Nat.Volatiles&Essent.Oils,2021;8(4):6208-6213

Usage of Elliptic Curve Cryptography Technique for the Data Security and Privacy in the Wireless Sensor Network

[1]Srinivasachary Sirisinahal, [2]MV Ramana Murthy, [3]S China Ramu

[1]Research scholar in Computer Science, Osmania University Hyderabad
[2]Former Professor, Dept. of Mathematics Osmania University Hyderabad
[3]Professor, Dept. of CSE, CBIT, Gandipet, Hyderabad

Abstract

The protection of data from unauthorized access, use, introduction, intrusion, change, examination, recording, or destruction is known as data security. Wireless sensor networks (WSNs) are networks of sensors that are spatially dispersed and dedicated to monitoring and recording the physical conditions of the environment before transmitting the collected data to a central location. Security is currently regarded as one of the most critical issues in WSN development. The key issue in the effective execution of WSN is dealing with application security adequately. The purpose of this paper is to discuss the role of cryptography in WSN to improve data security. The goal here is to learn about another security strategy that uses cryptography to secure data in data centres.

Keywords: WSN, Secured data transmission, elliptic curve cryptography, encryption, decryption.

Introduction

Cryptography is the science of secret writing; the first documented use of cryptography occurred when an Egyptian scribe used non-standard hieroglyphs in an inscription. Cryptography has a wide range of applications, from diplomatic messages to wartime battle plans. With the use of computers and communications, new forms of untrusted medium have emerged, including virtually any network, particularly the Internet. Public key algorithms and private keys are the two main types of cryptography algorithms. The public key in cryptography is based on the intractable nature of certain mathematical problems. The first public key system is RSA, which is based on the assumption that it is difficult to put a whole number in mailmen with two large primordial mailmen.

The plain text message is written in simple English that anyone can understand. The message is encoded using cryptographic techniques known as cypher text message.

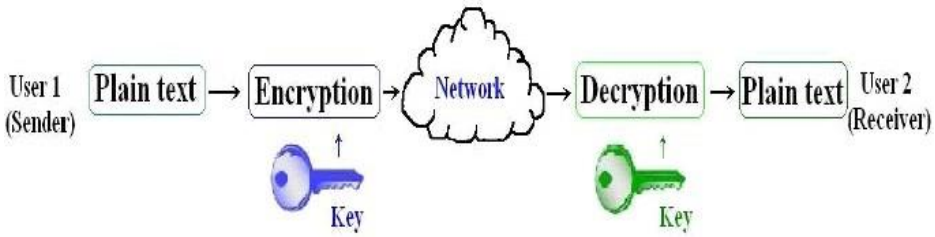

Fig. 1: Encryption and Decryption Mechanism

There are three type of techniques 1) Symmetric Key Cryptography 2) Asymmetric Key cryptography 3) Hash function.

Symmetric Key Cryptography

Symmetric encryption is the oldest and most well-known technique. A secret key, which can be a number, a word, or simply a string of random letters, is used to alter the content of a message in some way. This could be as simple as moving each letter up or down the alphabet a few positions. As long as both the sender and the recipient know the secret key, all messages using this key can be encrypted and decrypted.

Asymmetric Cryptography

The difficulty with secret keys is bartering them over the Internet or a huge network while keeping them out of the hands of the wrong people. Anyone with the secret key can decrypt the message. One solution is asymmetric encryption, which employs two related keys as a key pair. Anyone with access to your public key can send you a message. A second, private key is kept hidden so that it is only accessible to you. Any message (text, binary files, or documents) encrypted with the public key can only be decrypted with the same algorithm and the matching private key. Only the corresponding public key can decrypt a message encrypted with the private key. As a result, you won't have to concern about sending public keys over the Internet (the keys are supposed to be public). Asymmetric encryption has the disadvantage of being slower than symmetric encryption. Encrypting and decrypting the message's content requires significantly more processing power.

Hash Function Cryptography

Hashing is a function. Cryptography (one way cryptography) is a technique for generating fixed-size data blocks from variable-length entry data. Capturing the data's digital fingerprint is another term for it, and the exit data is known as message digest or one-way encryption. If the data is changed after the hash function is generated, the hash function's second value will be different. Even minor changes to the data, such as inserting a comma into a text, cause significant differences in the hash values. The hash values solve the message integrity problem.

Wireless Sensor Network

Wireless sensor networks (WSN) have become very popular and have even become a part of our daily lives as a result of the rapid advancement of wireless communications and embedded micro-electronic-system technologies. WSN design is typically application driven, which means that the network's behaviour is dictated by the needs of a specific application. However, because of their linear scalability, small software footprint, low hardware implementation cost, low bandwidth requirement, and high device performance, WSNs have gained increasing attention in recent years. It is worth noting that today's software applications, including WSNs, are primarily distinguished by their component-based structures, which are typically heterogeneous and distributed. In contrast, WSNs must typically self-configure and support ad hoc routing.

"It has limited processing capability, battery power and storage" [1]. "WSN is used in a wide range of application domains as to monitor physical or environmental conditions" [2] and industrial maintenance [3]. "Security and privacy issues of WSN pose a big challenge especially when it deployed in hostile environments and security-critical applications as health care and even military operations" [1]. "In order to provide a high level of security to these applications, ECC can be used in first step to establishment of shared secret keys between nodes and authentication in order to improve security services in WSN" [4].

Literature Review

"There are many works done for ensuring the security in cloud servers using different type of algorithms such as RSA, AES, DES and ECC". [5] "Elliptic curve Cryptography is one of the many encryption techniques used in the organizations for providing secured data for the user. The works related to encryption in WSN ended ECC showing up a lot of advantages". [6] "In their research study, the researchers emphasize about various trends that are emerging in the WSN environment and have depicted the information on how the data synchronization are providing seamless support to the organizations, in terms of effectively managing their technical infrastructure, facilitating their staff in terms of accessing the enterprise applications of the organizations." [7] "One of the closely related work proposed the concept of providing secured application by ECC architecture using Sql server 2005 and JAVA application programming software. They carried out the implementation using Trusted Platform Mobile (TPM), which provides a trust for building computing base" [8]. "Studies proved that ECC algorithm was one among the best algorithms compared to other algorithms, which provide a higher level of security using less number of bits. But considering the security levels, ECC cannot be able to provide high level security than RSA." [9] "However, except a little no successful attacks have been evident on this family of curves due to the design of the elliptic curve." [10]

Elliptic Curve Cryptography

Rivest, Shamir, and Adleman invented the "RSA algorithm, which is one of the most basic public-key cryptosystems. The parameters are n, p, and q, as well as e and d. The modulus n is defined as the product of two distinct large random primes: n = pq. The RSA algorithm can be used to encrypt messages and create digital signatures for electronic documents. The RSA algorithm requires the modular exponentiation to be computed, which is broken down into a series of modular multiplications by the use of exponentiation heuristics."

Problems in RSA

- For RSA, the key length is longer.
- The RSA algorithm generates processing overhead.
- Because RSA uses 1024 bit keys, the overall system security strength is reduced to 80 bits, whereas the total strength required is 128 bits.
- RSA requires a minimum key size of 3072 bits to support this strength.
- Time consumption is greater.

"Elliptic Curve Cryptography (ECC) is effectively used as a touch of preparing to instantiate public key cryptography conventions, for instance executing keys and digital signatures. There are diverse motivations behind energy of using elliptic bends as they offer more little key sizes and more possible executions" [11].

Elliptic curves are mathematical constructions derived from number theory and algebraic geometry that have recently found numerous applications in cryptography. An elliptic curve can be defined over any field (e.g., real, rational, complex). In cryptography, however, elliptic curves are typically defined over finite fields. Elliptic curves are simple functions represented by gently looping lines in the (x, y) plane. It can provide faster and smaller-key versions of public-key methods while maintaining the same level of security. The fact that they use a different type of mathematical group for public-key arithmetic gives them an advantage. Today, all practical public-key systems make use of arithmetic with large finite groups properties.

An elliptic curve is a set of equation points. $Y^2=x^3+ax+b$, where a and b are real numbers and x and y have real-number values. Because the highest exponent in such equations is 3, they are said to be cubic. We must plot the elliptic curve using the above equation. The sum of three points on an elliptic curve that lie in a straight line is O. The inverse of point p is the point with the same x coordinate but the inverse of the y coordinate; that is, if p=(x, y), then –p=(x,-y). It is worth noting that these two points can be joined by a vertical line. It is worth noting that p+ (-p) = p-p=O. A straight line is drawn between two points P and Q with different x coordinates to find the third point of intersection R. In order to form a group structure, we must define addition on these three points as follows: P+Q = -R, P+Q is defined as the mirror image of the third point of intersection.

An elliptic curve is a plane and asymmetrical curve that transverses a finite field comprised of the points sustaining the following elliptic curve equation:

$$\mathbf{y^2=x^3+ax+b}.$$

a, b, x and y are real numbers and elliptic curve changes with various choices of a and b.

When plotted, this algebraic function ($y^2=x^3+ax+b$) will appear as a symmetrical curve parallel to the x-axis in the elliptic curve cryptography algorithm. Unlike other forms of public-key cryptography, the elliptic curve method is based on a single one-way feature that makes it easier to complete a calculation but makes it impractical to invert or withdraw the results of the calculation to find the initial numbers. This property improves the security and efficiency of the elliptic curve cryptography algorithm.

Table 1 shows a comparison of Elliptic Curve security and RSA Security based on their key size.

Table 1: Comparison of Key Size in RSA and ECC

ECC (Key Size in Bits)	RSA (Key Size in Bits)	Key Size Ratio
160	1024	1:6
256	3024	1:12
384	7680	1:20
512	16360	1:30

Graph 1: Comparison of Key Size in RSA and ECC

From the above table it can be concluded that the ECC has more security and privacy as compared to the RSA.

Conclusion

Elliptic Curve Cryptography is more secure and efficient than first generation public key techniques like RSA, which are currently in use. When it comes to system upgrades, vendors should seriously consider the elliptic curve option for the computational and bandwidth advantages it provides at comparable security. Although the security of ECC has not been thoroughly evaluated, it is expected to be widely used in a variety of fields in the future. When the RSA and ECC cyphers were compared, the ECC cypher was found to have significantly lower overheads than the RSA cypher. Because it can provide the same level of security as RSA while using shorter keys, the ECC has many advantages.

References

I.-F. Akyildiz, T. Melodia, and K.-R. Chowdhury, “A survey on wireless multimedia sensor networks,” Computer Networks, Elsevier, vol. 51, pp. pp. 921–960, 2004.

A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, “Wireless sensor networks for habitat monitoring,” in 1st Workshop on Wireless Sensor Networks and Applications, 2002.

J. McCulloch, S. M. Guru, and D. Hugo, “Wireless sensor network deployment for water use efficiency in irrigation,” in Workshop on Real-World Wireless Sensor Networks, 2008.

D. Malan, “Crypto for tiny objects,” Harvard University, Cambridge, Massachusetts, USA, Tech. Rep., January 2004.

Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing." In Information Security for South Africa (ISSA), 2010, pp. 1-7. IEEE, 2010.

Singla, Sanjoli, and Jasmeet Singh. "Cloud data security using authentication and encryption technique." Global Journal of Computer Science and Technology 13, no. 3 (2013).

Koblitz, Neal, Alfred Menezes, and Scott Vanstone. "The state of elliptic curve cryptography." In Towards a quarter-century of public key cryptography, pp. 103-123. Springer US, 2000.

Lauter, Kristin. "The advantages of elliptic curve cryptography for wireless security." IEEE Wireless communications 11, no. 1 (2004): 62-67.

Alowolodu, O. D., B. K. Alese, A. O. Adetunmbi, O. S. Adewale, and O. S. Ogundele. "Elliptic curve cryptography for securing cloud computing applications." International Journal of Computer Applications 66, no. 23 (2013).

Gampala, Veerraju, Srilakshmi Inuganti, and Satish Muppidi. "Data security in cloud computing with elliptic curve cryptography." International Journal of Soft Computing and Engineering (IJSCE) 2, no. 3 (2012): 138-141.

D. J. Bernstein and T. Lange (editors). eBACS: ECRYPT Benchmarking of Cryptographic Systems, http://bench. crypto, October 2013.

Bhar, Sreya. "Encryption Key Generation by Using Modified Hand-Geometry Based Cryptosystem to Secure SMS in Android." *International Journal of Computer Science and Engineering (IJCSE)* 4.5 (2015): 17-26.

Vaishnav, Naman, and Hardik Upadhyay. "Comprehensive Study on Key Management Schemes in Manet." International Journal of Computer Science and Engineering (IJCSE) 5.2, Feb Mar 2016, 81-90

Dakshayini, M., Shivanand Channi, and P. Jayarekha. "Load Balancing System for Traffic Network using Virtual Routing Techniques." *Development (IJECIERD)* 3.3 (2013): 35-44.

Ghosh, Ramkrishna. "An efficient and robust modified RSA based security algorithm in modern cryptography." *Journal of Computer Science Engineering and Information Technology Research (JCSEITR)* 6.2 (2016): 15-22.

Al-Khouri, Ali M. "PKI Technology: A Government Experience." International Journal of Information Systems Management Research and Development (IJISMRD) ISSN(P): 2250-236X; ISSN(E): 2319-4480 Vol. 4, Issue 2, Apr 2014, 1-16