© 2017 IJSRSET | Volume 3 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Security in Wireless Ad-Hoc Network Using Encrypted Data Transmission

Archana Chakor[1], Pooja Sangle[2], Trushali Tandel[3], Manish Gangavane[4]

[1,2,3]Padmabhushan Vasantdada Patil Pratishthan's College of Engineering, Maharashtra, Mumbai, India
[4]Department of Computer Engineering, Mumbai University, Mumbai, Maharashtra, India

ABSTRACT

Currently, there has been an increasing trend in outsourcing data to remote cloud, where the people outsource their data at Cloud Service Provider(CSP) who offers huge storage space with low cost. Thus users can reduce the maintenance and burden of local data storage. Our design is based on Elliptic Curve Cryptography. Most importantly, our protocol is confidential: it never reveals the data contents to the malicious parties. The proposed scheme also considers the Dynamic data operations at block level while maintaining the same security assurance. Through security analysis, we prove that our method is secure and through performance and experimental results, we also prove that our method is efficient. To compare with existing schemes, our scheme is more secure and efficient.

Keywords : Cryptography, Stegnography, ECC, LSB, Encyption, Decryption

I. INTRODUCTION

A wireless ad hoc network (WANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks. With the invention of Storage, the days of keeping all your documents, photos, music files etc. on your computer's hardware are gradually coming to a close. Today, the storage is fulfilling the need for more storage space to hold all of your digital data. Storage can be used from smaller computing devices to desktop computers and servers. The data when stored on Storage space has the following threats:

1. When data is distributed, it is stored at multiple locations increasing the risk of unauthorized physical access to the data.
2. The number of people with access to the data who could be compromised (i.e. bribed or coerced) increases dramatically.

To secure data, most systems use a combination of techniques, that is Encryption, which means they use a complex algorithm to encode information. To decode the encrypted files, a user needs an encryption key. While it's possible to crack encrypted information, most hackers don't have access to the amount of computer processing power they would need to decrypt information.

Steganography is a technology that hides a message within an object, a text, or a picture. It is often confused with cryptography, not in name but in appearance and usage.

II. METHODS AND MATERIAL

A. Objective

The main objective for developing this application is that, it can provide the user with security of data. It will provide encryption to data as well as steganography to data. It will also provide the transfer of data from one machine to another in from of files. Only the authorized user and administrator can access the application.

B. Problem Statement

For some applications User-Id and password are not protected. As a result anyone who is interested in using the application can access it. Sending a plain text of data to the receiver is not secure. Since the data is readable any one can get the information. In this project we will be sending the data from one system to another system using encryption. Even if the message is encoded before sending the message, it can be decoded by the hacker by making use of certain algorithm. To prevent this, in addition to encryption we will also apply steganography to data. The main aim of this project or application is to provide high quality of data security and transfer of data from source to destination.

C. Methodology Used

The system planning also includes the selection of technology for the development of the modules and the application. The technology which will be used in this project is JAVA and HTML. The JAVA technology will be used for providing platform independency to the application and for doing the bit level calculations in the modules. The HTML technology would be used for the development of help modules which will be meant for providing to the application.

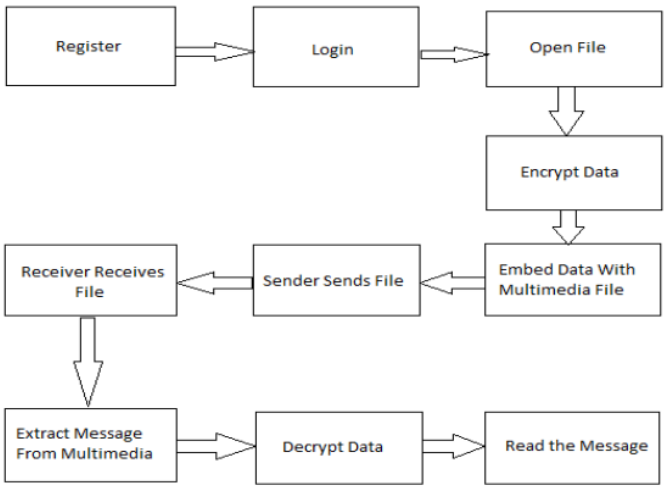

Figure 1. System Block Diagram

In our system the user will first register itself by using it's appropriate id and password. Once the user is authenticated the system will ask the user to open the file which he/she want to transmit. The file which is to be transmitted will be encrypted by using the corresponding encryption algorithm. After the encryption of the file we will embed the file with multimedia file and will send it to the receiver.

At the receiver side receiver will get the notification that he/she has received some file. Then receiver will extract the original file from the multimedia file and will decrypt it. In this way receiver will be able to read the original file.

The application which we will be developing is a stand-alone application. This application, apart from providing data security communicates with other machines for file transfer. The machines which will be communicating might not have same platform. For embedding the files and the message the image, audio, video files need to be rendered at bit level. So a very secure technique is required for dealing at bit level.

D. Literature Survey

In today's ever growing cyber world where very large amount of data is transferred daily the web or internet. This data may contain some sensitive information like in online transaction it contains account details; the security of this sensitive data becomes topmost priority and a major challenge. The security in wireless sensor networks is currently provided mostly through symmetric key cryptography. These protocols are based on the idea of keys before the deployment of the wireless sensor network. However, due to the limitation on memory resources of wireless sensor nodes, these protocols are not able to achieve perfect security and also face a key Management problem in large scale wireless sensor networks.

Elliptic curve cryptography [ECC] is a public-key cryptosystem. Every user has a public and a private key. Public key is used for encryption/signature verification. Private Key is used for decryption/signature generation. Elliptic curves are used as an extension to other current cryptosystems - that is Elliptic Curve Diffie-Hellman Key Exchange and Elliptic Curve Digital Signature Algorithm.

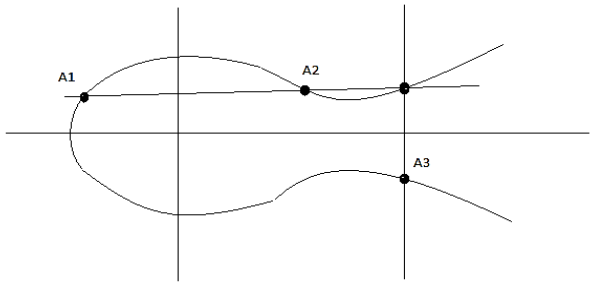

Figure 1. ECC Curve

A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The Steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes.

Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography.

The LSB is the lowest significant bit in the byte value of the image pixel.

The LSB based image stegnography embeds
the secret in tha least significant bits of pixel value of the cover image.

Figure 2. Message byte

Figure 3. Pixel embedded with message byte

Paper1: Capacity of Ad Hoc Wireless Network

Author: Jinyang Li, Charles Blake, Robert Morris
M.I.T.Laboratory for Computer Sceince

Ad hoc wireless networks promise convenient infrastructure-free communication. We expect the total capacity of such networks to grow with the area they cover, due to spatial re-use of the spectrum: nodes sufficiently far apart can transmit concurrently. However, ad hoc routing requires that nodes cooperate to forward each others' packets.

This means that the throughput available to each single node's applications is limited not channel capacity, but also by the forwarding load imposed by distant nodes. This effect could seriously limit the usefulness of ad hoc routing.[1]

Paper 2: The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks

Author: Christian Bettstetter, Student Member, IEEE, Giovanni Resta, and Paolo Santi JULY-SEPTEMBER 2003

The random waypoint model is a commonly used mobility model in the simulation of ad hoc networks. It is known that the spatial distribution of network nodes moving according to this model is, in general, nonuniform.

Performance analysis in the presence of mobility is of major importance in the design of wireless communication and computer networks. Since real movement patterns are difficult to obtain, a common approach is to use synthetic mobility models which resemble, to some extent, the behavior of real "mobile entities".[3]

Paper 3:A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks

Author: An Liu Department of Computer Science NC State University, Raleigh, NC 27695

Public Key Cryptography (PKC) has been the enabling technology underlying many security services and protocols in traditional networks such as the Internet. In the context of wireless sensor networks, elliptic curve cryptography (ECC), one of the most efficient types of PKC, is being investigated to provide PKC support in sensor network applications so that the existing PKC-based solutions can be exploited.

This paper presents the design, implementation, and evaluation of ECC, a configurable library for ECC operations in wireless sensor networks. The primary objective of ECC is to provide a ready-to-use, publicly available software package for ECC-based PKC operations that can be flexibly configured and integrated into sensor network applications.

Recent technological advances have made it possible to develop wireless sensor networks consisting of a large number of low-cost, low -power, and multi-functional sensor nodes that communicate over short distances through wireless link.

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields [16]. Elliptic curves used in cryptography are typically defined over two types of finite fields: prime fields Fp, where p is a large prime number, and binary extension fields F2m. For space reasons, we focus on elliptic curves over Fp in this paper.[2]

III. RESULTS AND DISCUSSION

User interface

The user interface requires the system to send the data or file securely. Each data or file will be encrypted first and then using steganography it is converted into image or audio. These will help to secure the file or data from attackers. This way, the query will be written for execution of the system.

Hardware Interface:
Routers will be used to acquire the connection between two or more system.

Software Interface:
The software interfacesconsists of the database and the application program.

Database: The database stores the records implemented in Java database Server. However, this can be changed to any other relational database of choice. JDBC Server is fast and easy, it can store a very large record and requires little configuration.

Application Program: The application program is developed with Java programming language and it provides a user interface for the Wireless Ad-hoc Network System .The advantages of Java programming language are its robustness, easy to program, has an excellent database connectivity, runs on the two most common operating system platforms like Windows and Linux

Non-Functional Requirement : The non-functional requirements of the software system will be as follows:

Reliability: The system shall be reliable such that it can store and display all the necessary information.

Maintainability: The software system shall be maintained easily as it is easy to understand and update, but the hardware needed to be cleaned regularly.

Availability: The software system shall be available to the user for processing their requirements at any given time.

Scalability: The capability of a system, network, or process to handle a growing amount of work, or its potential to be enlarged in order to accommodate that growth.

User classes and Characteristics: The input given to the system is obtained by the user. In this case, the user have to send the data or file to the respective person securely using encryption and steganography. The user details also play an important key in the system wherein the information related to the user such as name of the user and password. This information will make the software system analyze that the input is given from an authorized user.

Performance Requirements: The system showcases it performance through its easy availability and maintainability. The system shall be designed in a way such that it is easy to make the user understand the process in which the system works. For this purpose, there is a need for the system to be maintained and available.

Safety Requirements: The system shall maintain the safety of the database contents. This is the reason user authentication is required. Also timestamps will be used after every updating of record. This will set a save point so that in case of any trash or error the queries can be rollback or committed.

IV. CONCLUSION

The conclusion that can be drawn from above is using this application will help the users to secure their data in an efficient way and thus increasing security of the data.

V. REFERENCES

[1]. Capacity of Ad Hoc Wireless Networks" Jinyang Li Charles Blake Douglas S. J. De Couto Hu Imm Lee M.I.T. Laboratory for Computer Science fjinyang, cblake, decouto, hilee

[2]. A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks∗ An Liu Department of Computer Science NC State University, Raleigh, NC 27695 email: aliu3@ncsu.edu

[3]. The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks Christian Bettstetter, Student Member, IEEE, Giovanni Resta, and Paolo Santi IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 2, NO. 3, JULY-SEPTEMBER 2003

[4]. Imote2: High-performance wireless sensor network node. http://www.xbow.com/Products/Product_pdf_ files/Wireless_pdf/Imote2_Datasheet.pdf.

[5]. MICAz: Wireless measurement system. http: //www.xbow.com/Products/Product_pdf_ files/Wireless_pdf/MICAz_Datasheet.pdf.

[6]. The openssl project. http://www.openssl.org/.

[7]. SSL 3.0 specification. http://wp.netscape.com/eng/ ssl3/. 15

[8]. TelosB mote platform. http://www.xbow.com/ Products/Product_pdf_files/Wireless_pdf/ TelosB_Datasheet.pdf.

[9]. TinyOS: An open-source OS for the networked sensor regime. http://www.tinyos.net/.

[10]. Tmote sky: Reliable low-power wireless sensor networking eases development and deployment. http://www. moteiv.com/products-tmotesky.php.

[11]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: A survey. Computer Networks, 38(4):393–422, 2002.

[12]. American Bankers Association. ANSI X9.62-1998: Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA), 1999.

[13]. Certicom Research. Standards for efficient cryptography – SEC 1: Elliptic curve cryptography. http://www.secg. org/download/aid-385/sec1_final.pdf, September 2000.

[14]. Certicom Research. Standards for efficient cryptography – SEC 2: Recommended elliptic curve domain parameters. http://www.secg.org/collateral/sec2_ final.pdf, September 2000.

[15]. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Research in Security and Privacy, pages 197–213, 2003.

[16]. W. Dai. Crypto++ library 5.5. http://www.cryptopp. com/, May 2007. [14J. Deng, R. Han, and S. Mishra. Secure code distribution in dynamically programmable wireless sensor networks. In Proceedings of the Fifth International Conference on Information Processing in Sensor Networks (IPSN '06), April 2006.

[17]. W. Diffie and M.E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22:644– 654, November 1976.

[18]. W. Du, J. Deng, Y. S. Han, and P. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03), pages 42–51, October 2003.

[19]. L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communications Security, pages 41–47, November 2002.

[20]. D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler. The nesC language: A holistic approach to networked embedded systems. In Proceedings of Programming Language Design and Implementation (PLDI '03), June 2003.