International Journal of Electronics and Communication Engineering.
ISSN 0974-2166 Volume 7, Number 1 (2014), pp. 7-12

http://www.irphouse.com

Public Key Cryptanalysis Scheme Using Hierarchical Structure in Wireless Sensor Networks

K.Aanandha Saravanan[1] N.Vignesh Prasanna[2]
D.Balaji[3] Sivakumar[4] Karthick[5]

[1, 2&3]Asst.Professor, ECE Department, [4&5]Asst.Professor,EEE Department,
VelTech Dr.RR &Dr.SR Technical University

Abstract

The growth of wireless sensor networks is widely spread over different applications, need of security mechanism is been the main issue nowadays. Therefore it is necessary to communicate between the sensor node protectively .The key management mechanism plays a major role in providing security in wireless sensor network. We propose an architecture which is established between the sensor node, cluster head and mobile sink with the use of one way hash function. When a message is transmitted its first packet consists of public key and the message header, when the first message is authenticated then the message header uses hash function to generate then next message block , which consist of message and hash key. The polynomial pool used by the mobile sink and cluster head will be different from the pool used by cluster and cluster head . Mobile sink will use the key from mobile polynomial pool and cluster node will use the key from the static pool and mobile pool and the sensor node will use the key from static pool.

Keywords- DIFFIE-HELLMAN ALGORITHM, ECSDA, SIGNATURE VAPOUR, HASH FUNCTION

1. INTRODUCTION

Recent Achievements in the miniature electronic and wireless communication has led to development of WSNs. WIRELESS SENSOR NETWORKS (WSN's) are widely becoming popular in the present world due to low power and low cost which are even deceasing as we write this. They basically are consisting of a Sensor Node, a transreceiver and a microprocessor which is wirelessly connected to each other. This has a wide variety of application right from agriculture to latest Industrial monitoring equipment.

In many of these applications, Information from the sensor is transmitted to the base station to process the vital information .The Authentication and key management mechanisms are vital in information transfer. The sensor nodes which transfer data they usually go, for broadcast as they don't have specific node ids which operate. So key wise security scheme is used for the transmission of the data over such networks .In this method the data are used are encrypted using a particular key, decryption key is only available in the nodes. But when such a scheme is used then the keys are usually stored in the sensor nodes, so when the Nodes is compromised the attacker has an access to the key so it can launch nay of the attacks, so the encryption has to be made an efficient one. In replication attack there is a problem in authentication and key management mechanism in wireless networks. There may be several adversaries with powerful resources (e.g., laptops). They can launch both external as well as internal attacks. In the external attacks, adversaries can eavesdrop for sensitive information, inject forged messages, and replay previously intercepted messages. They can also launch Denial-of-Service (DoS) attacks and jam the communication channel. But, we assume that the DoS and jam attacks cannot continue constantly without being detected and removed. In the internal attacks, adversaries are able to compromise some sensor nodes and obtain the sensitive information (e.g., secret keys). Later, the sensitive information may be used for attacking the rest of senor nodes in the network. For instance, it takes 14 seconds for an exponential operation of 1024-bit RSA on Mica1 motes. Besides resource constraints, sensor nodes are vulnerable to node compromise attacks. This renders application of conventional symmetric key cryptography based broadcast authentication schemes to WSNs impractical. Several author proposed a broadcast mechanism which exhibits a symmetry key process to authenticate messages .This model becomes failure due to delayed disclosure of nodes. Where some author describes *a message authentication scheme based on ECC.*

2. PROPOSED MODEL

The model we propose to use three-tier architecture with Elliptic Curve Digital Signature Algorithm and signature vapour and Diffie-Hellman Algorithm. This algorithm will be will be briefly explained in next sections one by one.

A.THREE TIER ARCHITECTURE

In this we have chosen Blundo Scheme to construct our approach, Use of the Blundo scheme, therefore, greatly eases the presentation of our study and enables us to provide a clearer security analysis. In three-tier architecture , the sensor node are grouped into two groups .First group consist of normal *Sensor* which perform the data acquisition or the data collection of the hostile environment, Secondly the sensor group of the data are *Stationary Access Points Or Cluster Heads* when this node collects data from the sensors which are group under it. Now the servers or the device which rely on the data from the network are called *Mobile Sinks*. Those are the servers which generally work on data are the Mobile sinks. Now the three tier architecture is formed when the sensor group under one stationary access node, which is again

connected to the mobile sink , so when the mobile sink needs the data , it contacts the particular cluster heads which in turn collects the data from the sensors. Now if an sensor wants to transmit sensor wants to transmit then it has two ways,

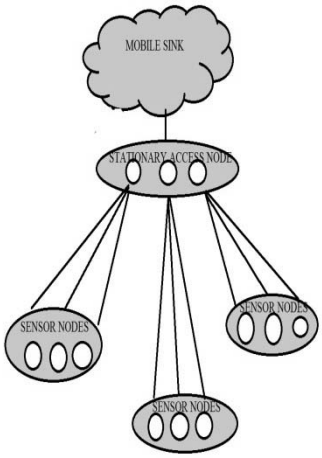

Fig.1. Three Tier System Model

Firstly, direct key discovery i.e. is the sensor nodes contacts the access exchanges the key with it which in turn contacts the mobile sink .Secondly, indirect via stationary node i.e. it contacts a stationary node which in turn contacts another stationary node which contacts the sink .In this model we use two encryption we use two encryption methods namely Diffie-Hellman Algorithm and ECSDA two differentiate between the two models, first we use an ECDSA algorithm, and signature vapour between mobile sink and stationary nodes and whereas the Diffie-Hellman Algorithm and signature vapour is used in between the stationary node and sensors .This means that the data will be made will be authenticated twice while it travels from sensor node to mobile sink the algorithms will be discussed briefly in the following sections. For clarity, we consider that one sender broadcasts messages to many receivers. In the network with multiple senders, each sender and its corresponding receivers are just the case we are considering. We consider that the entire sensor node has been given adequate power supply and has enough life cycle, we consider only one mobile sink to be, in real life situation the no. of mobile is not limited . Nor is the no of sensor nodes in each cluster, neither the no. of the clusters used. Our proposal can be used to any situation present in the real life world. The main advantage of the system is that an attacker has to know the private key to launch an attack which becomes little difficult in the scenario.

B. SIGNATURE VAPOUR

The Signature vapour is an technique to generate an self sufficient message which when authenticated can lead to generation of the packet, this concept is used to reduce the generational computation time required to authenticate all the message, as the message will needed to be authenticated only once in the whole transmission of the

whole packet. It can be described in three easy steps i.e. 1. Generating extended block 2. Broadcasting the extended block .3. Verifying the extended block.

1. Generating Extended block

In this method, Message M containing the *'n'* message is broken into 'k' blocks of B_i, 1<i<k, Then each block is broken into b messages m_j, 1<j<b.

Now, each block of the message is concatenated using the function CON as shown below.

CON $(B_i) = m_{(i-1)\ b+1}||.||m_{ib}$, $1 \leq i \leq k$

Then, $CON(Bi)$,$1 \leq i \leq k$, is padded with authenticators, denoted by $PAD(CON(Bi))$ as shown in equation (3).$CON(Bj)$, $1 \leq j \leq k-1$, is padded with digest $dj+1$ which is the digest of $PAD(CON(Bj+1))$. Now when the signature in the first field is authenticated then the whole message is authenticated by the use of hash function

2. Broadcasting the Extended block

Authentication the each message depends on the arrival of the last packet which makes the authentication possible of the next message using the digest present in the first message , Hence the message has to be received in an sequential manner.

We employ the sequential broadcast and reliable broadcast to guarantee the successful authentication of extended blocks with low overhead. As well, they ensure the integrity of *M* to applications.

3 .Verification of the Extended Block

According to broadcasting extended blocks step, $EB0$ reaches receivers in R first. $d1$ in $EB0$ is authenticated by the signature, that is, if $D(PUs,E(PRs, d1)) = d1$, $d1$ is authentic. Extended blocks in $EB*$ are authenticated in an efficient way, just using a collision resistant hash. Digest di, $1 \leq i \leq k$, in $EBi-1$ that reaches receivers in R in advance is used to authenticate EBi.

C. ECDSA

The ECDSA signature is on the basis of ECC, which offers equivalent security with substantially smaller key size compared to RSA. Thus, ECC has the advantages in computation, bandwidth and memory savings. Because of the advantages, $d1$ in $EB0$ is signed with an ECDSA signature. Here, we introduce briefly generation and verification of the ECDSA signature.

Sender s and receivers in Rs establish elliptic curve domain parameters $T = (p, a, b, G, q, h)$ in advance. Storing T in sensor nodes before deployment is an option. p is a prime that specifies the finite field Fp. a and b are coefficients of the elliptic curve $y2 \equiv x3+ax+b \pmod p$ where $4a3+27b2 \equiv 0 \pmod p$. G refers to the base point on the elliptic curve. q is a prime indicating the order of G. h is the cofactor $h = \#Ep(a, b)/q$ where $\#Ep(a, b)$ stands for the number of points on the elliptic curve. To sign digest $d1$, sender s creates the key pair (PRs, PUs) that satisfies $PUs = PRsG$ where PRs is an integer in Fp and PUs is a point on the elliptic curve. Then, it selects an ephemeral key pair (u,U) that satisfies $U = uG$ where u is an integer in Fp and U is a point on the

elliptic curve. It computes $r \equiv xU \pmod{q}$ where xU is the x coordinate of point U, and $de = H(d1)$ where H is a collision resistant hash. It sets $e = de$ if $\_log2q\_ \geq Lde$ where Lde refers to the length of de. Otherwise, let e equal the leftmost $\_log2q\_$ bits of de. At last, it computes $w \equiv u^{-1}(e + rPRs) \pmod{q}$. r and w are the ECDSA signature. The complete expression of $EB0$ is $EB0 = d1||r||w$. Verification of $d1$ proceeds as follows. The receiver computes $de = H(d1)$ where H is a collision resistant hash. Then it sets $e = de$ if $\_log2q\_ \geq Lde$ where Lde refers to the length of de. Otherwise, let e equal the leftmost $\_log2q\_$ bits of de. It computes $v1 \equiv ew-1 \pmod{q}$, $v2 \equiv rw-1 \pmod{q}$, $V = v1G + v2PUs$, and $v \equiv xV \pmod{q}$ where xV is x coordinate of point V. At last, it compares v to r to verify whether $d1$ is authentic.

D Diffie-Hellman Algorithm

This algorithm uses an shared secret key concept on the data encryption and decryption the main objective of the uses of the concept that a*b =b*a. Here the two users generate any two prime which mutually exclusive .The process of the key generation is listed below

Let A & B need to communicate , they first decide two numbers '*c'* and *'e'*

Now both of them generate the private numbers *'p'* & *' q'* which are there secret key

Now A computes the public key

$x=c^p \bmod e$

Now B compute the public key

$y=c^q \bmod e$

Now they both calculate the secret key

$z= x^p \bmod e= y^q \bmod e$

6. Calculate $(c^{pq})^{-1}$.

$(c^p)^{|C|-q} = c^{p(|C|-q)} = c^{p|C|-pq} = c^{p|C|}c^{-pq} = (c^{|C|})^p c^{-pq} = 1^p c^{-pq} = c^{-pq} = (c^{pq})^{-1}$.

ii. Encryption

Now the data m is converted into integer using proper function then it is signed by sending as

$tx=mc^{pq}$

iii. Decryption

Now the data can be decrypted by

$m=txc^{-pq}$.

3. CONCLUSION

In this paper we proposed the safety architecture for the wireless sensor networks. The proposed paper improved the resilience against the Mobile Node Replication attack with compared to polynomial pool method , Use of two different algorithm and signature vapour leads to WSNs being less vulnerable to the attacks done by the Adversaries. The security scheme has imporved performance against various attacks.

4. REFERENCES

[1] A.Rasheed and R.Mahanatra,'An energy efficient hybrid data collection sheme in wireless sensor networks'Sensor networks and information processing, 2007.
[2] Wong, Wing and Wang, 'Verifiable secret redistribution for threshold sharing scheme,Mellon University,Sept 2002.
[3] B.Wu,J.Wu,'Secure and efficient key management in mobile adhoc wireless network',2005.
[4] Rafoneli and Hutchson,'Survey of key management for secures group communication'ACM Computer survey.
[5] Johnson and maltz,'Dynamic source routing in adhoc wireless network',Mobile communication,1996.
[6] Duma and Shahmedri,'A hybrid key tree scheme for multicast to balance security and efficiency requirement,2003.
[7] Karlof,Magner,'Secure routing in WSN attack and counter measures in adhoc network,Sept 2003.