International Journal of Computer and Communication Technology

Volume 6 | Issue 2 Article 13

April 2015

A PUBLIC KEY DISTRIBUTION AND BROADCAST AUTHENTICATION SCHEME FOR WIRELESS SENSOR NETWORKS

SHANTALA DEVI PATIL
Department of CSE, REVA ITM, Bangalore, India, shantala.sj@gmail.com

VIJAYAKUMAR B P
Department of TCE, MSRIT, Bangalore, India, vijaykbp@yahoo.co.in

Recommended Citation
PATIL, SHANTALA DEVI and B P, VIJAYAKUMAR (2015) "A PUBLIC KEY DISTRIBUTION AND BROADCAST AUTHENTICATION SCHEME FOR WIRELESS SENSOR NETWORKS," *International Journal of Computer and Communication Technology*: Vol. 6 : Iss. 2 , Article 13.
DOI: 10.47893/IJCCT.2015.1290
Available at: https://www.interscience.in/ijcct/vol6/iss2/13

A PUBLIC KEY DISTRIBUTION AND BROADCAST AUTHENTICATION SCHEME FOR WIRELESS SENSOR NETWORKS

[1]SHANTALA DEVI PATIL & [2]VIJAYAKUMAR B P

[1]Department of CSE, REVA ITM, Bangalore, India
[2]Department of TCE, MSRIT, Bangalore, India
Email: shantala.sj@gmail.com, vijaykbp@yahoo.co.in

Abstract - In Wireless Sensor Networks, Broadcast communication is the most fundamental and prevailing communication pattern. Securing the broadcast messages from the adversary is critical issue. To defend the WSNs against the adversary attacks of impersonation of a broadcast source or receiver, modification/fabrication of the broadcast message, attacker injecting malicious traffic to deplete the energy from the sensors, broadcast authentication of source and receivers becomes extremely inevitable. In this paper, we propose a novel ECC based public key distribution protocol and broadcast authentication scheme. The proposed method provides high security and has low overhead.

Keywords*: pkc , key management, broadcast authentication.*

1. INTRODUCTION

A Wireless Sensor Networks consists of a large number of resource constrained sensor nodes[2] that are spatially distributed in an hostile environment and the with resource rich node called as the Base Station(BS). The sensor nodes task is to sense physical phenomena from its immediate surroundings, process and transmit the sensed data to the other nodes or Base stations. WSNs are used in applications that are sensitive to environmental parameters that require monitoring, tracking and controlling. In the course of WSN's computing and communication aspect broadcast transmission is one of the most dominant communication and there are two types a: *network broadcast b: local broadcast*. Usually, broadcast communication in WSN is used to collect data from sensors and update the routing information. Since the nodes after the deployment cannot be manually maintained and monitored, security becomes critical.

In such a scenario maintaining and monitoring of sensor node and their network of communication becomes a major issue and information security will be a critical challenge in WSN because attacks from adversaries(with powerful resources)[4] can be active or passive and internal or external and attacks against basic WSN operation or against security mechanisms. Similarly, the attacks of impersonation of a broadcast source or receiver, modification/fabrication of the broadcast message [1] and attacker injecting malicious traffic to deplete the energy from the sensors will be a major problem. Broadcast authentication of source and receivers becomes important factor and we have proposed to consider this aspect in our work.

Authentication [2] is a procedure in which the sending entity signs the message using the private key and the receiving entity verifies the authenticity of the message with the public key of the sender. Verifying and guaranteeing the public key and its distribution belong to the sender becomes a challenging issue in WSN that uses broadcast communication. Usually, it is solved by the Certificate authority (CA) a trusted third party certifying that a public key belongs to a sender. Hence we propose a novel public key distribution protocol to distribute the public keys securely in which the public keys are usable only by the non-malicious nodes(regular nodes) and a scheme to achieve broadcast communication using the public keys received through the public key distribution protocol.

The remainder of this paper is organized as follows. Section 2 reviews the related work in WSN. Section 3 discusses the system description followed by proposed method in section 4. Section 5 concludes this paper.

2. RELATED WORK

The existing authentication schemes are given below

Certificate –Based Authentication Scheme: In [6] Each user and the Sink of WSN is pre-deployed with Public/private key pair. The sink serves as a CA. The sink issues each user a Public key certificate and broadcasts the message using this certificate. The receiver sensor nodes verify the authenticity of the received message. But the scheme is inefficient to support user revocation and takes two signature operations for verification which is energy consuming.

Merkel Hash Tree Based Scheme: In the basic Merkel tree based authentication scheme[6], the sink collects all the public keys on the current network users and constructs a Merkel hash tree. Each node obtains its AAI according to the corresponding leaf nodes location in the Merkel Hash Tree. The user revocation problem is reduced to a great extent and

storage is efficient but communication is inefficient.

ID based Scheme[6]: adopts an automatic public key update technique , it eliminates the existence of the certificates or the AAI and requires much smaller space storage space to support user revocation.

Perrig et al. [7] proposed µTESLA, a well known broadcast authentication scheme for the WSNs. It is based on symmetric key cryptographic techniques, and hence is secure. However as proved by [29] the symmetric key based algorithms are not as secure against the node compromise. Many variants of µTESLA are proposed for WSNs (e.g., [8] [9] [10] [11]) to improve its performance. The variants as well as µTESLA, however, are subject to the following defects. First, maintenance of time synchronization in WSNs is a complicated task. Second, distribution of the initial parameters introduces heavy overhead since it is implemented by the unicast transmission. Third, delayed authentication is inevitable.

Ren et al. [12] and Du et al. [13] propose to authenticate broadcast messages of WSNs with PKC since overhead of PKC for WSNs has significantly been reduced by using Elliptic Curve Cryptography (ECC). Nevertheless, the PKC based broadcast authentication schemes so far are not affordable by current generation of sensor nodes because of the intensive use of Elliptic Curve Digital Signature Algorithm (ECDSA). Gennaro *et al*. [14] propose signature amortization to sign efficiently digital streams. A number of improvements are developed soon (e.g., [15] [16] [17] [18] [19]).

The existing clustering schemes are listed below

LEACH [25]) is the first clustering algorithm that was proposed for reducing power consumption in WSNs. In LEACH, the clustering task is rotated among the nodes, based on duration. Direct communication is used by each cluster head (CH) to forward the data to the base station (BS).But LEACH is not applicable to networks deployed in large regions., PEGASIS [26] The main idea in PEGASIS is for each node to receive from and transmit to close neighbors and take turns being the leader for transmission to the BS. This approach will distribute the energy load evenly among the sensor nodes in the network. Initially the nodes are placed randomly in the play field, and therefore, the i –th node is at a random location. The nodes will be organized to form a chain, which can either be accomplished by the sensor nodes themselves using a greedy algorithm starting from some node. Alternatively, the BS can compute this chain and broadcast it to all the sensor nodes., TEEN [27] TEEN is suitable for time-critical sensing applications**.** Moreover this protocol is quite efficient in terms of energy consumption and response time. The main disadvantage of this scheme is that when periodic reports are needed and if the threshold is not received, the user will not get any data from the network at all. This scheme inappropriate for periodic monitoring of events. and APTEEN [28] APTEEN is an improvement to TEEN to overcome its limitation and aims at both capturing periodic data collections as LEACH and reacting to time-critical events as TEEN. All the Cluster Heads form a network and above them lies the Base Station- with highest power and no resource restriction.

3. SYSTEM DESCRIPTION

3.1 SYSTEM MODEL

WSN comprises of spatially distributed sensor nodes in hostile unattended environment. All the sensor nodes of the WSN communicate with the Base Station. Base station's function is to aggregate the data and process it. For simplicity, we consider a WSN with clusters. The organization of the network is shown in Figure 1.

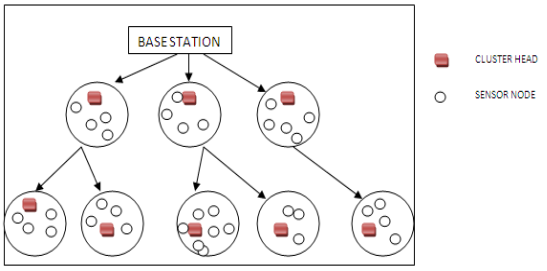

Figure 1: Organization Of Nodes In Wsn

Clustering is grouping of nodes into a feasible size and then assigning each cluster a cluster head. The cluster head is a node with highest energy in the cluster that is capable of performing the data aggregation and processing, usually pre-assigned or elected. The main objective of clustering is to extend the lifetime of the WSN by reducing the energy consumption. Also, clustering makes WSN easily scalable, by attaching a new cluster with a cluster head.

3.2 SECURITY MODEL

To achieve secure communication and provide authentication, keys are critical. In WSN Key distribution is based on 2 methods 1:Symmetric method: where the sender and the receiver both use same secret key and 2:Public Key Method: this method involves the use of pair of keys at both sender and receiver. The Public key method is more secure than that of symmetric key method as there is no need for key sharing and key management is easy since it's more resilient to node capture attacks.

Because the WSN's were highly resource constrained and also that public key cryptography(PKC) involved heavy calculations , it was claimed that PKC is highly infeasible in the WSN environment until proved otherwise. Extensive research was carried out for implementing the PKC algorithms on the WSN viz the RSA, Diffie Hellman Key Exchange Algorithm and ECC on various sensor nodes. From the analysis it was proved that ECC is better than RSA as the key size of RSA-1024 bits is too large compared to ECC of 160 bits.

The ECC implementation for WSNs, public keys generation takes 34 seconds (sec), and shared secrets can be distributed within the same time by using just over 1 KB of SRAM and 34 KB of ROM.

ECC algorithm is based on the following rules:
When two points on the elliptic curve are added, we obtain the third point that also lies on the elliptic curve.
In an elliptic curve the multiplication of a point on the curve with an integer i.e., k*P can also be obtained by addition and thus be defined as the sum of k copies of P. For eg: 2*P=P+P and 3*P=P+P+P and so on.
The ECC algorithm works as follows in all the sensor nodes:
A: Key Generation
Let F be a non-secret fixed curve point.
1: A node selects a secret random number PR that is the secret key of the node.
2: The Public key PU of a node is calculated as PU=PR*F. PU is publicized by the node.
B: Message Transmission
Say node A(has key pair PUa and PRa) wishes to send a message M to node B(has key pair PUb and PRb)
1: The node A computes PRa*Pub and uses the result as secret key.
2: The node B can retrieve the secret key by calculating PRb*PUa
since,
PRb*PUa=PRb*(PRa*F)=(PRb*PRa)*F=PRa*(PRb*F)=PRa*PUb.

3.3. NOTATIONS IN PROPOSED MECHANISM
For the sake of convenience, the following notations are used.*Base Station(BS):*It has two keys-public key(PUbs) and the private key(PKbs) generated using the ECC algorithm (as explained above) and pre-deployed. A copy of the public key of base station is pre-deployed in the cluster heads. *Cluster Head(CH):* also have a pair of public key (PUch) and the private key (PRch). The public key of the Cluster heads is pre-deployed in all the sensor nodes. Also acts as Certificate authority that cannot be compromised by the adversaries. The CH has a table called as the SensorNodeTable which stores the details of all the nodes that have registered itself to the cluster during the bootstrapping phase. *Sensor nodes*: has the public key and the private keys(PUs/PRs) and identity IDs.Nonce: is a unique random number, generated by the node.Hash function(H): A cryptographic hash function is an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value. The data to be encoded is called the "message," and the hash value is called the message digest or simply digest. Certificate identity : IDs. The notations are summarized in the table 1

SYMBOL	DEFINITION
BS	Base staion
PUbs	Public key of base station
PRbs	Private key of base station
CH	Cluster head
PUch	Public key of cluster head
PRch	Private key of cluster head
S	Sensor node
PUs	Public key of sensor node
PRs	Private key of sensor node
IDs	Identity of sensor node
Nonce	Random value
KS	Session key
H	Hash function
E	Encryption
D	Decryption
CertREQ	Request for certificate
||	Concatenation
Cs	certificate

TABLE 1: NOTATION USED IN PROPOSED PROTOCOL

4. PROPOSED METHOD

In this section we discuss the proposed method. The proposed method has two functions 1: the public key distribution protocol 2: broadcast authentication scheme

4.1. THE PUBLIC KEY DISTRIBUTION PROTOCOL

In the bootstrapping stage , all the nodes register themselves to the CH, the details of all the registered nodes is stored in the SensorNodeTable by the CH.

Protocol Scenario:
The main aim of the protocol is to securely distribute the public key to all the nodes in the cluster. This is achieved by 3 step procedure:
1: The sensor node requests for a Certificate from the Sensor node for validating itself to the Cluster.
2:The cluster head creates a Certificate for the requested sensor node and broadcasts it to all the sensor nodes in the cluster.
3: The sensor nodes of that cluster, who receive the certificate from the Cluster Head, update their table with the public key of the new sensor node.

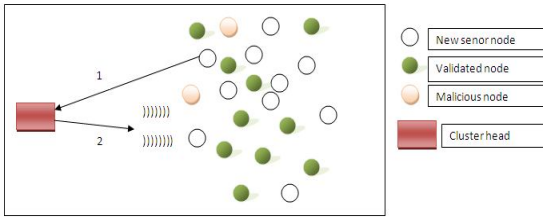

Figure 2: Protocol Scenario Within A Cluster

A brief discussion of the 3 step procedure is given in the following section and summarized in Table 2

Step 1: Sender selects a nonce – unique random number and finds the Hash H of the nonce which is stored in the sender as the secret session key KS,

KS(IDs)=H(nonce)

and sends a Certificate request to the CH. The certificate request contains the IDs, the PUs and nonce which are encrypted using the PUch.

CertREQ= EPUch(IDs||PUs||nonce)

Step 2: The CH receives the CertREQ, decrypts using the PRch, updates the SensorNodeTable at the CH with the node details

IDs||PUs||nonce =DPRch(CertREQ)

and then calculates the HASH H of the Nonce ,which also updates/stores in the SensorNodeTable

KS(IDs)=H(nonce)

that is encypted with the CH private key and broadcasts to the other receiver nodes in the cluster

EPRch(KS(IDs))

The CH replies back with the encrypted Certificate Cs which contains the IDs, the PUs and nonce which are encrypted using the PUch.

Cs=IDc||IDs||EPRch(IDc||IDs||PUs||nonce)

EKS(IDs)(Cs))

Step 3: The sender S receives the encrypted certificate from the CH, which it can decrypt using the secret key calculated by hashing the nonce and broadcast the same to the other nodes. The other nodes have already received the secret key from the CH only valid receivers who have the public key of the CH can decrypt and utilize the certificate obtained from the sender. At the receiver to obtain the public key of the sender

KS(IDs)=DPUch(EPRch(KS(IDs)))

Cs=D KS(IDs)(EKS(IDs)(Cs))

The public key distribution protocol is efficient for the WSNs. The certificate remains valid unless explicitly revoked by the CH or the Base station , the PRs can be used to encrypt the broadcast message as long as the certificate is revoked. The receivers never contact the CA throughout the protocol.

The public key distribution protocol is quiet secure way to exchange the PUs with the receivers, as all the time the message is kept confidential by encrypting it. The messages can be utilized, only by the nodes that are registered and have the CHs public key. Hence this strongly secures the protocol.

4.2.BROADCASTAUTHENTICATION SCHEME

The Broadcast authentication scheme is as follows:

Step 1: Each user of the WSN is equipped with a public/private key pair (PU/PR), and signs every broadcast message M with PR using a digital signature scheme such as ECDSA [10]. The message that is broadcast is of the form

Eks(IDs)(M||SIGPRIDs {h(IDs||M)}, IDc)

Step 2: The broadcast message is received by the other nodes which perform the verification. Message verification contains two steps: the sender verification by decrypting the message with the KS(IDs) obtained during the public key distribution and the message signature verification as in ECDSA[10].

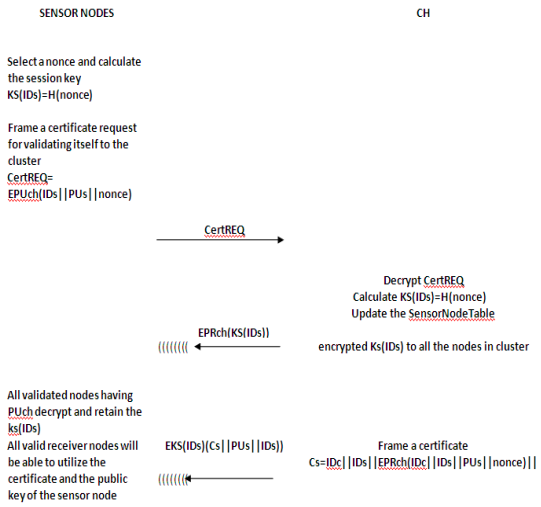

TABLE 2: SUMMARY OF KEY DISTRIBUTION PROTOCOL

5. CONCLUSION

Many WSN applications require communication between the sensor nodes to be secure and free from attacks by malicious nodes. This is achieved from the proposed protocol that secures communication by distributing the public key securely. The public key that is broadcast, can be retrieved only by the regular nodes, where as malicious nodes cannot. The proposed scheme has low overhead and retains high security by avoiding all the malicious nodes from being able to interpret the messages received from the sender nor the CH. This Scheme does not require any time synchronization and also achieves immediate authentication.

REFERENCES

[1] Sunil Gupta, Harsh Kumar Verma " Authentication protocol for wireless sensor networks" Paper at World Academy of Science, Engineering and Technology 2010.

[2] Dan Khanh Vu "Wireless Sensor Network Architecture And Its Security Challenges" Thesis submitted at California State University, Sacramento, 2010.

[3] A. Perrig Et Al. SPINS: Security Protocols for Sensor Networks. Wireless Networks vol. 8, 2002, Pages 521-

[4] Q. Huang ET Al. Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks. WSNA '03, September 19, 2003, Pages 141-150

[5] Rashmita Rautray and Itun Sarangi " A Survey on authentication Protocols for Wireless Sensor Networkss". International Journal of Engineering Science and Technology. 2011.

[6] K.ren ,K.Zng,W.Lou.P.Moron" On Broadcast Authentication in Wireless Sensor Networks" IEEE transactions on WSN,vol 6.no 11,November 2007.

[7] A .Dhawale,M.B.CHandak,N.v.Thakur,"Authentication techniqures in WSN" MPGI conference , Proceedings published by International Journal of Computer Applications® (IJCA)ISSN: 0975 – 8887. 7-8 April 2012.

[8] C. Jiang, B. Li and H. Xu (2007), "An efficient scheme for user authentication in wireless sensor networks", 21st International Conference on Advanced Information Networking and Applications Workshops, pp 438 - 442.

[9] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," In proceedings of INFOCOM, 2003.

[10] D. Hankerson, A. Menezes, S. Vanstone, "Guide to Elliptic Curve Cryptography," ISBN 0-387-95273-X, 2004.

[11] H.-R. Tseng, R.H. Jan and W. Yang (2007), "An improved dynamic user authentication scheme for wireless sensor networks", Global Telecommunications Conference, pp 986 – 990

[12] Roberto Di Pietro, Luigi V. Mancini and Alessandro Mei (2006), "Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks", Springer Science + Business Media, LLC 2006

[13] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Defending DoS attacks on broadcast authentication in wireless sensor networks," in Proc. 2008 IEEE ICC, pp. 1653–1657.

[14] R. Gennaro and P. Rohatgi, "How to sign digital streams," in Advances in Cryptology-CRYPTO, Lecture Notes in Computer Science, 1997, vol.1294, pp. 180–197.

[15] C. K. Wong and S. Lam, "Digital signatures for flows and multicasts," IEEE/ACM Trans. Networking, vol. 7, no. 4, pp. 502–513, 1999.

[16] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in Proc. 2000 IEEE Symposium on Security and Privacy, pp. 56–73.

[17] S. Miner and J. Staddon, "Graph-based authentication of digital streams," in Proc. 2001 IEEE Symposium on Security and Privacy, pp. 232–246.

[18] J. M. Park, E. Chong, and H. Siegel, "Efficient multicast packet authen- tication using signature amortization," in Proc. 2002 IEEE Symposium on Security and Privacy, pp. 227–240.

[19] A. Pannetrat and R. Molva, "Efficient multicast packet authentication," in 2003 Network and Distributed System Security Symposium.

[20] D. Liu and P. Ning, "Multilevel µTESLA: broadcast authentication for distributed sensor networks," ACM Trans. Embeded Computing Syst., vol. 3, no. 4, pp. 800–836, 2004.

[21] Y. Zhou and Y. Fang, "BABRA: batch-based broadcast authentication in wireless sensor networks," in Proc. 2006 IEEE GLOBECOM, pp. 1–5.

[22] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broad- cast authentication in wireless sensor networks," ACM Trans. Sensor Networking, vol. 4, no. 1, pp. 1–35, 2008.

[23] T. Kwon and J. Hong, "Secure and efficient broadcast authentication in wireless sensor networks," IEEE Trans. Computers, vol. 59, no. 8, pp.1120–1133, 2010.

[24] M. Younis, M. Youssef and K. Arisha, ìEnergy- aware management in cluster-based sensor networksî, Computer Networks 43 (5), 2003, 649ñ 668.

[25] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, ìEnergy-efficient communication protocol for wireless microsensor networks,î in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000, no. 10, vol.2, Jan. 2000, 4-7.

[26] S. Lindsey and C.S. Raghavendra, ìPEGASIS: power efficient gathering in sensor information systems,î in: Proceedings of the IEEE Aerospace Conference, BigSky, Montana, March 2002.

[27] A. Manjeshwar and D.P. Agrawal, ìTEEN: a protocol for enhanced efficiency in wireless sensor networks,î in: Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.

[28] A. Manjeshwar and D.P. Agarwal, ìAPTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks,î in: Parallel and Distributed Processing Symposium. Proceedings International, IPDPS 2002, 2002, 195ñ202.

[29] Al-Sakib Khan Pathan and Choong Seon Hong "Feasibility of PKC in Resource-Constrained Wireless Sensor Networks" Proceedings of International Workshop on Internet and Distributed Computing Systems (IDCS' 08) 24 December, 2008, Khulna, Bangladesh

◈◈◈