication and the initial key exchange, the establishment of sending clusters to extend pairwise communication to broadcast inside the communication range, and encrypted and authenticated communication of sensor data.

3.1. Pairwise Key Establishment

The pairwise secret key which is shared by two or more number of nodes, can be determined by using scheme proposed by Blundo-et-al. [19]. This scheme is totally based on Blom [20] and is secure and resistant against collusion of a maximum number of users. The scheme basically uses Polynomial-key pre-distribution technique having low communication overhead, but their computational overhead is relatively higher and can not provide sufficient security to against node capture attack[17]. Therefore polynomial-keying technique works well when the number of compromised nodes is less than a specific value and once this value is exceeded, the entire network could be crashed by the adversary[15]. To overcome these limitations of existing schemes, the use distributed pairwise key establishment scheme (DPKE)[19] for large-scale WSNs sounds better. DPKE can provide the complete connectivity of a network without the prior information of sensor's location and good network resilience also can be achieved. This scheme has lower communication overheads in comparison with the previous scheme. It can support a larger network size.

3.2. Establishment of Sending Clusters

Every node establishes a randomly generated key within its neighborhood so that the secure communication can be established [13]. This key is used by the node to encrypt and authenticate its messages. If a node receives a message of which the content cannot be decrypted and authenticated, it calculates the pairwise secret for the sender and itself[15],[17]. The protocol enables a node to establish its key in a new environment as well as the other nodes' keys are known with request and reply messages. The process of encryption, decryption or establishment

of randomly generated key can be used at any time and with any other legitimate node of the network[15]. Thus it solves the mobility of the sensor nodes as well as the deployment of new nodes at a later point of time.

3.3. Secure Communication of Sensor Data

As per Dworkin M[10] whenever the sender node wants to transmit the data to the receiver node, the node broadcasts messages to their neighbourhood. The message is encrypted in such a way that its length should not be changed [10]. The counter sj is also added to the message which results in ordered and unique messages but this is an extra overhead[13]. A message loss by any of the neighbors would require two additional messages (request of counter value and reply). RC5 algorithm [11] can also be used but this leads to bad runtime behaviour. AES algorithm[21] which gives best performance can also be used , but requires large lookup-tables. In addition to this AES algorithm is not constructed for a key length shorter than 128 bits, which are often used in sensor networks. Serpent [12] algorithm can be used which has good runtime behaviour because it can be implemented using logical operations only. It re-quires only 16 rounds but it does not allow any published attacks to be successful [13]. The encryption algorithm can be reused for the well-know CBC-MAC[13] to ensure the integrity and the authentication of sensor data. Once again, there is no need to add the complete output of the MAC-function as a checksum to the message, because 16 bytes of overhead per message seems to be inappropriate for sensor networks.

4. CLUSTER BASED KEY AGREEMENT PROTOCOLS (CBKAP)

There are different applications where several intermediate nodes participate in the network for secure routing and packet forwarding[17]. Therefore there should be a group key management scheme to provide these functionalities [16]. CBKAP proto-cols are more efficient than pairwise key establishment schemes for WSNs because devices do not waste energy every time they wish to communicate with another de-vice by establishing a new shared secret key. The majority of cluster-based key agreement schemes [1], [2], [3], assume a specific hierarchical structure of the clusters or some tree-structure and then apply a general key agreement protocol. The CBKAP protocol is first applied locally in every cluster and then, the clusters' keys are used from the same or another key agreement mechanism to form the final group key[16]. For the inter-cluster communication between two nodes, the corresponding Cluster Heads(CHs) which share common keys with other CHs must decrypt and re-encrypt the messages they relay using the corresponding cluster-keys. For each CBKAP protocol elliptic curve analog can be used. The communication cost can be calculated based on the number of rounds required by the protocol. Finally, every protocol includes the key establishment phase, usually referred as Initial Key Agreement phase and the key maintenance phase usually referred as Group Key Maintenance phase, for the management of group membership changes. Key establishment phase follows the cluster-setup phase, where the creation of clusters takes place. All cluster-based CBKAP protocols assume a specific cluster structure and well known clustering algorithms. It can also be assumed that the cluster structure has already been formed like number of layers, grouping into clusters, election of CHs etc. and thus there is no need to calculate the overhead introduced by the cluster-setup phase.

4.1. Hierarchical Key Agreement Protocol (HKAP) Protocol

Yao et al. in 2003 [4] proposed the Hierarchical Key Agreement Protocol (HKAP) which uses a cluster-based hierarchical structure of mobile nodes and then applies some well known CBKAP protocols in every cluster. The protocol forms a cluster using a number of nodes and applies an existing CBKAP protocol to the members of each cluster in order to generate a cluster key. Then, a CBKAP protocol is applied to all CHs to generate the group key. Finally, the group key is

distributed to all the group members with the use of a key distribution protocol. The protocol comprises of three main phases.

Phase 1: The nodes are organized in a hierarchical cluster based and clustering is based on the geographical relationship between the mobile nodes.

Phase 2: Each member chooses a secret key. Then, cluster key is established after ex-ecution of CBKAP protocol by all agreed members of the network.

Phase 3: Each CH broadcasts the computed upper keys to all the members of its clusters.

4.2. GKA-CH Protocol

Teo and Tan[7] proposed the Group Key Agreement (GKA) protocol for Circular Hierarchical(CH) group model (GKA-CH) [5]. and the Burmester-Desmedt [6] GKA protocol is applied in every layer of a circular-hierarchical group structure. More specifically, the whole group is arranged in h hierarchical layers with each layer having one or more subgroups. Every subgroup is organized in a circle, containing an equal number of members and is managed by a subgroup controller. The GKA-CH protocol comprises of four phases.

Phase 1: The subgroup key of every subgroup is calculated using the Burmester-Desmedt (BD) GKA protocol in the lowest level, Lh−1, [10].

Phase 2: The subgroup key produced in phase 1 is used as the random number for the execution of the BDGKA protocol for the upper layers.

Phase 3: The final subgroup key K is calculated by all the subgroup members of the highest layer L0, by using the subgroup keys produced in phase 2. Now the group key K is encrypted with its subgroup key and is broadcasted by the member of the subgroup.

Phase 4: In the last phase of the protocol, every subgroup member decrypts the message from phase 3 to finally get the group key K. The subgroup controllers will have to first decrypt the message and then re-encrypt it using its subgroup key and finally broadcast the key to its subgroup members.

4.3. PB-GKA-HGM Protocol

[

The password-based GKA protocol for hierarchical group models (PB-GKA-HGM) is proposed by Teo and Tan [7]. This protocol creates a hierarchical structure based on three main entities: the main controller C in highest layer, various subgroup controllers (Si) and several members (M) in every subgroup. The protocol is password based.

The establishment of the common group key is then performed in three phases.

Phase 1: Each Si computes the subgroup key Ki after the completion of the instructions with the subgroup members.
Phase 2: Si interacts with the controller C to obtain the final group key K.

Phase 3: The group key K is sent downward securely by the controller to the sub-group controllers which in turn are responsible to securely forward the K to their members. Key confirmation messages are also sent along to verify and confirm the subgroup key Ki and final group key K.

4.4. AP-1 and AP-2 Protocols

The cluster-based GKA protocols, AP-1 and AP-2 were proposed by Dutta and Dowling [6]. AP-1 is based on the constant round multi-party dynamic key agreement protocol DB [8] whereas AP-2 uses the pairing-based group key agreement protocol DBS [9] and assumes that the CHs are arranged in a tree-structure. Both protocols assume that a group of nodes is organized in a number of clusters according to their relative proximity to one another and perform a GKA protocol to generate a cluster key. The protocols are comprised of two main phases:

Phase 1: This phase is named as Initialization Key Agreement phase (IKA) which specifies the procedures for the establishment of the common group key.

Phase 2: This phase is named as Group Key Maintenance Phase (GKM) which specifies the procedures for membership changes.

5. COMPARISON BETWEEN DIFFERENT PROTOCOLS

Table 1. Comparison between different Cluster Based Key Agreement Protocols.

Protocols / **Comparison Parameters**	**HKAP**	**GKA-CH**	**PB-GKA-HGM**	**AP-1 & AP-2**
Topology	Cluster-based hierarchical structure of mobile nodes	Circular hierarchical group structure of nodes.	Hierarchical structure based on main controller, subgroup controller and members entities.	Cluster based GKA protocols.
Protocol Used	Use simple existing GKA protocols	Burmester-Desmedt protocol is used in each layer.	Hierarchical group models GKA protocol is used.	Based on constant round multiparity dynamic GKA and pairing based protocol.
Key Type	Group key is generated by applying GKA protocol to all CHs	Each group is arranged in hierarchical layers having one or more subgroups.	Password based protocol. Subgroup member and controller uses the password and a pairwise secret keys	The secret group key is generated by using the CH.
Structure	All nodes are grouped in one hop cluster.	Each cluster is organized in a circuit having equal number of members.	Each cluster is organized in a hierarchical fashion.	CHs are arranged in tree-structure
Media of Transmission	Uses a powerful radio	Uses a powerful radio	Uses a powerful radio	Uses a powerful radio transmission

	transmission for communication	transmission for communication	transmission for communication	for communication
Number of Phases	Comprises three phases: Phase1: Hierarchical organization of nodes. Phase2: Establish cluster key Phase3: Broadcast the upper keys	Comprises Four phases: Phases 1-to-3: subgroup key is calculated for every subgroup, starting from the lowest layer to the highest layer. Phase4: Group key K is encrypted and broadcasted using symmetric key cryptography.	Comprises three phases: Phase1: computes the subgroup key Phase 2: Obtain final group key by the controller. Phase3: Forward the group key to the members of the cluster.	Comprises two phases: Phase1: Initialization Key Agreement phase. Phase 2: Group Key Maintenance Phase.
Assumptions	Nodes Mobility affects only group key	Authentication can be done by using the different signature scheme.	Both pairwise keys and password are securely pre-loaded into the environment.	Efficient in handling dynamic membership changes by the members.
Application Criteria	Well suited for infrastructure based WSNs.	Only suited for infrastructure based WSNs.	Suited for infrastructure based WSNs where CH and BS are acting as subgroup and main controller respectively.	Well suited for infrastructure based WSNs.

6. CONCLUSIONS

The main aim of this paper is to focus on security architecture that provides security for a WSN. Key management techniques that have been proposed for WSN have been discussed. One of the main key establishment approaches used in WSN is setting up pairwise secret keys between the mobile sensor nodes to establish a sending cluster per node in which it can communicate its messages securely. This paper have also fo-cused on how the integration of clustering technique and key management scheme works efficiently to provide security in the different applications of WSN. Compari-son of different CBKAP protocols clearly brings out the how these protocols are dif-ferent from each other and in which situation these protocols are applicable in various WSN application domain.

ACKNOWLEDGEMENTS

This work was supported by AICTE under the reference no: 8023/RID/RPS-28/(NER)/2011-12 as part of "Design of An Integrated Security Scheme for Wireless Sensor Network" project.

REFERENCES

[1] R. Dutta & T. Dowling, (2009) "Secure and Efficient Group Key Agreements for Cluster Based Network" In Transactions on Computational Science Iv: Special Issue on Security in Computing. Lecture Notes in Computer Science, Vol. 5430. Springer-Verlag, Berlin, Heidelberg, 87-116.

[2] H. Shi, M. He, & Z. Qin, (2006) "Authenticated and Communication Efficient Group Key Agreement for Clustered Ad Hoc Networks" In 5th International Conference on Cryptology and Network Security –CANS 2006. Lecture Notes in Computer Science Vol. 4301, Springer-Verlag, pp 73-89.

[3] J. Silverman, (1986) The Arithmetic of Elliptic Curves, Springer Verlag.

[4] G. Yao, K. Ren, F. Bao, R.H. Deng, & D. Feng, (2003) "Making the Key Agreement Protocol in Mobile Ad Hoc Network More Efficient" In 1st International Conference on Applied Cryptography and Network Security - ACNS 2003, Lecture Notes in Computer Science Vol. 2846, Springer-Verlag, pp 343-356.

[5] J.C.M. Teo & C.H. Tan, (2005) "Energy-Efficient and Scalable Group Key Agreement for Large Ad Hoc Networks" In Proceedings of 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks. pp 114- 121.

[6] M. Burmester & Y. Desmedt, (1994) "A Secure and Efficient Conference Key Distribution System" In Advances in Cryptology - EUROCRYPT 1994, Lecture Notes in Computer Science Vol. 950, Springer-Verlag, pp 275-286.

[7] J.C. Teo, & C.H. Tan, (2007) "Denial-of-service resilience password-based group key agreement for wireless networks" In Proceedings of 3rd ACM Workshop on QoS and Security For Wireless and Mobile Networks. ACM, New York, NY, 136-143.

[8] R. Dutta, & R. Barua, (2008) "Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting" IEEE Trans. Inf. Theory 54(5), 2007-2025.

[9] R. Barua, R. Dutta, & P. Sarkar, (2003) " Extending Joux's Protocol to Multi Party Key Agreement" In Progress in Cryptology - INDOCRYPT 2003, Lecture Notes in Computer Science Vol. 2904, Springer-Verlag, pp 205-217.

[10] Dworkin M, (2001) NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation..

[11] Rivest, R (1995) "The RC5 Encryption Algorithm" In Proceedings of the 2nd Workshop on Fast Software Encryption (LNCS 1008). Springer-Verlag, pp 86 – 96, Berlin.

[12] Anderson, R., Biham, E., & Knudsen, L, (1998) "A Proposal for the Advanced Encryption Standard" http://ftp.cl.cam.ac.uk/ftp/users/rja14/serpent.pdf.

[13] S. Schmidt, H. Krahn, S. Fischer, & D. Watjen (2005) "A Security Architecture for Mobile Wireless Sensor Networks" LNCC 3313, Spronger-Verlag Berlin Heidelberg, pp 166-177.

[14] Guajardo, J., Bluemel, R., Krieger, U., & Paar, C, (2001) "Efficient Implementation of Elliptic Curve Cryptosystems on the TI MSP430x33x Family of Microcontrollers" In: Proceedings of the International Workshop on Practice and Theory in Public Key Cryptography '01 (LNCS 1992), Springer-Verlag, Berlin pp 365 – 382.

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

[16] E. Klaoudatou, E. Konstantinou, G. Kambourakis & S. Gritzalis (2011) "A Survey on Cluster-Based Group Key Agreement Protocols for WSNs" IEEE Communication Surveys & Tutorials, Vol 13, No 3.

[17] A. K. Das & D. Giri, (2011) "An identity Based Key Management Scheme in Wireless Sensor Networks" arXiv:1103.4676v1 [cs.CR].

[18] J.C. Lee, V.C.M. Leung, K.H. Wong, J. Cao & H.C.B. Chan, (2007) "Key Management Issues In Wireless Sensor Networks" Current Proposals And Future Developments. IEEE Wireless Communication.

[19] Blundo, C., Santis, A.D., Herzberg, A., Kutton, S., Vaccaro, U., & Yung, M (1993), " Perfectly-Secure Key Distribution for Dynamic Conferences" In Advances in Cryptology - CRYPTO '92 (LNCS 740). Springer-Verlag, pp 471 – 486, Berlin.

[20] Blom, R, (1985) "An Optimal Class of Symmetric Key Generation Systems. In Advances in Cryptology" EUROCRYPT '84 (LNCS 209). Springer-Verlag, pp 335 – 338, Berlin.

[21] National Institute of Standards and Technology (NIST), (2001) FIPS 197, Announcing the Advanced Encryption Standard. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Authors

Mr. V. K. Singh, Assistant professor II, joined Sikkim Manipal Institute of Technology, Mazitar, Sikkim, India in July, 2010 as an Assistant Professor II. He did his MCA and M. Tech from the department of CSE, SMIT. He has published a number of technical papers in various national and international journals in addition to presentation/ publication in several international / national conferences.

Dr. Kalpana Sharma, Professor of the Department of Computer Science & Engineering at Sikkim Manipal. Institute of Technology, Mazitar, Sikkim, India since August, 1998. She did her BE from National Institute of Technology, Silchar, India and M.Tech from IIT Kharagpur, India. She completed her P.hD in the field of Wireless Sensor Network Security. Her areas of research interest are Wireless Sensor Networks, Steganography, Network & Information Security, Real Time Systems and Software Engineering. She has published a number of technical papers in various national and international journals in addition to presentation/ publication in several international/ national conferences.