International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Designing a Model for Energy Efficient and Secured Data Communication Using RSA Algorithm in Wireless Sensor Networks

Sangeeta Patil[1], Padmapriya Patil[2]

[1]M. Tech, Department of Electronics and communication engineering,
Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

[2]Associate Professor, Department of Electronics and Communication Engineering,
Poojya Doddappa Appa College of engineering,
Gulbarga, Karnataka, India

Abstract*: Sensor network is used in various military applications which demand protection against eavesdropping. Therefore some sensor networks need secured data communication from sources to base stations. As sensor networks adopts multihop routing from sources to the base station, and that there are no central authority in between, securing such a network is challenging. In this work we first propose a clustering based technique for routing. Clusters are dynamically formed before every round of transmission. Every cluster has a cluster head which can manage the keys locally. as every cluster has independent time schedule, public key cryptography with symmetric keys is essential. Therefore we use RSA algorithm along with RSA based system for a secured sensor network.*

Keywords*:* wireless sensor network (WSN), Symmetric key, Asymmetric Key, RSA, Energy efficient

1. Introduction

Wireless sensor network consists of large number of battery powered sensor nodes and one or more base stations. Sensor nodes have limited memory and processing power. Sensor nodes sense the data and transmit it through the network to its Base station. User can get the data from the sensor nodes through the internet from the Base station. Such WSN are used in environmental monitoring, military applications such as battlefield surveillance, rescue operations, monitoring and tracking, etc. Now a day's such networks are used in many industrial and consumer applications, such as machine health monitoring, industrial process monitoring and control and so on.

Wireless sensor networks are deploying 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 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). Security in such networks is a big challenge. Symmetric key and public (asymmetric) key cryptography are the most widely used encryption methods in the area of communication. RSA security protocol stands for the Rivest, Shamir and Adleman who are the creator of the RSA. RSA is an asymmetric-key security protocol as it uses two different keys for its encryption and decryption purpose. It is the most popular and proven asymmetric key cryptography algorithm. It generates two key private key and public key. Private Key is secreting to the user and public key is known to other who wants to communicate with the user. For this reason it is also known as public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography.

RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. In symmetric key protocol there is key exchange problem because here communicating parties exchange a secrete key that is used for both encryption and decryption. But in RSA there is no key-exchange problem. It also provides digital signature and message integration. From this respect RSA is better than asymmetric protocol. But for sensor network security purpose it is not suitable as it is very power consuming security protocol. For this purpose a clustering based technique for routing is used in this work.

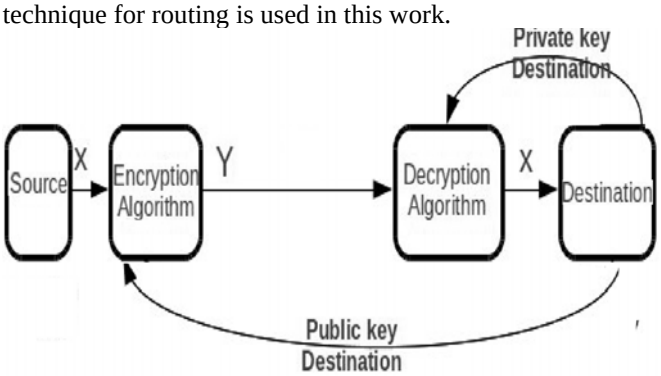

Figure 1: Security Block Diagram

In sensor network, for security the sources send plaintext message or data that is fed into the algorithm as input to intermediate nodes. Nodes encrypt the plaintext message by using destination public key; the encrypted message is called ciphertext. Decrypt the ciphertext message by using destination private key. Decrypted message is plaintext message; this plaintext message is send to the destination.

2. Literature Survey

In [1] proposed main methods used in attacks against the RSA cryptosystem, those are Pollard's p – 1 Method, Pollard's rho Method, Elliptic Curve Method, Quadratic Sieve and Number Field Sieve Methods. In fact, the existence of side-channel attacks shows that extensive study of the mathematical structure of the RSA algorithm is not enough.The greatest threats to the security of the RSA cryptosystem are flawed implementations. Against timing attacks they add a delay between the runtime and the private exponent so that every modular operation takes the same fixed time and the RSA cryptosystem is the de facto standard for public-key encryption and signature worldwide. It is implemented in the most popular security products and protocols in use today, and can be seen as one of the basis for secure communication in the Internet.

In [2] proposed main aspects of wireless sensor network security into four major categories: the obstacles to sensor network security, the requirements of a secure wireless sensor network, attacks, and defensive measures. The organization then follows this classification. They provide both a general overview of the rather broad area of wireless sensor network security.

In [3] proposed time and power consumption of public key cryptography algorithm for signature and key management by simulation. Cryptographic algorithm for authentication and encryption can be implemented in two ways: using public keys or private keys. Here Sensor nodes must be reconfigured, calibrated, and reprogrammed. Such operations are very sensible to possible attacks. Finally, it must be mentioned that they ignore the problem of key management.

In [4] proposed several schemes to secure communications in WSNs.These schemes are classified into three classifications based on the cryptographic techniques: symmetric keys, asymmetric keys and one-way hashing functions. There are different classifications based on the application scenarios, including: deployment, organization, re-keying, cryptography and authentication and are also described critical success factors of wireless sensor networks, those are soft message encryption, multiple communication paths, efficient data aggregation, malicious node detection, node revocation-awareness. In [5] proposed Current state-of-the-art protocols and algorithms for securing internet communication. By using a security protocols will make the sensor network a more attractive option.

3. Problem Statement

Major problems and limitations of sensor security are Limited Resources, Limited Memory, Storage Space and Power Limitations. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Asymmetric protocol like RSA has not been implemented due to high power constrain and for memory issue. Existing secured sensor network adopts pair-based encryption which results in very high energy consumption.

4. Methodology

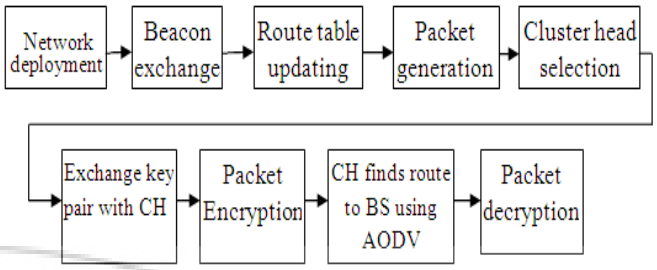

Figure 2: Methodology

In wireless sensor network security is big challenge, for security purpose we use RSA algorithm. Here we deploy the network with number of nodes. To find the neighbor nodes the source node send beckon (hello) message to each node. The major drawback is source node encrypts the data, encrypted data is send to the next node and next node decrypts it. Like this every node encrypt the data and decrypt the data, then a lot of energy was wasted. For this purpose we use clustering based technique for routing, here cluster head selection is done. The CH is selected based on the energy and which has maximum number of neighbor nodes. Once the CH is selected the other nodes join to it and providing cluster ID to each CH to generate a public and private key.

The source node send a data to CH, node first check whether there is CH present or not .If it is present node send a data to CH, if CH not found then it initialize the process. the source node send RREQ through the CH to base station (BS).The BS send RREP to source node, It will available in routing table. if it is available in routing table forward the packet directly, otherwise it has to find the route to BS. After this source node send the packet, if there is no BS then it stores the packet in the buffer by calling method bufferize.

Find route from source to BS, then it exchange key pair with CH, here encrypt the data by using public key and decrypt the data by using private key.

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. 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

5. Key Distribution

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. 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 message sent by its cluster node and hence save the energy for decryption of the information message.

5.1 Encryption

Encryption is done using the public key component e and the modulus n. To whomever we need to send the message, we encrypt the message with their public key (e,n). Encryption is done by taking an exponentiation of the message m with the public key e and then taking a modulus of it. The following steps are done in encryption.

1. Obtain the recipient's public key (n,e)
2. Represent the plaintext message as a positive integer m < n
3. Compute the ciphertext $c = m^{\wedge e} \bmod n$.
4. Send the ciphertext c to the recipient.

5.2 Decryption

Decryption is done using the Private key. The person who is receiving the encrypted message uses his own private key to decrypt the message. Decryption is similar to the encryption except that the keys used are different.

1. Recipient uses his private key (n,d) to compute $m = c^{\wedge d} \bmod n$.
2. Extract the plaintext from the integer representative m.

6. RSA algorithm

Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}

Encryption	
Plaintext:	M < n
Ciphertext:	$C = M^e \pmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

6.1 Network deployment

Here, deployed a network with BS and many nodes & taken source nodes. Sensor node sending route request to BS and BS receiving the route request, it sends route reply to the source node. The source node receiving the route reply, it sends ACK to the BS.

6.2 Cluster head selection

For cluster head selection, used LEACH (Low energy adaptive clustering hierarchy) protocol. Its aim is to reduce energy consumption within the WSN and prolong the lifetime of the network. For Routing using flooding or selective broadcast protocol and AODV protocol. The AODV (Ad-hoc on-demand Distance vector) protocol is reactive protocol, route will be established based on the user request and provides direct communication between CH to BS. The selective broadcast protocol is used to provide direct communication from source node to CH and it is intended to limit the number of packet transmission by means of selecting neighbour nodes acting as intermediate node.

7. Simulation Results and Analysis

We simulate secure data communication from source node to base station using RSA algorithm using Gossiping in OMNET++ 3.3pl. For the experiment, the random networks of different number of Nodes are varied as an input is used in an area of (500 x 500). Simulation time is set to 1000sec. And packet size of 512 byte long.

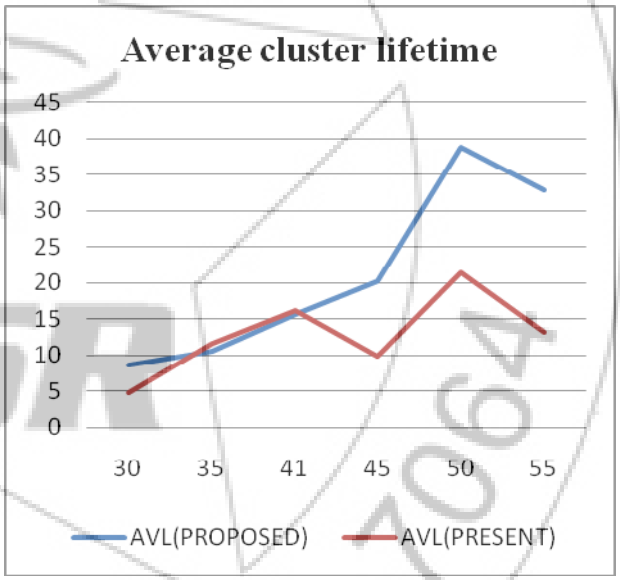

Figure 3: Nodes V/S Average cluster lifetime

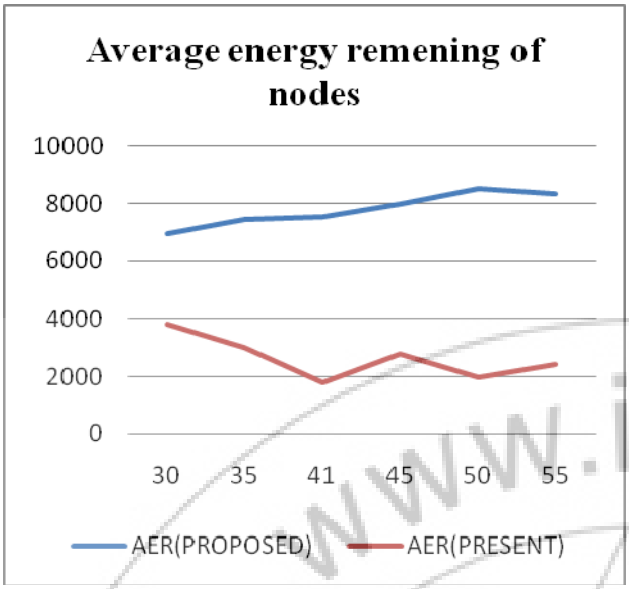

Figure 4: Nodes V/S Energy Remained In the Network

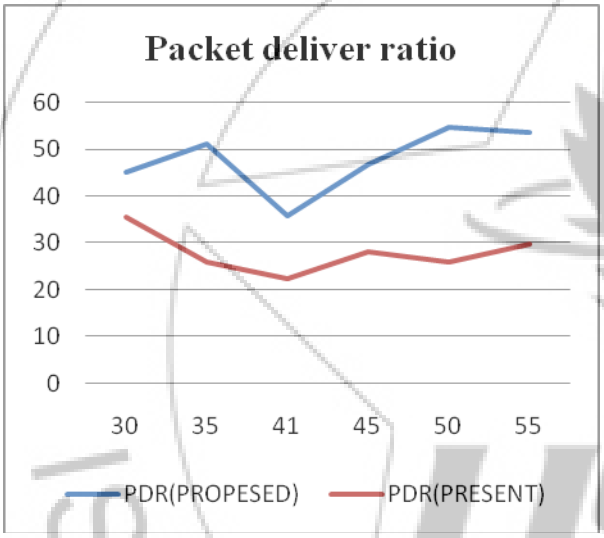

Figure 5: Nodes V/S Packet Delivery Ratio

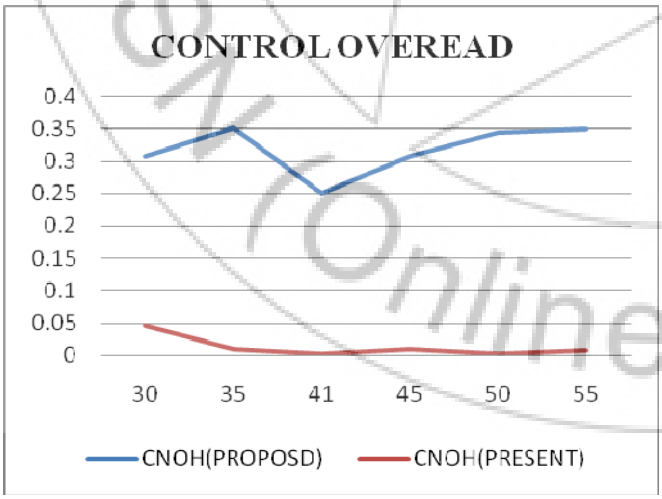

Figure 6: Nodes V/S Control Overhead

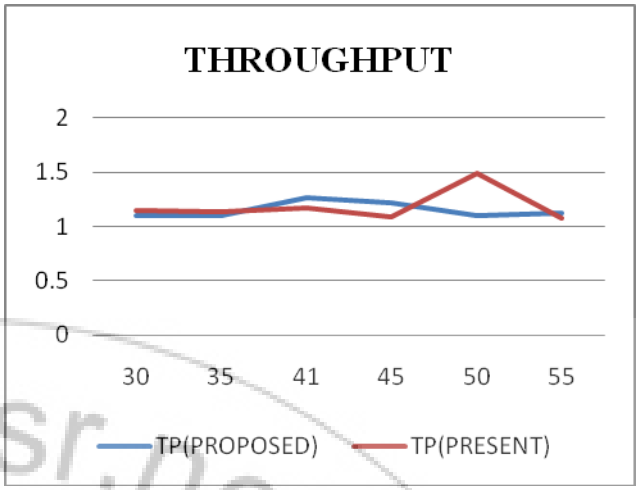

Figure 7: Nodes V/S Throughput

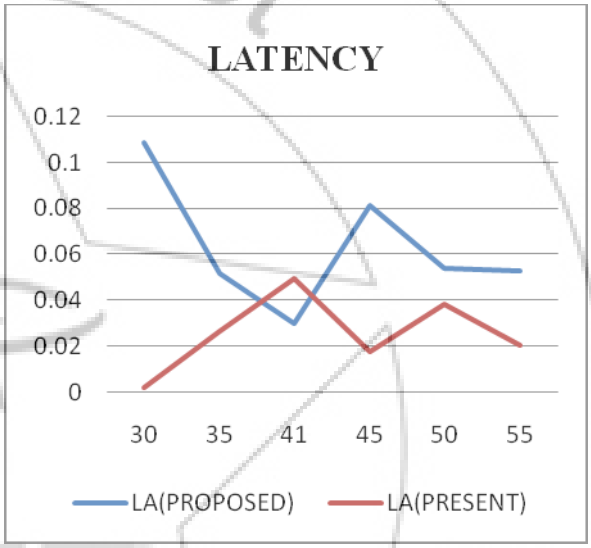

Figure 8: Nodes V/S Latency

8. Conclusion

In this paper, we have shown the implementation of RSA security protocol for sensor network. Through the OMNET platform based simulations, it is observed that in the proposed model the energy consumption using RSA security protocol is quite optimistic. Here we have increased the number of nodes and compare the parameters such as network lifetime of the cluster, average energy remaining of nodes, PDR, Throughput, Latency and control overhead of the present and proposed system through the graph. In this, network lifetime of the cluster, average energy remaining of nodes, PDR have been increased and Throughput, control overhead are decreased, because in present system technique used is routing non cluster and in proposed routing CH is used. By using routing CH we decreased number of encryption and decryption to reduce the energy consumption. Here by using RSA algorithm we send secured data communication from sources to base station.

9. Future Scope

With the help of RSA algorithm secure data transmission can be done in many applications which are used in WSNs. In

future we try to use enhanced protocol for CH selection which reduces delay and energy consumption in WSNs.

References

[1] John Paul Walters, Zhengqiang Liang, Weisong Shi, andVipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing 17:367-388, 2009.
[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: A survey, Computer Networks 38(4) (2002) 393–422.
[3] CrossbowTechnologyIncorporation.<http://www.xbow.com>.
[4] D. Boyle, T. Newe, "Security Protocols for use with Wireless Sensor Networks: A Survey of Security Architectures", Proceedings of the Third International Conference on Wireless and Mobile Communications, 2010.
[5] 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.
[6] D. W. Carman, P. S. Krus, and B. J. Matt. "Constraints and approaches for distributed sensor network security. Technical Report", 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, 2000.
[7] 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.
[8] 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*
[9] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38(4) (2002) 393–422.
[10] Stefan Katzenbeisser. Recent Advances in RSA Cryptography. Kluwer Academic Publishers, 2001.
[11] Madden, S., et al., TAG: A Tiny AGgregation Service for Ad-Hoc Sensor Networks. 2002: OSDI.