International Journal of Grid Distribution Computing
Vol.7, no.3 (2014), pp.23-28
http://dx.doi.org/10.14257/ijgdc.2014.7.3.03

# Security Vulnerability and Robust Security Requirements using Key Management in Sensor Network

Jaykumar Shantilal Patel[1] and Dr. Vijaykumar M. Chavda[2]

*[1]Chaudhari Technical Institute, MCA Department, Opp. S. T. Bus Depot, Sector-7, Gandhinagar, (Gujarat-INDIA)*
*[2]N. P. College of Computer Studies and Management-Kadi (Gujarat-INDIA)*
*[1]jay_sp_mca@yahoo.co.in, [2]dr.vijaychavda@gmail.com*

## *Abstract*

*Encrypt message with strongly secure key which is known only by sending and recipient end is a significant aspect to acquire robust security in sensor network. The secure exchange of key between sender and receiver is too much difficult task in resource constraint sensor network. To achieve secure key agreement is challenging task for sensor network environment. The key management helps to maintain confidentiality of secret information from unauthorized users. It can also check the integrity of the exchanged message to verify the authenticity. This paper discusses various constraints available in sensor network, vulnerability through the existence of various security attacks at each layer for the communication and lastly the security requirement using the key management. Here we present the public key management using Elliptic Curve Cryptography to ensure robust security in sensor network environment.*

**Keywords:** *Security constraint, Security vulnerability, Security attacks, Robust security, Key management, Public key, Elliptic Curve Cryptography (ECC)*

## 1. Introduction

In recent years, wireless sensor networks applications are increasing very fast such as battle field, disaster recovery, environmental monitoring and healthcare *etc.*, [1]. A wireless sensor networks is a collection of a large number sensor nodes that has limited computation, communication, storage and power resources distributed in a designed area without any fixed structure [1-3]. According to R. Abouhogail [4] the sensor network should have feature advantages like:

1. The space storage can be reduced.
2. The computational efforts can be reduced.
3. The communication costs can be saved.

The broadcast nature of communication, infrastructural constraint, power limitation and hostile environment for the deployment may lead to adversaries in sensor network. The adversaries of two types can introduce during the communication one passive and another active. The passive types of adversaries only eavesdrops the information communicating over the sensor network while the active adversary can eavesdrop and alter the information communicating over sensor network. So, we can say that passive attacks are attack on the confidentiality while the active attacks are attack on the authenticity. As a security primitive, key establishment plays the most crucial role in the designing of the security mechanism in

ISSN: 2005-4262 IJGDC

the wireless sensor networks (WSNs) [5]. Node can be compromised by an adversary to perform malicious activities. Currently, there is not any complete security framework that secures wireless sensor network from these kinds of inside attacks [1]. Most routing protocols used in WSNs do not consider security aspects due to resource constraints of the sensors including low computational power, limited memory, small power supplies and limited communication range [6, 7]. Unfortunately, the resource limitation of sensor nodes poses a great challenge for designing an efficient and effective key establishment scheme for WSNs [5]. Key management plays an important role on security in wireless sensor networks [8]. However, key management is WSNs is a difficult problem because of resource constraints of the sensor nodes [5]. Good Key management is very important to get protection in any communication system [4]. Information security is the hot topic of research for decades to deal the prevailing security requirements [9]. The numbers of mechanisms are available to provide robust security in sensor network using asymmetric or symmetric concept of cryptography. The algorithm is enriched with various calculations through which the cipher text becomes unpredictable and breaking the security by eavesdropper becomes harder [10]. The secure exchange of secrete key is the major issue related to the symmetric cryptography implementation. The asymmetric one is better than the symmetric in term of providing robust security. Only the requirement is to select the optimum algorithm for such resource constraint sensor network environment that has less communication as well as less computational overhead. In wireless network the packet must be lightweight, due to that it takes a large amount of time to transmit large file [11]. We found that the elliptic curve cryptography is the optimum way to implement public key concept in sensor network environment. The TinyOS is the real example that justifies the implementation of public key mechanism like ECC using MICA2 or MICAz motes. If one can wants to simulate the result on TinyOS using MICA2 or MICAz mote, has to use simulator TOSSIM. TOSSIM is a simulator designed for TinyOS to simulate various sensor network applications like security application.

## 2. Constraints in Sensor Network

The traditional security mechanism of normal computer network may not directly shift to the sensor network because of the resource constraint nature of the nodes. In order to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes [12]. Communication is more costly than computation in sensor networks [13]. Further, higher security levels in sensor networks usually correspond to more energy consumption for cryptographic functions. Thus, Sensor networks could be divided into different security levels depending on energy cost [14, 15]. Some of the major constraints of a WSN are listed below:

***Resource:*** Sensor node has limited resources, having low computational capability, low communication bandwidth and limited storage due to the battery operated devices.

***Message size:*** Usually the message size for the sensor network is very small in compare with the traditional network. Due to the small message size there is no concept of segmentation in most of the sensor network applications.

***Addressing:*** Sensor network is generally deployed with large number of sensor nodes. Due to these large number of sensor nodes it is too much difficult to build global addressing scheme for the communication because it ultimately lead to the additional computation to maintain the large number of the nodes across the large sensor network.

***Location awareness:*** Location awareness is very important in the sensor network because all communication across the sensor network environment is generally based on the location awareness of each node.

## 3. Security Vulnerability

The broadcast nature of communication, lack of infrastructure and hostile environment for the deployment may lead to vulnerability in sensor network. The different attacks are possible in various constraints based sensor network. The numbers of attacks are mention below that can lead to vulnerability in security feature of sensor network.

### 3.1. Security Attacks in Sensor Network:

Sensor network uses Application layer, Transport layer, Network layer, Data-link layer and Physical layer for the communication across the sensor network. These layers are having its own functionality and security requirements. According to the implementation they provide security. Every layer has its own set of protocol for unique functionality. Different attacks are transpiring at different layer for the communication. Following table shows the detail information regarding numbers of layer and relevant attacks as well as protocol implementation in sensor network.

**Table 1. Security Attacks on Specific Layer with Protocol Implementation [16]**

| Layers | Attacks | Protocols |
|---|---|---|
| Application Layer | Attacks on reality | BOOTP, DHCP, DNS, HTTP, POP3, SSH, Telnet |
| Transport Layer | Flooding, Inject false messages (data integrity attack), Energy drain attacks, De-synchronization | TCP, UDP, SPX |
| Network Layer | Spoofing, Selective forwarding or black, holes, Sinkhole, Sybil attack, Wormhole, Acknowledgement spoofing, HELLO Flooding | RIP, OSPF, EGP, IPX, IPV6, ARP |
| Data-Link Layer | Collision | Frame Relay, FDDI, Ethernet |
| Physical Layer | Jamming, Tampering | SoNet, ISDN, SDH |

## 4. Robust Security Requirements

Security requirements mainly focus on authentication, confidentiality and integrity. The authentication can achieve through hash or MAC / HMAC algorithms. Confidentiality can achieve through encryption algorithms. The encryption algorithms may have symmetric or asymmetric in nature. The integrity may ensure that the data that is send by authorized sender may receive at authorized receiver end as it is without modifying or alteration. Here the concept of authentication, confidentiality or integrity is selected based on the nature of the application being used for the communication across the sensor network.

***Availability:*** Ensure that services offered by entire sensor network should be available to all the node s whenever required even the presence of denial of services attacks.

***Authentication:*** Provide authentication to all the node and base station for utilizing the available limited resources. It also ensures that only the authorized node can participant for the communication.

***Integrity:*** Ensure that the message is not altered during the communication. In other word it ensures that there is no any active adversary present during the communication.

***Confidentiality:*** It prevent from the eavesdropping. Ensure the data that is to be transmitted must be confident to source and destination party only.

***Non repudiation:*** Prevent the malicious nodes to hide their activities.

***Data freshness:*** Ensure that data is recent and not replied by the adversary.

***Robustness:*** Ensure when some nodes are compromised because of any reason the entire network should not be disturb or compromised.

***Self-Healing:*** Nodes should be of self-healing / failure tolerant in nature.

***Time Synchronization:*** The protocols or algorithms used to provide robust security should be time synchronized, means these protocol or algorithm should not be manipulated to produce the incorrect data.

## 5. Public Key Scheme

WSNs have mostly been using symmetric key and other non public-key encryption schemes [17]. The main drawback of the scheme is that they are not flexible as public-key scheme but they are computationally faster. The secret sharing is the major issue for the symmetric key scheme. Due to the resource constraint nature and limited computational as well as limited communication capacity, the traditional public key algorithms are not directly shifted to the sensor network environment. They need to be optimized in terms of resource utilization and computational as well as communicational overhead. The implementations of such resource constraint public key algorithms are tested over the MICA2 mote using TinyOS environment. The Elliptic Curve Cryptography (ECC) is an ideal example of public key algorithm implemented in sensor network environment. The RSA algorithm is the competitor of ECC but having large computation and communication overhead due to it large key size. Elliptic curve cryptography (ECC) has a faster computation time, smaller keys, and uses less memory and bandwidth than RSA [18]. Both ECC and RSA can be accelerated with dedicated co-processors. Recently, ECC has been used [17–20] for WSNs.

### 5.1. RSA and ECC

Both RSA and ECC have been in research for many years. RSA was developed in 1977 and stand for Rivest Shamir Adleman algorithm. Still the RSA is one of the most popular symmetric key algorithms. The strength of the RSA is depends on complication of factoring very large numbers. ECC was developed in 1985 by Koblitz and Miller. The strength of the ECC algorithm is depends on the mathematics of elliptic curves. ECC can obtain the same security level as RSA while using a smaller key [20]. A 160-bit ECC key has the same security as a 1024-bit RSA key [18]. A 224-bit ECC key compares to the 2048-bit RSA key [18]. This is due to the fact that it takes exponential algorithms to solve the elliptic curve discrete logarithm problem as opposed to small runtime algorithms to solve the large number factorization in RSA [18]. ECC is computed by point multiplication on elliptic curves over prime integer fields or binary polynomial fields. The performance was even more favorable when comparing ECC-224 to RSA-2048 [18].

### 5.2. TinyOS public-key implementation:

TinyOS name it means suggest that it is tiny operating system designed for small environment like sensor nodes. MICA2 mote is a part of TinyOS. The MICA2 provide access control, authentication, confidentiality and integrity through TinySec. The TinySec is a feasible security solution. TinySec is not perfectly resilient to attacks. It relies on a single key, and therefore is unable to securely perform a rekey if necessary [21]. Discrete Logarithm Problem (DLP) is used to overcome TinySec's inability to securely distribute encryption keys [20]. The Diffie Hellman scheme is based on Discrete Logarithm Problem. It allows two nodes to agree on a secret key for communication over insecure channel. A MICA2 mote using ECC can effectively and securely distribute the 80-bit TinySec keys [20]. ECC is as secure as Diffie–Hellman while using vastly smaller key sizes. ECC also offers perfect forward security [20]. ECCM 2.0, it took on average 34.1 s to compute the 163-bit encryption keys [21].

### 5.3. Key management using ECC:

The key management using ECC is efficient in terms of speed, memory requirement and security level. The points on curve are considered for performing elliptic curve operation. The Bilinear paring based elliptic curve operations are much more convenient to perform the cryptographic primitive to achieve robust security in sensor network environment. The operations generally performed are scalar point addition and scalar point multiplication. Such kinds of operation are having less computation and communication overhead that is preferable in sensor network environment.

## 6. Conclusion

In this paper, we demonstrate various constraints in sensor network. We also specify the vulnerability situation where the various security attacks are occur at each layer during the communication. We also demonstrate the security requirement in sensor network and finally we suggest the public key management scheme using Elliptic Curve Cryptography to reduce storage space requirement, reduce communication as well as computational overhead and provide robust security using elliptic curve operation like point addition and point multiplications.

## References

[1] J. Xu, J. Wang, S. Xie, W. Chen and J. Kim, "Study on Intrusion Detection Policy for Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 7, no. 1, (**2013)** January, pp. 1-6.

[2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: a Survey", Computer Networks, vol. 38, no. 4, (**2002)**, pp. 393-422.

[3] K. Martinez, J. Hart, and R. Ong, "Environmental Sensor Networks", IEEE Computer, vol. 37, no. 8, (**2004)**, pp. 50-56.

[4] R. Abouhogail, "Security Assessment for Key Management in Mobile Ad Hoc Networks", International Journal of Security and Its Applications, vol. 8, no. 1, (**2014)**, pp. 169-182, http://dx.doi.org/10.14257/ijsia.2014.8.1.16,.

[5] J. Zhang, J. Tan, and J. Li, "Key Distribution using Double Keyed-hash Chains for Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 7, no. 5, (**2013),** pp. 17-28, http://dx.doi.org/10.14257/ijsia.2013.7.5.02.

[6] E. Ngai, J. Liu, and M. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks", IEEE International Conference on Communications, (**2006**).

[7] D. Martins and H. Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", 13th International Conference on Network-Based Information Systems, (**2010**).

[8] M. Jain, "Wireless Sensor Networks: Security Issues and Challenges", International Journal of Computer and Information Technology, vol. 2, no. 1, (**2011**), pp. 62-67.

[9] N. Sethi and D. Sharma, "A Novel Method of Image Encryption Using Logistic Mapping", International Journal of Computer Science Engineering, vol. 1, no. 2, (**2012**) November.

[10] S. Karmakar and S. Chandra, "An Approach for Ensuring Security and its Verification", International Journal of Computer Science Engineering", vol. 2, no. 3, (**2013**) May.

[11] M. Dinesh and E. Redddy, "Ultimate Video Spreading With Qos over Wireless Network Using Selective Repeat Algorithm",International Journal of Computer Science Engineering, vol. 2, no. 4, (**2013**) July.

[12] D. Carman, P. Krus, and B. Matt, "Constraints and Approaches for Distributed Sensor Network Security", Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, (**2000**).

[13] J. Sen, "A Survey on Wireless Sensor Network Security", International Journal of Communication Networks and Information Security, vol. 1, no. 2, (**2009**) August.

[14] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. Srivastava, "On Communication Security in Wireless ad-Hoc Sensor Networks", Proceedings of 11th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, (**2002**).

[15] L. Yuan and G. Qu, "Design Space Exploration for Energy-efficient Secure Sensor Networks", Proceedings of IEEE International Conference on Application-Specific Systems, Architectures, and Processors, (**2002**) July.

[16] P. Jaykumar and C. Vijaykumar, "Sensor Network Security Issues in Each Layer", International Journal of Computer Science Engineering, vol. 2, no. 5, (**2013**) September.

[17] A. Wander, N. Gura, and H. Eberle, "Energy Analysis of Public-key Cryptography for Wireless Sensor Networks", Third IEEE International Conference on Pervasive Computing and Communications (PERCOM), (**2005**).

[18] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs", Proceedings of the 6th International Workshop on Cryptographic Hardware and Embedded Systems, (**2004**) August; Boston, Massachusetts.

[19] X. Du, M. Guizani, Y. Xiao, S. Ci, and H. Chen, "A Routing-driven Elliptic Curve Cryptography based key Management Scheme for Heterogeneous Sensor Networks", IEEE Transactions on Wireless Communications, vol. 8, no. 3, (**2009**).

[20] X. Yang, K. Venkata, B. Sun, X. Du, F. Hu, and M. Galloway, "A Survey of Key Management Schemes in Wireless Sensor Networks", Science Direct - Computer Communications, (**2007**), pp. 2314-2341.

[21] D. Malan, M. Welsh, and M.D. Smith, "A Public-key Infrastructure for Key Distribution in TinyOS based on Elliptic Curve Cryptography", Proceedings of 1st IEEE International Conference Communications and Networks (SECON), (**2004**) October; Santa Clara, CA.