International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
2nd National Conference on Innovative Paradigms in Engineering & Technology (NCIPET 2013) – www.ijais.org

Literature Survey on Security Techniques and Authentication Protocols for Wireless Sensor Networks

Shifa S Sayyed
Department of Information technology
Priyadarshani Institute of technology, Nagpur, MH
India

S R Jain
Department of Information technology,
Priyadarshani Institute of technology,Nagpur, MH
India

ABSTRACT

Wireless sensor networks (WSNs) have gained attention Worldwide in recent years. Because of potential of physical isolation, these sensors have wide range of applications in land based security, military security and much more. As WSNs exchange there environmental conditions with each other, security become important aspect. In WSNs due to battery constraint problem, efficient secure and authentication algorithm is needed which take much lesser time to execution time. In this paper different authentication algorithms are introduced. Most of the literatures indicate that it is impossible to implement cryptographical algorithm because of its battery issue. Many symmetric and asymmetric algorithms have been implemented till yet with large keys. Some papers have provided different keys execution with time constraints.

Keywords

Security, cryptographic algorithm, GPS, Rabin public key cryptosystem, Android SDK, J Eclipse

1. INTRODUCTION

Wireless sensor network is a collection of nodes networked in a cooperative manner. This node has self processing capabilities. Sensor nodes may contain different types of memory. This sensors exchange environmental information with each other or to a base station. While exchanging information, tremendous security is needed if application depends on military sensing or surveillance. The energy of batteries has to be rationally used, to ensure a long time operation of sensors. By providing security to this type of sensors, cryptographically algorithm should take lesser execution time.

WSNs are vulnerable to various types of attacks or to node compromises that exploit known and unknown susceptibilities of protocols, software and hardware, and threaten the security, integrity, authenticity, and availability of data.

Many symmetric and asymmetric algorithms have been used yet to give secure communication to wireless sensor networks. Because of the large keys used by the algorithm, they take more execution time which effect battery of nodes. Rabin Cryptosystem is asymmetric authentication technique, whose security, like that of RSA, is related to the difficulty of factorization. For encryption, a square modulo n must be calculated. This is more efficient than RSA, which requires the calculation of at least a cube. For decryption, the Chinese remainder theorem is applied, along with two modular exponentiations. Here the efficiency is comparable to RSA [2].

The implementation of cryptographic systems presents several requirements and challenges, particularly for constrained environments (memory and area requirements). An important aspect is the power and energy consumption relating to public key algorithm. Ecliptic curve algorithm use large key and take more time to execute [3]. [4] This paper briefly reviews the delegation based authentication protocol of Lee and Yeh for PCSs, and describes its weakness. To increase the communicational efficiency, and save authentication time, their protocol employs off-line authentication processes; such that *VLR* does not need to contact *HLR* frequently, and can rapidly re-authenticate *MS*. The enhanced protocol employs a backward hash chain to provide authentication and non-repudiation in offline authentication processes. The analyses of the enhanced protocol are similar to those of the protocol of Lee and Yeh for user identity privacy, non - repudiation in on-line authentication processes, key management, computational costs and communicational loads.

2. SECURITY REQUIREMENT

WSN demands the following general security goals [2][3][4]:

1) *Security*: Protecting information from unauthorized access and protecting it from modification.

1) *Confidentiality*: It ensures that certain information is never get open to unauthorized entities.

2) *Integrity*: This ensures message has not been distorted by malicious nodes or by communication faults. It deals with the correctness of data.

3*) Authentication*: This authenticates the source of message.

4) *Availability*: It ensures desired service may be available whenever required.

3. BACKGROUND AND RELATED WORK

WSNs are vulnerable to various types of attacks or to node compromises that exploit known and unknown susceptibilities of protocols, software and hardware, and threaten the security, integrity, authenticity, and availability of data. The power source supply for wireless sensors networks has mainly been disposable, primary batteries. However, there are some challenges with using disposable batteries for wireless sensors - maintaining sensors in hard to service locations, and scaling a sensor network to thousands of nodes[1].

Various cryptographic solutions have been proposed till now based on symmetric and asymmetric algorithms. [2] Rabin asymmetric algorithm used for security, confidentiality, and authentication. This paper depends on Key generation using large prime numbers. Authentication is provided by Chinese remainder theorem. For encryption, a square modulo n must be calculated. This is more efficient than RSA, which requires the calculation of at least a cube. For decryption, the Chinese remainder theorem is applied, along with two modular exponentiations. [3][4] This paper examines the use of ECC in such constrained environments and discusses the basis of its security, explores its performance and lastly, surveys the use of ECC applications on the market today.

The ECC has the highest strength-per-bit compared to other public key cryptosystems. Small key sizes translate into savings in bandwidth, memory and processing power. This makes ECC the obvious choice in this situation. This paper deals with discrete logarithmic Algorithm, Factorizing algorithm and RSA challenge.

In this paper they proposed only one Web programming language script to be with four Web browsers in order to determine which type of algorithm is suitable to which type of Web browser in terms of their performance and compatibility. Active Server Pages (ASP) has been selected and five different types of encryption algorithms have been chosen to be analyzed to observe their performance. The simplest method of encryption is by considering a text contain in a single line of text [5].

This paper highlights that the existing authentication protocols, based on RSA asymmetric cryptography, are not appropriate for such devices due to their limitations in computing power, memory capacity, key sizes and cryptographic support. Therefore, an efficient protocol for resource constrained platforms that achieve a level of security similar to the one achieved by the protocols in use today is designed and implemented. This protocol is based solely on Hyperelliptic curve asymmetric cryptography and the results prove that the performance achieved is good compared to RSA [6].

4. SURVEY ON SECURITY TECHNIQUES

A. Elliptic curve Algorithm

Step 1: Consider an elliptic curve (E) with appoint P.

Step 2: Now, generate a random number d.

Step 3: Q=d*P

This is called as elliptic curve discrete logarithmic problem. As long as the curve is big enough, it is almost impossible to find d. Above problem make this algorithm to take much time to execute for battery dependant wireless sensor nodes.

B. RSA Algorithm

Step 1: Choose large prime numbers P & Q.

Step 2 : Calculate N=P*Q

Step 3: Select the public key E such that it is not a factor of (P-1) and (Q-1).

Step 4: Select the public key D such that the following equation is true

(D*E) mod (P-1)*(Q-1) = 1

Step 5: For Encryption CT=PT^{E} mod N

Step 6: For Decryption PT=CT^{D} mod N

The RSA Algorithm is based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. Because of the large prime number as a key for encryption, this algorithm take more time to execute but less time than ECC.

C. Rabin Authentication Algorithm

Key Generation Phase:

The system S creates a Key pair, by the following steps

Step 1: Choose two large distinct primes p and q. One may choose p=q=3(mod 4) to simplify the computation of square roots modulo p and q.

Step 2: Compute n=pq

Step 3: S’s public key is n and S’s private key is (p, q)

Encryption Phase:

The system S creates cipher text by the following steps

Step 1: Receives the key pair from key generation phase.

Step 2: Calculate cipher text C= m2 mod n.

Step 3: Generated cipher text sends to the remote system.

Authentication Phase:

Step 1: Receives the request C and checks the validity.

Step 2: with the help of Chinese remainder theorem, the four square roots ml, m2, m3 and m4 are calculated.

Step 3: Check the received C value for presence of anyone of ml, m2, m3 and m4. If the value of C is equal to any of the square root value, then accept the login request.

Step 4: Otherwise reject the request.

Step 5: The four square roots are in the set {O, n - I}):

Step 6: One of these square roots is the original plaintext.

Rabin is asymmetric algorithm, which means that it is hard at factorization. Again as it is using large prime numbers as key, it takes much time to execute but lesser than ECC and RSA algorithm.

The table below shows the comparative analysis of cryptographic algorithm based on their key parameter used and performance over wireless sensing network.

Paper title	**Features**	**Algorithm**	**Limitations**
Ecliptic curve based	Public key, Work on finite fields.	Finds discrete logarithm of a random ecliptic curve element with respect to the publicly known base point.	Large key size, take more time, difficult to implement
RSA	Public key, based on exponential in a finite field over integer modulo a prime.	Encryption and decryption using Extended Euclidean algorithm	Large key size, more execution time
Rabin	Asymmetric key, Hard integer factorization, Authentication provided at receiving end.	Key generated by large prime numbers, authentication is provided by using Chinese remainder theorem.	More execution time

Fig: Comparison analysis between cryptographic algorithms

5. EXPERIMENTAL ARCHITECTURE

The authentication protocol must be able to generate a secure channel communication between two layers on top of an insecure network. Below arcitecture shows an experimental process done on Rabin authentication algorithm. In this, wireless sensor nodes first get located with the help of GPS or manual configuration. Tracked longnitude and latitude will be inputed to the Key generation phase. Recieving keys from key generation phase ,ciphertext text will be calculated using Rabin cryptographic algorithm. This cipher text will be trasmitted to remote stytem for Authenticity.

Accessing and checking the authentication of a user is important for any types of network-based applications. Recently, more number of schemes is proposed. Still high security is yet not achieved. In this paper we propose a new authentication scheme using improved Rabin public-key cryptosystem which is location based.

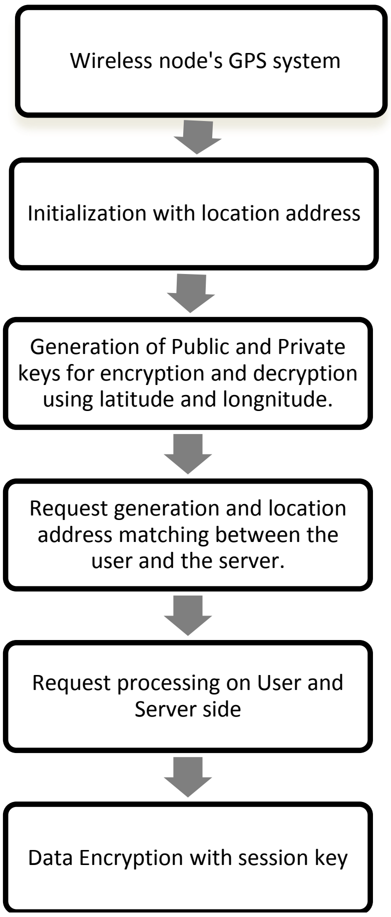

Wireless node's GPS system
Initialization with location address
Generation of Public and Private keys for encryption and decryption using latitude and longnitude.
Request generation and location address matching between the user and the server.
Request processing on User and Server side
Data Encryption with session key

Fig 1: **Process Arcitecture**

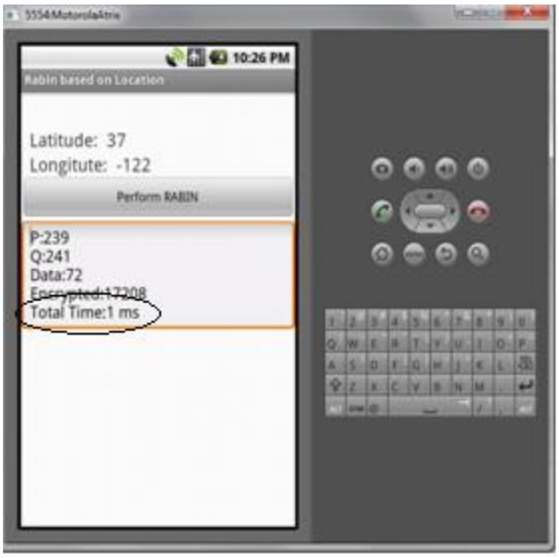
6. EXPERIMENTALS AND RESULTS

Objective of this experiment is to find the location based Public key Cryptosystem. The communication between the server and the user will take place by encrypting the Location address of the respected sensor node. Also to improve the performance analysis and the security of the Rabin Algorithm.

Comparative analysis in previous experiments shows that ECC (Ecliptic curve cryptography) and RSA take more time than Rabin algorithm. This paper mainly focused on improvement of Rabin execution time. Analysis from experiment shows that for encryption it is taking only 1ms to execute.

An Android Virtual Device (AVD) is an emulator configuration that lets you model an actual device by defining hardware and software options to be emulated by the Android Emulator. Fig 3 shows experimental analysis of encryption phase using Java Eclipse Android SDK.

Fig 3: Experimental analysis on AVD Manager.



Latitude: 37
Longitute: -122

P:239
Q:241
Data:72
Encrypted:17208
Total Time:1 ms

7. CONCLUSION

Sensor networks 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 network.

Experiments taken on location based Rabin cryptographic system shows that it may take much lesser time than any other existing algorithm. Finally, due to location based capability, security implementation become much easier.

8. REFERENCES

[1] Garcia-Hernandez, C. F., Ibarguengoytia-Gonzalez, P. H and Perez-DiaZo J. A 'Wireless Sensor Networks and Applications: A Survey', IJCSNS, 7(3),264-273 (2007)

[2] K .Saravana selvi T. "Rabin Public Key Cryptosystem for Mobile Authentication.". IEEE- (ICAESM -2012) March 30, 31, 2012.

[3] Dr. Lawrence Washington." Elliptic Curve Cryptography and Its Applications to Mobile Devices." Wendy Chou, University of Maryland, College Park. Department of Mathematics.

[4] Dr. R. Shanmugalakshmi ,"Research Issues on Elliptic Curve Cryptography and Its applications - IJCSNS, VOL.9 No.6, June 2009,

[5] S.Z.S. Idrus,S.A.Aljunid,S.M.Asi, "Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1.January 2008

[6] S. Prasanna Ganesan " An Asymmetric Authentication Protocol for Mobile Devices Using HyperElliptic Curve Cryptography." India. 2010 IEEE.

[7] Jian-zhu Lu and Jipeng Zhou" On the Security of an Efficient Mobile Authentication Scheme for Wireless Networks." 2010 IEEE.

[8] A Perrig, R Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," Wireless Networks, vol. 8, no. 5, pp. 521-534, 2002.