RESEARCH ARTICLE OPEN ACCESS

Analysis of RSA and ELGAMAL Algorithm for Wireless Sensor Network

Surekha J.*, Anita Madona M.**
*(*Computer Science, Auxilium College, and vellore*)
**(*Computer Science, Auxilium College, and vellore*)

----------**********----------

Abstract:

Wireless sensor network (WSN) is primarily designed for real-time collection and analysis of data in hostile environments. One of the major challenges of WSN is security. Network security is the most vital component in information security, because it is responsible for securing all information passed through the networks. The security of WSN poses challenges because of the criticality of the data sensed by a node and in turn the node meets severe constraints, such as minimal power, computational, and communicational capabilities. An identification of a suitable cryptographic algorithm for WSN is an important challenge due to the computational time, computation capability, and storage resources of the sensor nodes. Many symmetric algorithms have been implemented for sensor networks. In earlier studies, it is found that asymmetric algorithms, such as ELGAMAL and RSA, have not been implemented due to high-power constraint and for memory constraints. In this paper, it can be implemented for wireless sensor in an efficient manner using optimized computation. In this paper, the performance of the RSA cryptography algorithm is compared with the ELGAMAL algorithm by evaluating the cluster-based wireless network topology environment. The simulation results of both RSA and ELGAMAL show the comparative study using the NS2 simulation tool. The result shows that the RSA algorithm consumes a less computational time, data transmitting, and has a good storage capacity than the ELGAMAL.

Keywords— Asymmetric cryptography, ELGAMAL, RSA, security, wireless sensor network (WSN).

----------**********----------

I. INTRODUCTION

Wireless sensor network (WSN) is a continuously self-configuring network of sensor devices connected without wires. WSN consists of autonomous sensor nodes attached to one or more base stations [5]. A sensor network is composed of a lot of sensor nodes that are densely deployed either inside the phenomenon or very close to it. These sensor nodes in- turn consist of sending, data processing, and communication components. WSN depending on the environment where nodes are deployed, appropriate protection measures should be taken for data confidentiality, data integrity, and authentication between communicating entities, while considering the time, storage, computational, and communication efficiency requirements. To support such security services, one needs the key management techniques. Security in WSNs is a major challenge traditional security technique, and its algorithms. The required tradeoff makes it an important challenge to design the secure and an efficient cryptographic algorithm for WSNs [3]. An asymmetric encryption (also called public key cryptography) uses two-related keys (public and private) for data encryption and decryption, and takes away the security risk of key sharing. The private key is never exposed. A message that is encrypted using the public key can only be decrypted by applying the same algorithm and using the matching private key [1].

Likewise, a message that is encrypted using the private key can only be decrypted using the matching public key [1]. Public key cryptography was omitted from the use in the WSN because of its great consumption of energy and bandwidth, which

was very crucial in sensor network, as shown in Fig. 1.

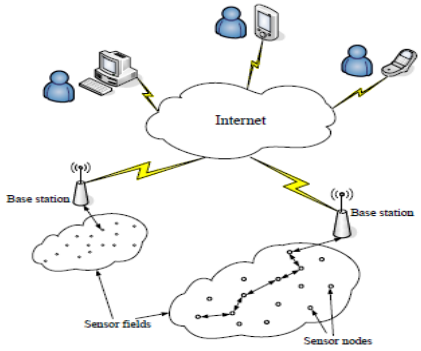


Fig. 1 Interconnection of WSN

Nowadays, sensor becomes a powerful in terms of CPU and memory power. Therefore, recently, there has been a change in the research community from the symmetric key cryptography to the public key cryptography.

I. PROBLEM STATEMENT

In general, all security algorithms are not giving the solutions to WSN. That cannot be implemented directly due to the limitations in WSNs. Security requirements of WSNs are similar to the conventional computer networks. Any security solution to sensor networks must preserve confidentiality integrity, availability, authentication, and non-repudiation within the network [2]. For a long time, it was supposed that the public key cryptography was not suitable for WSNs, since it require high-processing control, but later studies of asymmetric algorithm verified the possibility of those techniques in WSNs.

II. PROPOSED SOLUTION:

The asymmetric key (public key) cryptography uses two different keys for the purpose of encryption and decryption [11]. Public key cryptography eliminates the key distribution problem. Here, one of the two keys must be kept secret. It is impossible or at least impractical to decipher a message without knowing the private key. Therefore, information is more secured. It provides data confidentiality, data authentication, availability, and data integrity. RSA is one of the first practicable public key cryptosystems and is widely used for secure data transmission in WSN. Since the RSA algorithm is used for the number of computations among the existing public key cryptosystems. It will be a wise decision to implement RSA in the WSN for beneficial result of limited resource and the computational time for sensor network. The ELGAMAL encryption can be described by modulo exponential. More amount of computational is required for the generation of keys, encryption, and decryption of the information. For this reason, the strength per key is substantially greater in an algorithm of RSA and ELGAMAL. Hence, public key cryptography is suitable for WSNs.

III. RSA AND ELGAMAL ALGORITHM FOR WSN

A. RSA Algorithm

RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman are the developers of the RSA cryptosystem of MIT in 1997. It was described in 1978 [4]. Some of the famous security system, which is composed of three faces: 1) prime key generation, 2) encryption, and 3) decryption phase. An RSA is one of the first practicable public key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key, which is kept secret. In the RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

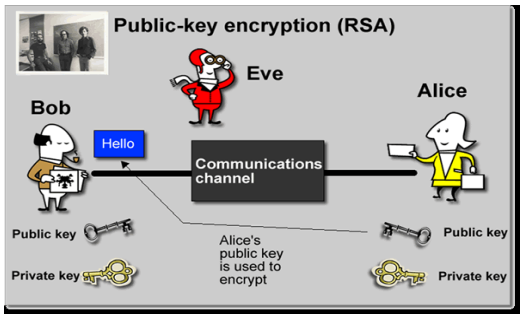


Fig. 2 RSA encryption

In this technique, we used RSA cryptosystem algorithm, in which included the private key and the public key. The public key is used only for encrypt the messages and it can be seen to all. It is not secret

key. The private key is used for decrypt the messages. The private key is also called the secret key. The RSA algorithm can distribute the encryption key openly, it is also very easy to update the encryption keys, and for the different communication objects, just keep the decryption keys secret [4], as shown in Fig. 2.

B. ELGAMAL Algorithm

It was developed in the year 1984 by Taher ELGAMAL. It is an asymmetric key algorithm and is based on D–H key exchange. The ELGAMAL encryption can be described over any cyclic group G. The security relies upon the issue of a problem in G related to computing discrete logarithms [9]. Fast generalized encryption for long messages and data expansion rate has the two biggest advantages of this algorithm. The main limitation of the ELGAMAL is the requirement for randomness and its slower speed [2].

The DSA is a variant of the ELGAMAL signature scheme, which should not be confused with the ELGAMAL encryption [12] (see Fig. 3). ELGAMAL algorithm consists of three components such as key generation, encryption and decryption algorithm [4].

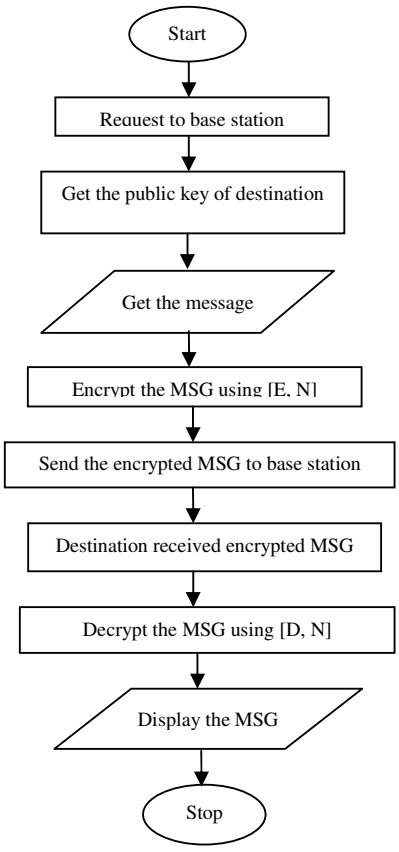
-El-Gamal PKC

Public Parameter Creation	
A trusted third party chooses and publishes a large prime p and a primitive root g modulo p.	
Key Creation	
Ali	**Salim**
1. Choose a private key $1 \le a \le p\text{-}1$. 2. Compute $A \equiv g^a \pmod p$. 3. Publish the public key A.	
Encryption	
	1. Choose plaintext m. 2. Choose random ephemeral key k. 3. Use Ali's public key A to compute: i. $c_1 \equiv g^k \pmod p$ ii. $c_2 \equiv mA^k \pmod p$ 4. Send ciphertext (c_1, c_2) to Ali.
Decryption	
Compute $(c_1^a)^{-1} c_2 \pmod p$. This quantity is equal to m.	

Fig. 3 ELGAMAL encryption

IV. WORKING OF RSA AND ELGAMAL ALGORITHM FOR WSN

Considering a continuous monitoring WSN, here, uses the RSA and ELGAMAL algorithms for security. Hence, public key and private key are generated in every node. In this paper, public key and private keys generated at all the nodes are assigned in a key table and put in a node which is called the base station. The base station also contains the routing table, having the exact location of all the other nodes. Based on the routing table, the base station assigns two other nodes, which are nearer to the base station as cluster heads. Finally, two other nodes are assigned as a source node and a destination node randomly with respect to each and every application [3]. The security of RSA is inherent with the difficulty of factoring large numbers. The RSA encryption and decryption algorithms require a single modular exponentiation operation.



The RSA ingredients are as follows:

- P,q, two prime numbers,
  (private , chosen),
- n =pq
  (public, calculated),
- e, with gcd (φ(n),e) =1; 1<e< φ(n)
  (public, calculated),
- d≡ e-1 mod φ(n)
  (private, chosen).

The private key consists of {d, n} and the public key consists of {e, n}. Suppose the user Bob from the destination wishes to send the message M to Alice, if only the user Alice in source has published its public key. Then, Bob calculates C = Me mod n and transmits C. On receipt of this cipher text, the user Alice decrypts by calculating M = Cd mod n [3].

A. ELGAMAL Algorithm

This public key cryptosystem requires a modular exponentiation operation. The size of the modulus determines the security strength of the cipher [3]. Key generation requires a large strong random prime number p to be chosen and their product computed. Select d to be a member of the group G= < Zp *, X > such that $1 \leq d \leq p-2$. Select e1 to be a primitive root in the group

G = < Zp *, X >. Then compute

e2 = e1d mod p

The public key is the {e1, e2, p} while {d} is the private key. To encrypt a secret m, it is represented as a binary integer less than n also to select the random integer r in the group

G = < Zp *, X >.

To decrypt the resulting cipher text c1, c2, it is raised to the power d modulo p.

c1 = e1 r mod p,

c2 = (m* e2r) mod,
{Encryption}

m = [c2 (c 1d)-1] mod p.
{Decryption}

V. WORKING AND SIMULATION SCENARIO

Here, we aim to model a scenario for WSN, which is suitable algorithm of RSA and ELGAMAL. We have modified the RSA security protocol in two ways. First, we have design a model for secured data communication from cluster node to cluster head. Second, we have modified the RSA to reduce the computation cost, as shown in Fig. 4.

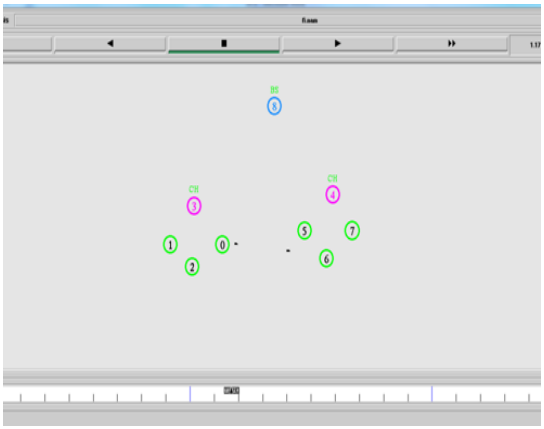
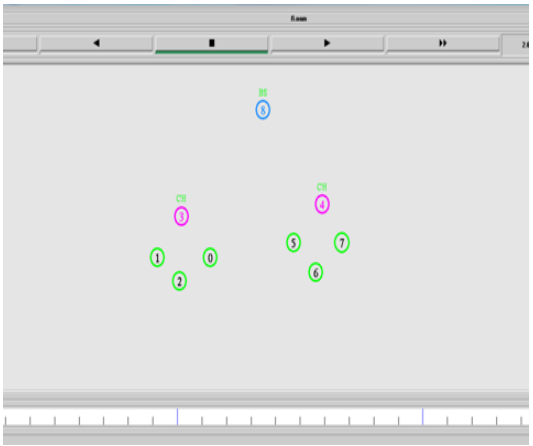


Fig. 4 Screenshot of network architecture design

Each cluster has a cluster head and other node in the cluster is called cluster node. It is the duties of the cluster head to communicate with the base station and



ther cluster nodes of the network (see Fig. 5).

Fig. 5 Secure communication

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 pairs, 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 head with its private key and gets the private key of all the cluster heads, which want to communicate with it.

VI. RESULT

A. *Performance Analysis*

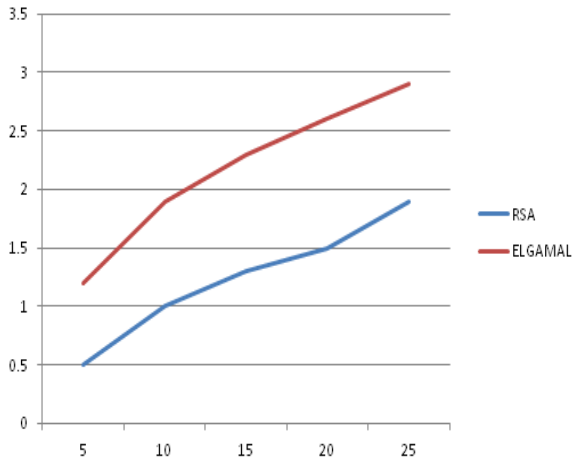


Fig. 6 The performance of RSA and ELGAMAL

The WSN is simulated using NS2, which consists of around ten sensors nodes, where five nodes act as sensors nodes, while other two nodes act as cluster heads, each one as a source node, and one as a base station[3]. These are randomly deployed in any hostile environment. For security purposes, we use the RSA algorithm; hence, a public key and a private key are generated in every node. These public key and private keys of all the nodes are assigned in a key table and put in a node, which is called the base station. While transmitting the data in the field of network, the amount of time taken in that environment, the algorithm of RSA takes less time to transmit data from one node to another, whereas ELGAMAL takes two times longer process than the RSA, as shown in Figs. 6–9.

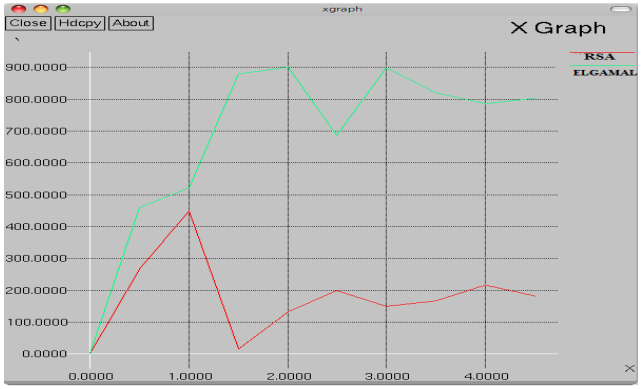


Fig. 7 Memory Usage of RSA and ELGAMAL

We can see that memory usage of RSA and ELGAMAL algorithm storage capacity that has been used (see Fig. 7). RSA takes low memory usage and storage capacity. But ELGAMAL takes more memory usage to compare RSA. Therefore, RSA is better than ELGAMAL during the transmission data and time comparison of these algorithms.

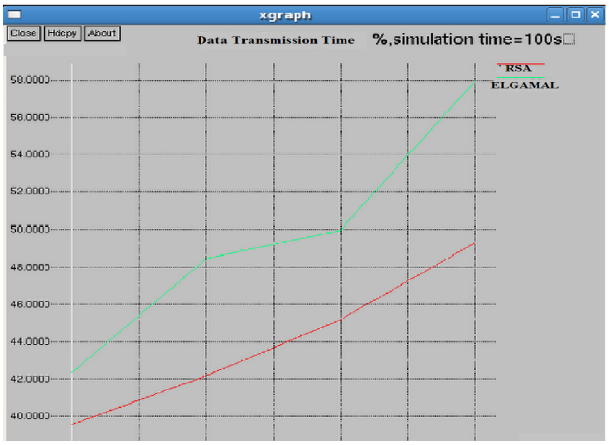


Fig. 8 Transmission time of RSA and ELGAMAL

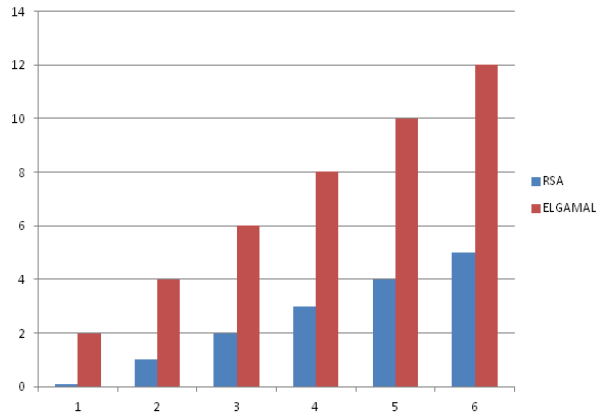


Fig. 9 Overall comparisons of RSA and ELGAMAL

VII. CONCLUSION

RSA and ELGAMAL algorithms perform the key distribution as well as encryption/decryption process. The RSA has to generate different keys for encryption and decryption process. The RSA algorithm does not allow the inverse modular exponentiation. Hence, an intruder cannot find the sensed information without knowing the private key even if he knows the public key. This is the main advantage of RSA algorithm, and also there is no (n−1) key distribution problem found in the symmetric key algorithms. From the observation, RSA algorithm provides better security for WSNs, and it consumes 14.5% less computational time and communicational capability than the ELGAMAL algorithm. Therefore, RSA is adoptable for the WSNs as it consumes less amount of time. RSA increases the network security, and also the algorithm is suitable for WSN when compared with the ELGAMAL algorithm. In the future, this analysis can be implemented in better simulators to get better results.

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their valuable comments, which greatly improved the readability of this paper. J. Surekha would also like to thank Ms. M. Anita Madona, Assistant Professor, Department of Computer Science, who guided for my work, and also express my whole hearted thanks to my parents and friends for their encouragements to bring this work to a successful completion.

REFERENCES

[1] Madhumita Panda, “Security in Wireless Sensor Networks using Cryptographic Techniques”, American Journal of Engineering Research (AJER). 2014.

[2] Annapoorna Shetty, “A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm”, International Journal of Innovative Research in Computer and Communication Engineering. October 2014.

[3] Kayalvizhi.R, “Energy Analysis of RSA and ELGAMAL Algorithms for wireless Sensor Networks”, proceedings of the 8th WSEAS international conference on applied electromagnetic, wireless and optical communications, 2011.

[4] Ankush Sharma, “Implementation & Analysis of RSA and ElGamal Algorithm”, Proceedings of the National Conference on ‘Advances in Basic & Applied Sciences, (ABAS-2014).

[5] Dona Maria Mani, “A Comparison between RSA and ECC In Wireless Sensor Networks”, International Journal of Engineering Research & Technology (IJERT), 2013.

[6] Mohd. Rizwan beg, “Energy Efficient PKI Secure Key Management Technique In Wireless Sensor Network Using DHA & ECC”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), February 2012.

[7] Sirwan A. Mohammed, "Design And Simulation Of Network Using Ns2", International Journal of Electronics, Communication & Instrumentation Engineering Research and Development, 2013.

[8] Narender Tyagi, "Comparative Analysis of Symmetric Key Encryption Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, 2014.

[9] Mini Malhotra, "Study of Various Cryptographic Algorithms", International Journal of Scientific Engineering and Research, 2013.

[10] Nayana Hegde, "Simulation of Wireless Sensor Network Security Model Using NS2", International Journal of Latest Trends in Engineering and Technology, 2014.

[11] Gaurav R. Patel, "A Comprehensive Study on Various Modifications in RSA Algorithm", International journal of engineering development and research, 2012.

[12] Kapil Madhur, "Modified ElGamal over RSA Digital Signature Algorithm (MERDSA)", International Journal of Advanced Research in Computer Science and Software Engineering, 2012.

[13] R.p. Modi, "Dynamic Cryptographic Techniques for Wireless Sensor Networks", International Conference on Machine Learning and Computing, 2011.

[14] Saurabh Singh, "Security for Wireless Sensor Network", International Journal on Computer Science and Engineering, 2011.

[15] Sumedha Kaushik, "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, 2012.