Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.297 – 305

RESEARCH ARTICLE

SECURITY PROTOCOL FOR SENSOR NETWORK USING RSA

Sridevi, Assistant Professor, Department of Computer Science, KU, Dharwad

Abstract: As sensor networks may interact with sensitive data and operate in hostile unattended environments, it is imperative that security concern be addressed from the beginning of the system. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor networks. There has to be some comprise between the security and the energy. Many symmetric protocols have been implemented for sensor networks. The major problem in symmetric key security protocol is the key distribution problem. But asymmetric protocol like RSA has not been implemented due to high power constrain and for memory issue. In this research paper, RSA can be implemented for sensor in an efficient manner by using optimized computation. The problem of using power function for large encryption and decryption key for encryption and decryption method respectively has been optimized. This reduces the cost of computation for RSA and also designs a model to reduce the power consumption of the cluster head by decrypting the information message at the base station of the cluster node which uses the public key of its corresponding cluster node to encrypt the message.

Keywords: Base station, security, sensor networks, RSA

1. Introduction

Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety of real-world challenges. Their low cost provides a means to deploy large sensor arrays in a variety of conditions capable of performing both military and civilian tasks .Wireless sensor networks are large scale, usually slow moving or static wireless ad-hoc networks. Sensor networks are composed of up to thousands or millions of small nodes (motes) designed to sense environment and collect data. The motes are usually organized into clusters where each cluster is connected to a more powerful base station (BS). These networks have many practical applications which include military use, rescue operations, monitoring and tracking, etc. Security in such networks is a big challenge. In fact, the wireless nature of the links, the limited amount of energy that each mote has, its limited processing and storage resources and the absence of any physical protection render the motes very susceptible to multiple kinds of security attacks. The memory and the processing capability are much less than the today's computer. For example, Mica2 Motes consists of an 8 MHz 8-bit ATMEGA128L CPU with only 4 Kbytes of RAM space for data, 126 Kbytes of program memory, and 512Kbyte of flash memory. Traditionally; security is achieved through cryptographic methods which can be implemented either in hardware or in software. Hardware implementations are viewed to be more secure and more efficient because they are faster in general and they offer more intrinsic security. Symmetric key and public (asymmetric) key cryptography are the most widely used encryption methods in the area of communication. In symmetric key cryptography, the communicating parties exchange a secrete key that is used for both encryption and decryption of the message. But in asymmetric key cryptographic two different keys are used for encryption and decryption purpose. For encryption a public key (PK) is used to encrypt the message whereas for decryption the private key is used to decrypt the message. Therefore, there is no problem like key exchange problem, faced in symmetric key security protocol. Even public key i.e. asymmetric key cryptographic security protocol can be used as message authentication.

This research paper implements the well-known RSA security protocol for sensor networks security. The sensor network is very much vulnerable to different type of attacks, it is very important to give some security policy to the system. RSA is an asymmetric security protocol where two different key is use**d** to encrypt and decrypt the information message respectively. But RSA security protocol is not suitable for sensor network security as it is very power consuming. We have made some modification of RSA to use it for the sensor network security.

2. Problems and Limitations of Sensor Security

A wireless sensor network is a special kind of network which has many constraints compared to a traditional computer network. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints. Some problems and limitations of sensor security are outlined as below.

(i) **Limited Resources:** All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

(ii) **Limited Memory and Storage Space:** A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

(iii) **Power Limitation:** Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When implementing a cryptographic function or protocol within a sensor node, the energy impact of the added security code must be considered.

(iv) **Security goals:** This research paper focus on the following basic security goals:

- **Confidentiality:** Many application of sensor network, such as military monitoring, required secured sensor data so that they cannot be disclosed to the attackers. This is the main goal of our security protocol.
- **Integrity:** It guarantees that if an adversary modifies a data message from an authentic sender, the receiver should be able to detect that tempering.
- **Authenticity:** It ensures that the data messages come from an intended sender.

3. Implementation

The RSA security protocol modified in three ways. Firstly, design a model for secured data communication from cluster node to cluster head. Secondly modified the RSA algorithm to reduce the computation cost. And thirdly changed the packet format. In our scenario we have taken initial power, transmission and receiving range is same for the entire cluster node and the cluster head as well. When the sensor nodes are deployed, they make a cluster within their range. We have shown the scenario in Figure 1.

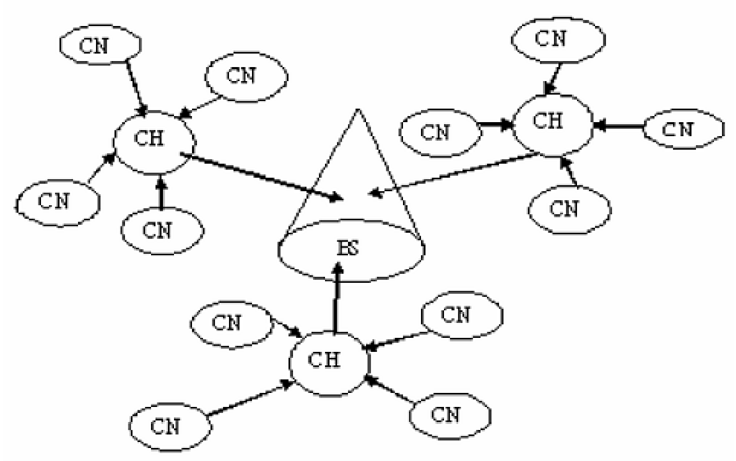


Figure 1: Cluster-Based Sensor Network

Each cluster has a cluster head and other node in the cluster is called cluster node. It is the duties of these cluster head to communicate with the base station of the network. In our scenario the base station broadcasts its public key in the network of its range. The entire cluster head stores the public key of the base station in its memory. Each cluster head generate two different large distinct prime numbers p and q. Then using these two values it generates a public key suite (e, n) and a private key suite (d, n). After generating the public and private key pair, cluster heads send their corresponding private key encrypted by the public key of the base station. The base station decrypts those messages sent by the cluster heads with its private key and gets the private key of all the cluster heads which want to communicate with it. Each cluster head broadcasts its public key to the cluster, it resides, periodically. After getting the public key of its cluster head, the cluster node stores it in its memory. It uses the public key for encrypting the message whenever it wants to send some information message to its cluster head. The corresponding cluster head after getting the information message do not decrypt it but just deliver it to the base station.

The base station decrypts the message by using its private key of the corresponding cluster head and gets the original message. In this way a secure communication between the base station and the cluster node is preserved. The cluster head does not encrypt or decrypt any information massage sent by its cluster node and hence save the energy for decryption of the information massage. As the cluster head deliver all the messages of its cluster node to the base station, it generally lost more energy than the cluster node. For this reason we model the network in such a fashion so that the cluster head does not engage in the message decryption or encryption process for information exchange between the cluster nodes (CN) and the base station (BS). Whenever cluster node generates a new private key suite and public key suite, it broadcasts the private key to the base station encrypted with the base station public key. Hence the cluster head (CH) engaged only key encryption process .At the same time it will broadcast its public key to its cluster node. As the number of key distribution is much less than the information exchange, less energy is consumed by the encryption process of the for the key distribution to the base station (BS) for the cluster head (CH).

All this steps have been shown in the figure1 below. Again for security purpose the base station re-generate the private and public key and broadcasts its public key encrypted by each public key of the cluster head. Hence only the cluster heads of the network access the public key of the base station and a secure communication between the base station and the cluster head preserved. The frequencies of broadcasting the public keys are different for base station and for the cluster head. As the base station has no energy and memory constrain problem, its broadcasting frequency of the public key is more than the cluster head's public key broadcasting. The communication model between the cluster node and the base station is depicted in figure 2.

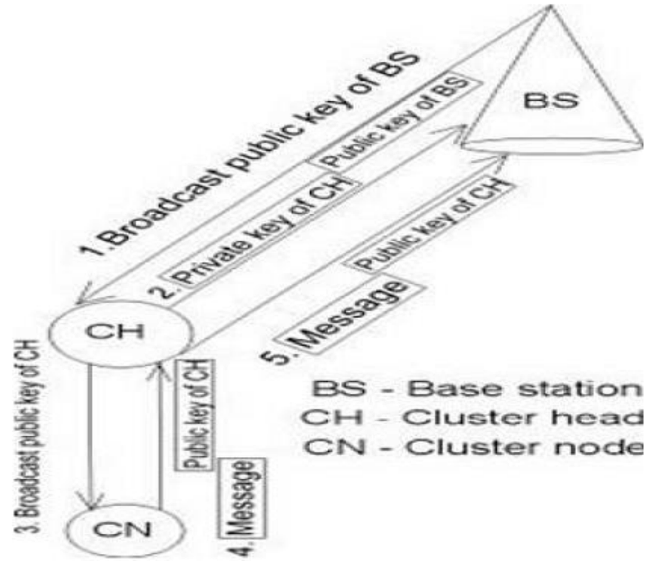


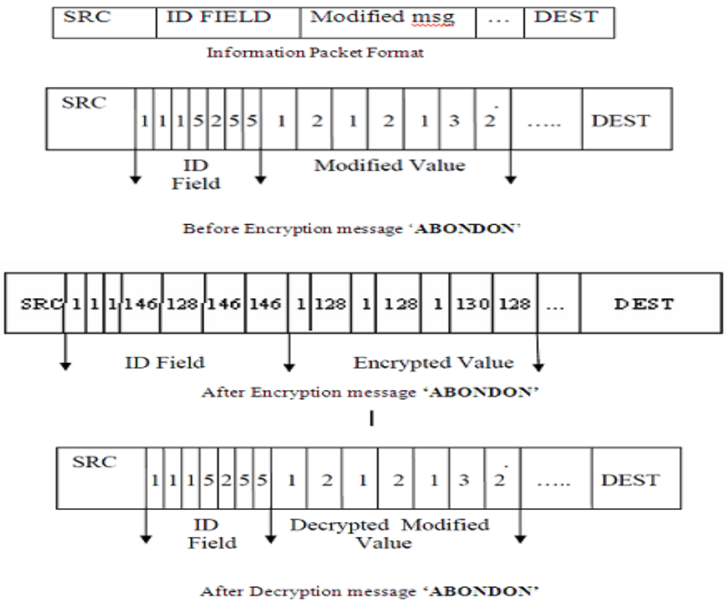
Figure 2: Communication Model from CN to BS

In our scenario the cluster node sends the information message encrypted with the public key (PK) of its cluster head (CH) and sends it to the base station (BS) through the cluster head by using RSA algorithm Energy and memory constrains are the vital part for the cluster node. The basic RSA algorithm is modified to make it applicable for sensor node. When cluster nodes want to send some information messages to its cluster head (CH), it changes the original ASCII value to a range between 1 and 3, comparing the ASCII value of the letter of the message. And thus we have to add a field called the identification field (msg->iden) in the data packet.

Let us consider that a message (msg) 'ABANDON' is to be sent by the cluster node to its cluster head. The field msg->Val contain the ASCII value of the letters of a message, msg. The cluster node compares the ASCII value of the letter 'A' and in the identification field it writes 1 and then the modified value becomes 1 as well. So, the large original value is changed to a modified value between ranges of 1 to 3. And to identify each symbol or character an additional field is added called identification field. In the example code we have shown this (64<msg^Val <67 THEN msg^Val=msg^Val-64 AND msg^iden=1). Similarly, 'a' will also have the same modified value as 'A' but the identification field is different. If 'b' has to be sent, same identification value will be used as 'a'. But the modified value of 'b' to be encrypted will be different, which is 2. Then the cluster node encrypted the modified value and the identification field with the public key of the cluster head of the cluster. The cluster node stores the encrypted value of the modified value when the public key is not changing for the cluster.

When the cluster node finds the same modified value has to be encrypted using the same public key, it will d the previous encrypted value and thus save the cost of encryption computation. But if the public key has changed then it has to find the encrypted value for the modified value and the identification field value also. In the base station, decryption method of RSA is applied. The base station decrypts the encrypted modified value of the message and the encrypted identification field. Then base station finds the modified value and the identification field as sent by the cluster node. The base station gets the original ASCII value of the symbol or character, sent by the cluster node by checking the identification field value. (IF msg->iden==1 THEN msg->val =msg->val+64)

In this way the base station gets the original message sent by the cluster node. As the frequency of public key broadcasting by the cluster head is much less than the frequency of sending information message by the cluster node, very less encryption process is applied for the cluster node. In the data packet we also add a field to preserve the integrity of it. The sender node adds all the modified value of the symbols or characters and encrypts the added value with the public key of the cluster head. When the base station gets the message, adds the modified values of the different characters or symbols and encrypts it with the public key of the cluster head. If the encrypted value is same as the value sent by the cluster node then integrity preserved otherwise the message is tempered. The algorithm given below is used for both the encryption and decryption process of a message. Suppose we choose p=11 and q=17. So n=187.



Information Packet Format

Before Encryption message '**ABONDON**'

After Encryption message '**ABONDON**'

After Decryption message '**ABONDON**'

Algorithms

In this section the algorithm for the implementation of the proposed security protocol is presented

```
Step 1. $i = 0$ and $p = 5$ and $k = (P_t)^5 \bmod n$     // $P_t$ is the modified value of the msg letters
Step 2. $AS[i] = k, B[i] = p$ and $k = (k * k) \bmod n$
Step 3. $P = p * 2$ and $i = i + 1$
Step 4. **Reapet** Steps 2 to 3 For key $> p$
Step 5. $l = 1, p = p/p2$ and $i = i - l, j = i$
Step 6. $l = \{l * A[i]\} \bmod n$ and key $=$ key $- p$
Step 7. If (key $> B[j]$) **THEN** key $=$ key $- B[j]$
Step 8. $l = (l * A[j]) \bmod n$ and $j - -$
Step 9. **Repeat** Steps 7 to 8 **IF** $j => 0$
Step 10. **IF** (key $< 5$) **THEN** compute $b \leftarrow (P_t)^k \bmod n$
Step 11. **Else** $b = 1$
Step 12. $C_t \leftarrow (l * b) \bmod n$;                    //$C_t$ is the Cipher text
```

4. Simulation Results

a) Fixed Cluster Head within the Network

In our scenario we take twelve bunch of messages sent as a round, sending from the four cluster nodes to the cluster head i.e. in each round three messages are sent by each cluster node(CN) to its cluster head(CH). We have assumed as the cluster node as fixed node and it is not changing for that cluster. We have consider the energy round graph for four different cases in CH and CN: (1).With no security. (2) Security with one public key (PK) of CH and BS for three messages from each CN. (3) Security with two public key of CH and one public key of BS for three messages from each CN. (4) Security with three public key of CH and three public key of BS for three messages from each

CN. The comparative result of energy round graph for CH and CN is shown in figure 3 and figure 4 respectively. The parameters for the simulation are as given in table 1.

Table 1 Sensor Network energy consumption Parameter

Total packet size	36 bytes
Processing power of sensor nodes	5nJ / bit
Transmission power	50nJ / bit
Receiving power	50nJ /bit
Initial Energy	5J
Encryption and Decryption energy consumed	6.22nJ /bit

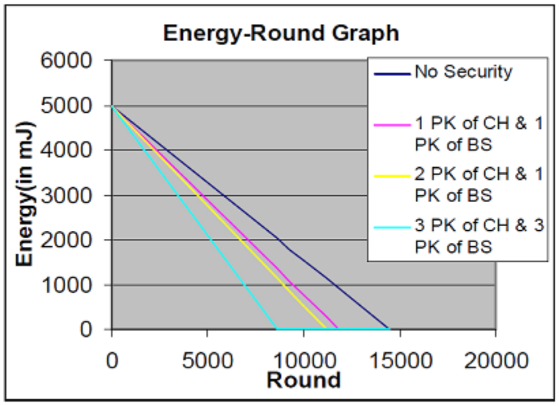


Figure 3: Energy-Round graph of Fixed Cluster Head (CH)

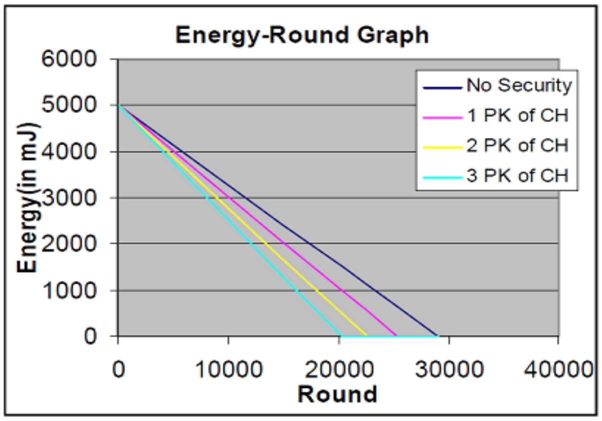


Figure 4: Energy-Round graph of Fixed Cluster Node (CN)

When there is no security CH can go to 14492 rounds. When one common public key of the CH is used to encrypt three messages of CN and one common public key is used to encrypt the private packet of CH, the CH goes to 11820 rounds. When two public key is used it goes to 11185 rounds. In last two cases the BS uses one public key to encrypt the private key of CH. The above graph shows that using 3 public key of CH and 3 public key of BS gives the highest security for any kind of network because CN encrypt each of its messages by different public keys of the CH and the CH sends each of its private key encrypted by different public keys of the BS. 1 PK of CH and 1 PK of BS give enough security to any kind of network. However, if the system wants less security then this can be achieved by increasing the number of messages in the round and this will enlarge the lifetime of the CH and CN as well. Less public key broadcasting of the BS will also enlarge the lifetime of the CH. Similarly, in Figure3 we have shown different cases for the cluster node. So, the overhead for RSA security for the cluster node is 18.4 %, 22.8%.

b) Changing the Cluster Head within the Network:

Till now the result we have got is about the fixed cluster head and cluster node in a cluster. Our aim is not only to consider the result of a fixed cluster head and cluster node in a cluster but also analyzing the lifetime of the cluster. We have studied two different cases regarding the system lifetime. The first one is the dynamic cluster head (CH) with threshold value set at the complete energy stored in that cluster head. When the cluster head dies another cluster node (CN) becomes the cluster head (CH) for that cluster according to the cluster head selection process. The second one is the dynamic cluster head with threshold value set at the energy half of the remaining value in it. When the threshold value is crossed the cluster head becomes an ordinary cluster node in that cluster. Then a cluster node of that cluster becomes the cluster head of that cluster.

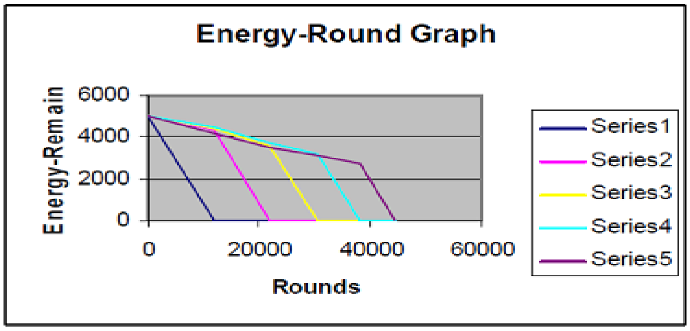


Figure 5 Energy-Round Graph of Dynamic Cluster Head With Threshold of its Total Energy

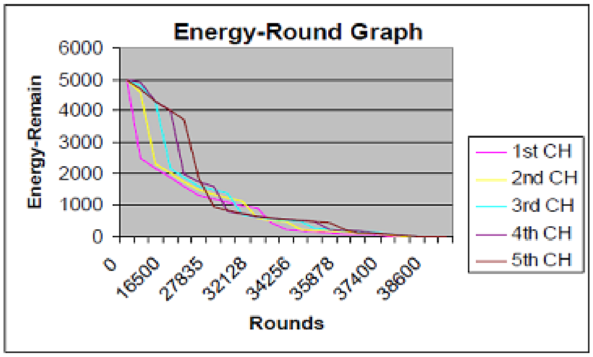


Figure 6: Energy-Round Graph for Dynamic Cluster Head with Threshold of Half Remaining Energy

In Figure 5, we can see that 1st cluster head (CH) dies after 11820 rounds. Then another node becomes the cluster head (CH). 2nd cluster head dies after 21961 rounds. 3rd, 4th, 5th cluster head (CH) dies after 30662, 38127, 44531 rounds respectively. So, the total cluster system dies after 44531 rounds. But the dieing of cluster heads took place sequentially i.e. one after another. Hence the network coverage of the system reduces with the dieing the cluster heads. So, the efficiency of the fixed cluster head based network reduces with the progression of the rounds. In Figure .6, we can see that the all the nodes of the cluster dies after the same number of rounds. The 1st, 2nd, 3rd, 4th, 5th cluster head (CH) dies after 37400, 38000, 38500, 38600, 38700 rounds respectively. So, dynamic cluster head system's network coverage and efficiency is far better than the fixed cluster head based system.

5. Conclusion

Through extensive simulations it is observed that in the proposed model the energy consumption using RSA security protocol is quite optimistic. We analyzed the energy consumed for security for both an individual cluster node and the whole cluster. Observed that dynamic cluster head based cluster's network coverage is quite high than the fixed cluster head based network. However in this model the Cluster head gets overloaded for very high security of the network which needs further study.

References

[1] D. Boyle, T. Newe, “Security Protocols for use with Wireless Sensor Networks: A Survey of Security Architectures”, Proceedings of the Third InternationalConference on Wireless and Mobile Communications, 2007

[2] Madden, S., et al., TAG: A Tiny AGgregation Service for Ad-Hoc Sensor Networks. 2002: OSDI.

[3] R.A Sheikh, Sung young Lee, Mohammad A. U. Khan, and Young Jae Song, “LSec: Lightweight Secure Protocol for Distributed Wireless Sensor Network”, IFIP International Federation for Information Processing 2006

[4] R.L. Rivest, A. Shamir, L.M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems’’, Communications of the ACM 21 (2) (1978) 120–126

[5] Oppermann et al., “UWB wireless sensor networks: UWEN-a practical example,” IEEE Comm. Mag., vol. 42, pp. 527–532, December 2004