International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 1 Article 10

October 2012

SECURITY IN WIRELESS SENSOR NETWORKS USING ASSYMETRIC KEY BASED TECHNIQUES

RASHMI MOTHKUR
ISE, M.S.R.I.T, Bangalore, India, rmothkur@gmail.com

GEORGE PHILIP C
ISE, M.S.R.I.T, Bangalore, India, gphilipc@gmail.com

SECURITY IN WIRELESS SENSOR NETWORKS USING ASSYMETRIC KEY BASED TECHNIQUES

RASHMI MOTHKUR[1], GEORGE PHILIP C[2]

[1]M.Tech (Software Engineering), [2]Associate Professor, ISE, M.S.R.I.T, Bangalore, India

Abstract- Wireless sensor networks (WSNs) have recently attracted a lot of interest in the research community due their wide range of applications in our lives ranging from military applications to civilian ones.. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. This problem is more critical if the network is deployed for some mission-critical applications such as in a tactical battlefield. Random failure of nodes is also very likely in real-life deployment scenarios. Due to resource constraints in the sensor nodes, traditional security mechanisms with large overhead of computation and communication are infeasible in WSNs. Security in sensor networks is, therefore, a particularly challenging task. In this current paper, we fundamentally focus on the security issue of WSNs and propose a protocol based on public key cryptography for external agent authentication and session key establishment. The proposed protocol is efficient and secure in compared to other public key based protocols in WSNs.

Keywords- *Wireless sensor networks, Security, Public key techniques, Cryptography, Authentication.*

I. INTRODUCTION

Wireless sensor networks consist of small nodes that sense their environment, process data, and communicate through wireless links. Sensor networks closely interact with their physical environment and with people, posing new security problems. Security in wireless sensor network is different compared to security in LANS, WANS, Internet etc. This is due to the constraints of sensor nodes on battery power, CPU, memory and WSN is Wireless, Ad hoc, Unattended. Hence it poses new security problems and research challenges. Many WSN are involved in critical and secure applications[4] like military surveillance and Enemy movement, hence providing security to data is critical challenge.

Due to the constraints, it is difficult to directly employ the conventional security mechanisms in WSNs. In order to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes . Some of the major constraints of a WSN are listed below[2].

Energy constraints: Energy is the biggest constraint for a Wireless Sensor Networks. In general, energy consumption in sensor nodes can be categorized in three parts: (i) energy for the sensor transducer (ii) energy for communication among sensor nodes and (iii) energy for microprocessor computation.

Memory limitations: A sensor is a tiny device with only a small amount of memory and storage space. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate results of computation. Usually there will be no enough space to run complicated algorithms after loading the OS and application code. Unreliable communication is another serious threat to sensor security. Normally the packet-based routing of sensor networks is based on connectionless protocols and thus inherently unreliable.

Security is a very important issue when designing any network or protocol. The proposed schemes in literature are not secure, since they use some simplified techniques to carry out the limitations of sensors, given that the majority of these protocols makes use of symmetric encryption for ensuring all the security services instead of a combination of symmetric and asymmetric (public) encryption.

This paper proposes a highly secure, low cost and efficient protocol based on public key cryptography for external agent authentication and communication between external agent and base station is through public key cryptography and communication between base station and sensor is through shared private key techniques.

The rest of this paper is organized as follows: Section 2 discusses related work in this field. Section 3 discusses security requirements in WSN. Section 4 presents the proposed protocol. Section 5 analyses the proposed protocol and the security requirements met by it. Section 6 discusses the efficiency of the proposed protocol.

II . RELATED WORK

A.Public Key Based Schemes:
Simplified SSL handshake: In [5], the authors give the energy cost analysis of a simplified version SSL [8] applied to WSN, which reduces the amount of exchanged data between any pair of nodes to save

energy and bandwidth. The simplified handshake is used to setup a secure key between any two sensors in the network as the one in SSL [8]. As a brief analysis of this scheme, it seems that it is not an energy saving, since a handshake between each pair of sensors is too expensive concerning the amount of exchanged data. Therefore this scheme cannot be applied to mobile sensor networks, since the mobility of sensors needs new handshake at each time a sensor changes its position and therefore its neighbor sensors, which consumes lot of energy.

Simplified Kerberos protocol: The authors in [3] proposed an adapted version of Kerberos [9] for WSN in order to setup a session key between each communicating pair of sensors by contacting a trusted third party which may be the base station or a cluster head in a hierarchical network. They assume that a long term key is shared between each node and the trusted authority which is responsible for the generation of the secret key for each pair of sensors. This scheme is very vulnerable against capture attacks to which sensors are very often exposed and as the previous work the handshaking is not energy saving and it may consume lot of network resources if the trusted third party is far from the pair of nodes.

TinyPK: The TinyPK system described in [7] is designed specifically to allow authentication and key agreement between resource constrained sensors. The protocol is designed to be used in conjunction with other symmetric encryption based protocols as TinySec [6], in order to deliver secret key to that underlying protocol. To do this, they implement the Diffie Hellman key exchange algorithm. As said above, using a session key between each pair of sensors is not efficient and it consumes lot of energy and network bandwidth for the setup of the session key beyond of the energy consumed by the encryption algorithms. Using this scheme, as an end-to-end security mechanism may be energy efficient, however Diffie Hellman key agreement is very sensitive to man in the middle attacks, which can be easily performed in such situation.

III. SECURITY REQUIREMENTS IN WSN

The security services in a WSN should protect the information transmitted over the public channels and the resources from attacks and misbehavior of nodes. The most important security requirements are given below:

Data Confidentiality: Ensuring that only authorized external agents can access the content of the messages. Main part of data Confidentiality comes when a session key is shared between sensor and External agent. It must be sent in a secure way against traffic analysis attack. Data Authentication: Ensuring that the data is originated from the correct source i.e Base Station. The external agent should be authenticated from Base station in order to communicate with Senor nodes.

Data Integrity: Ensuring that any received data has not been altered in transmission by unauthorized parties. The received data by external agent from requested sensor nodes should be free from any alteration or corruption.

Availability: Ensuring that services offered by whole WSN or by a single sensor node must be available whenever required. Data requested by an external agent from Sensor node should be available whenever required.

Node Colluding: Colluding two or more nodes do not shape out other nodes.

On explaining our protocol, we analyze and prove that our protocol satisfies all the above mentioned requirements of security for WSN's.

IV. THE PROPOSED PROTOCOL

The proposed protocol is based on RSA cryptosystem [10].The entities in the proposed protocol are Certification Authority (CA), External Agent (EA), Base station, Wireless Sensor network which consists of sensor nodes.

CA: Certification Authority which is having private and public key pairs and trusted by sensors. The role of the CA in this process is to guarantee that the individual granted the unique certificate is in fact who he or she claims to be.

EA: External Agent is an entity who tries to communicate with the WSN. External agent also has a private and public key pair and must be certified by the CA.

Base station (BS): A Base Station is a signal transmitter or receiver that controls the local wireless network and may also be the gateway between external environment and WSN. Base station plays a major role in WSN security.

Sensor nodes: A sensor (also called as mote) which is a constituent of WSN is capable of sensing, gathering, processing and communicating information to BS or EA.

Algorithm: Communication between EA and BS is based on RSA based encryption and Decryption. Communication between Base station and Sensors is Secret key based encryption and decryption .Communication between Sensor and External Agent as discussed in Watro et al [7] by using low key cryptography.

The fig 1 shows the architecture of the proposed system:

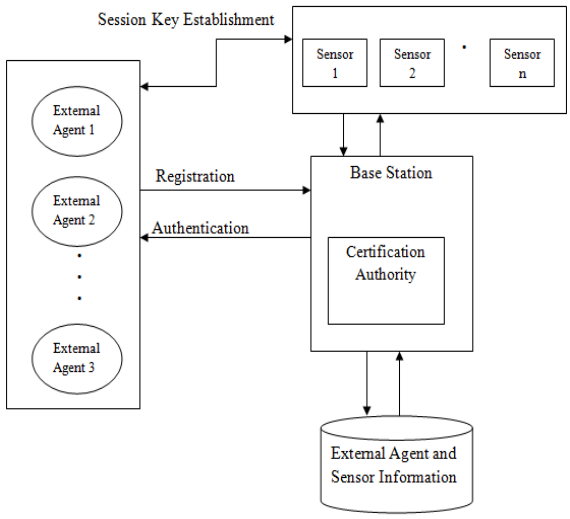

Fig 1 Architecture of the proposed system

The proposed protocol is explained in three important phases. Registration, Authentication, and Session Key establishment phase.

Registration phase: It is composed into 2 phases.

1.In first phase entities involved are External Agent and Base Station. The process involved is to register the External Agent public key with Base station.
R1) Any External Agent EAi wants to communicate with a sensor must be certified by a CA in which the WSN trusts.
R2) On certified by CA, EAi submits the public key EAPubKeyi to the base station.
R3) Base station validates the public key EA_{PubKey} submitted by the External Agent EAi, by checking whether it is certified by the CA in which the network trusts.
R4) Once certified the Base station stores the certified EA IP address, nonce in its database as a record for the external agent EAi
2.In second phase entities involved are Sensor and Base station. Each sensor in WSN registers with the Base station Base station maintains all registered sensors along with the information of the data each sensor holds.

Authentication Phase: This phase involves external agent authentication from Base station using public key cryptography.

TABLE 1: Notations of Proposed Protocol

Notation	Definition
C’	Ciphertext1
C’’	Ciphertext2
C’’’	Ciphertext3
E	Encrpt
D	Decrypt
N	nonce
chk	Checksum
h()	Hash function
REQ	Request from EA
t	Current time
T	Validity period issued by Certification authority

Algorithm1: External agent Authentication

If (t<T) then
//At external agent side
C’← $E_{EAPriKey}${REQ, N}
chk=h(N)
C’’←$E_{BSPubKey}${C’||chk}
//Send Ciphertext2 to Base Station
//At Base station side
$D_{BSPrivKey}${C’’}={C’||chk}
$D_{EAPubKey}${C’}={REQ,N}
//Verify for valid checksum
If (chk’==chk)
Valid checksum
else
Invalid checksum
Authentication failed.
End If
//verify for valid nonce
If(N’==N)
Valid nonce
else
Invalid nonce
Authentication failed
End If
C’’’=E_{bi}{REQ||EAPubKey||nonce}
//Send ciphertext3 to Sensor i.
//At Sensor side
D_{bi}{C’’’} = {REQ||EA_{PubKey}||nonce}.
else
//Certification validity period expired
Authentication failed
End If

A1)Certificate Authority sets specific certification validity period within which the External agent should communicate to Base Station for authentication.

A2) Any request from external agent i,e REQ to sensor i, along with nonce is encrypted with external agent private key called ciphertext1[1] C’=$E_{EAPriKey}${REQ, N}.

Encrypting the message with private key of EA, ensures that only EA could have sent it and provides Authentication of EA to the Base station. To check the integrity of Ciphertext1(C’), checksum (chk) of nonce is calculated as chk=h (nonce).The checksum

is calcuclated using MD5 Algorithm. Ciphertext1 and checksum of nonce is encrypted with the public key of base station i,e C"=$E_{BSPubKey}${C'||chk} which is called as Ciphertext2[1] . Encrypting the Ciphertext1 along with chk with the public key of base station ensures that only base station can decrypt it, thus providing secrecy of message. Then the message is transferred over an insecure public channel.

A3)Base station decrypts the message(Ciphertext2) with its own private key(BSPriKey), $D_{BSPriKey}${C''}.On decrypting Ciphertext2 the base station gets {C'||chk}.Base station decrypts the Ciphertext1 with the public key of External Agent(EAPubKey).Once it decrypts Ciphertext1,that is $D_{EAPubKey}$ {Ciphertext1} base station gets the REQ and nonce. Base station validates the nonce by calculating the hash of it using MD5 algorithm. If it is equal to chk, that is chk = h (nonce), then it proceeds to next step, else it rejects the request.

A4)The base station updates the nonce in its record for corresponding External agent, for every valid request from that External agent.

A5) On Authentication of External agent request, the base station instructs a sensor node (say i^{th} node) to respond against EAi's request. Base station stores a secret key with each sensor node of that WSN. Base station computes[1] Ciphertext3 C'''=E_{bi}{REQ||EAPubKey||nonce} and transfer the same to the i^{th} sensor node.

A6)On receiving ciphertext3, the Senor i^{th} node decrypts i.e. D_{bi}{C'''} = {REQ||EA_{PubKey}||nonce} .

Session Key Establishment phase: involves communication between External agent and Sensor.

Algorithm 2:

C''''=$E_{EAPubKey}${TinySessionKey}
$D_{EAPrivKey}${C''''}={TinySessionKey}
Use TinySessionKey for further communication

S1)In this phase sensor i frames a message i,e ciphertext 4 C''''=$E_{EAPubKey}${TinySessionkey}. As proposed in Watro [7], using of RSA algorithm to encrypt the message containing Session key with the public key of External agent assures only External agent can able to decrypt with its private key, which assures secrecy, which is an important factor while transmitting the session key. S2)On getting the Ciphertext4 the External agent decrypts the message with its private key and use the TinySessionKey for further communication.

S3)Sensor i sets a Session period within which External Agent can communicate with the sensor for data it require.

V. SECURITY ANALYSIS OF OUR PROPOSED PROTOCOL

In this section, we show that the proposed protocol provides security in all the conditions mentioned in the section 3.Each possible attack on wireless sensor network and the steps taken by the proposed algorithm is explained for each attack.

Traffic Analysis Attack : This is a special type of interference attack technique that looks at communication patterns between entities in a system. Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. If the entities lack in communication, denotes lack of activity between them.

Countermeasure by our proposed protocol:
From the start of communication from External agent to Base station and transferring of Session key to External agent are happening only once and in an encrypted format. Hence it doesn't give any clue to the adversary (No mathematical operations like XOR etc. or not performed on the contents of the message, if so the adversary can easily analyses the contents of the message).

Eaves Dropping and Passive Monitoring: The intercepting and reading of messages and information by unintended recipients. If the messages are not protected by cryptographic mechanisms, then definitely the adversary can capture the message.

Countermeasure by our proposed protocol:
Every message that is transmitted between External Agent and Base station, Base station and Sensor node, Sensor node and External Agent is in encrypted formats, hence no scope for Eaves dropping and passive monitoring.

Replay attack : is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution.

Countermeasure by our proposed protocol: nonce which is a non repeated value is used by base station as a distinguishing factor among requests from External Agent. In order to replay the valid request from External Agent, the adversary must know the nonce, which is not possible. The adversary must need private key of base station to decrypt Ciphertext2 to get nonce, which is not possible.

Impersonation Attack (Phishing): It is an attack in which is an adversary confuses by imitating as legitimate External agent or a base station. The

adversary has to capture the identity of an External agent to confuse a base station.

Countermeasure by our proposed protocol:
If an adversary can get the nonce of the message (through which a base station distinguishes the external entities) then it can confuse Base station. As the Ciphertext2 is in an encryption format and must be decrypted only by private key of base station, hence it's not possible for an adversary to impersonate External Agent. The entire message transferring between base station and sensor is done through a secret key, which is not possible for an adversary to get the secret key Node Compromise Attack: occurs when an attacker, though some subvert means gains control of the sensor node in the network after deployment. The adversary can simply extract information vital to network security such as security keys.

Countermeasure by our proposed protocol:
The base station will be continuously monitoring whether any node is captured or not. Every external Agent or user trying to connect to WSN ,the user authentication and data access must be done through Base station and after authentication. If a base station detects any node as compromised or malicious node, then the base station doesn't forward the message to that node.

Node Colluding Attack occurs when two nodes comes to an agreement to flood fraudulent messages in to the WSN.

Countermeasure by our proposed protocol:
The base station maintains a unique secret key for each sensor node in WSN. All the messages to a sensor node from a base station are encrypted through the secret key meant for that sensor node. Of course, this increases burden on the base station but to avoid colluding attack and the insider attack, it is the best possible solution.

VI. EFFICIENCY OF OUR PROPOSED PROTOCOL

To analyze the efficiency of our proposed protocol, it is compared with TinyPk [8] in terms of computation cost and communication cost. The comparison of Computation cost analysis is based on computation time for private key operation(T_{PK}), computation time for public key operation(T_{UK}), computation time for a hash key operation(T_H),computation time for a secret operation(T_{SK}).

TABLE 2: Computation Cost Analysis of Proposed Protocol

Protocol	External agent	Base station	Sensor node
Proposed	$T_{PK}+T_{UK}+T_H$	$T_{PK}+T_{UK}+T_H+T_{SK}$	$T_{SK}+T_{UK}$

Computation Cost Analysis: In the proposed protocol, the base station mainly performs two decryption activities provided with huge computational and energy resources . Base station doesn't have any burden on implementing these encryption and decryption activities. In TinyPk[7] a sensor with limited resources and energy is made to perform three RSA based encryption and decryption operations compared to only one in the proposed protocol.

Communication Cost Analysis: Both TinyPk[7] and our Proposed protocol consumes similar communication cost. As specified in [2], Communication is most costly than computation in WSN. In our proposed protocol we didn't increased the communication cost compared to Tiny PK. A sensor node in the WSN receives only one message from base station and transmits only one message to external agent. Once session key is established between External agent and the sensor node, the number of messages exchanged between those two is dependent on the application.

VII. CONCLUSION

In this paper, we have proposed a public key cryptography based protocol for user Authentication and Session key establishment between external agent and a sensor in a secure manner. In terms of computation and Communication costs, our proposed protocol is efficient in terms of sensor node computation and energy usage. Based on Author knowledge this is first of its kind protocol which is most secure low cost, user authentication and key establishment protocol.

REFERENCES

[1] Vorugunti Chandra Sekhar, Mrudula Sarvabhatla, "Security in wireless sensor networks using public key based techniques", International Conference on Computer Communication and Informatics (ICCCI -2012), Jan 2012

[2] Jaydep Sen, "A survey on Wireless Sensor network Security", Technical Report 55-77, International Journal of Coomunication Networks and Information Security (IJCNIS) Vol 1, No2 August 2009.

[3] G. Johann, S. Alexander, and T. Stefan, "The energy cost of cryptographic key establishment," Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, pp.380-382, 2007

[4] Th. Arampatzis, J. Lygeros, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks" Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, pp 719-724, 2005 .

[5] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S.C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks" ,Proceedings of PerCom, pp. 324-328, 2005.

[6] Karlof, N. Sastry, and D.Wagner, "Tinysec A linklayer security architecture for wireless sensor networks," Second

ACM Conference on Embedded Networked Sensor Systems (SensSys 2004), pp. 162-175,2004.

[7] Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: Securing sensor networks with public key technology", In Proceedings of the 2nd ACM Workshop on Security of Ad Hocand Sensor Networks (SASN'04), pp. 59-64, New York, USA,2004, ACM Pres

[8] B. Schneier, Cryptographie App.liqu'ee Algorithms, Protocoles, 2nd Edition, Wiley, 2001.

[9] J. T. Kohl, and B. C. Neuman, The Kerberos Network Authentication Service (Version 5), Internet Engineering Task Force (IETF), Internet Draft RFC 1510, 1993.

[10] R.LRivest,A.Shamir , and l.Adleman, "A method for obtaining digital signatures and public key crptosystems", Communications of the ACM , Vol.21,No.2,pp.120-126 1978.