IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-4, Special Issue-2, April 2016 E-ISSN: 2347-2693

A New Security Protocol Using Hybrid Cryptography Algorithms

Darshan Bhole[1], Aditi Mote[2], Prof. Rachana Patil [3]

[1]*Computer Engineering (BE), Mumbai University, India*
[2]*Computer Engineering (BE), Mumbai University, India*
[3]*Computer Engineering (ME), Mumbai University, India*

Available online at: www.ijcseonline.org

Abstract— A Computer Network is an interconnected group of autonomous computing nodes, which use a well-defined, mutually agreed set of rules and conventions known as protocols, interact with one-another meaningfully and allow resource sharing preferably in a predictable and controllable manner. Communication has a major impact on today's business. It is desired to communicate data with high security. Security Attacks compromises the security and hence various Symmetric and Asymmetric cryptographic algorithms have been proposed to achieve the security services such as Authentication, Confidentiality, Integrity, Non-Repudiation and Availability.At present, various types of cryptographic algorithms provide high security to information on controlled networks. These algorithms are required to provide data security and users authenticity.To improve the strength of these security algorithms, a new security protocol for online transaction can be designed using combination of both symmetric and asymmetric cryptographic techniques. This protocol provides three cryptographic primitives such as integrity, confidentiality and authentication. These three primitives can be achieved with the help of Advance Encryption Standard,Elliptic Curve Cryptography,XOR-Dual RSA algorithm and Message Digest MD5. It uses Elliptic Curve Cryptography and Advance Encryption both for encryption,XOR-Dual RSA algorithm for authentication and MD-5 for integrity. This new security protocol has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.

Keywords**—**Advanced Encryption Standard;Cryptography;Message Digest-5;WSN,XOR-Dual RSA;

I. INTRODUCTION

Curiosity is one of the most common human traits, matched by the wish to conceal private information. Spies and the military all resort to information hiding to pass messages securely,sometimes deliberately including misleading information [8] . Steganography, a mechanism for hiding information in apparently innocent pictures, may be used on its own or with other methods. Encryption fundamentally consists of scrambling a message so that its contents are not readily accessible while decryption is the reversing of that process [6]. These processes depend on particular algorithms, known as ciphers. Suitably scrambled text is known as cipher text while the original is, not surprisingly, plain text. Readability is neither a necessary nor sufficient condition for something to be plain text. The original might well not make any obvious sense when read, as would be the case, for example, if something already encrypted were being further encrypted. It's also quite possible to construct a mechanism whose output is readable text but which actually bears no relationship to the unencrypted original. A key is used in conjunction with a cipher to encrypt or decrypt text. The key might appear meaningful, as would be the case with a character string used as a password, but this transformation is irrelevant, the functionality of a key lies in its being a string of bits determining the mapping of the plain text to the cipher text.

Even after a decade of availability and promising commercial successes, security remains the number one concern for enterprise WLAN deployments. The very nature of networking means that users can exchange information across a distance and over a shared medium. The security implication of this is that a hacker does not need to actually walk up to a server or a user's computer in order to gain access to critical files or communications. With wireless LAN, this threat is especially pronounced, because a hacker doesn't even need to reside in the same physical location.

II. RELATED WORK

WulingRen, Zhejiang Gongshang, 2010 proposed the solution to the short comings; 128-bit E0 stream ciphers in some cases can be cracked, Low credibility of PIN, High probability of non-link key cheat, Address Spoofing present in existing security system of Bluetooth. They proposed a hybrid system based on DES and RSA. DES is a symmetric key cryptographic algorithm and RSA is an asymmetric key cryptographic algorithm. In which public and private key pair is used. Here DES use symmetric key and the size of the key is 56-bit only that is more vulnerable to attacks like brute force attack, man-in-middle attack etc.

1. (Subasree) Security Protocol Architecture [7]
As shown in Fig. , the plain text is encrypted with the help of ECC and the derived cipher text is communicated to the destination through any secured channel. Simultaneously, the Hash value is calculated through MD5 for the same plain text, which already has been converted into the cipher text by ECC. This Hash value has been encrypted with DUAL RSA and the encrypted message of this Hash value also sent to the destination. In this protocol, it is difficult to extract the plain text from the cipher text, because the Hash value is encrypted with DUAL RSA and the plain text is encrypted with ECC. The Hash value is calculated with MD5 . However, there are two disadvantages. First , the message is encrypted by Asymmetric Algorithms (ECC and DUAL RSA Public key encryptions) that are slow compared to symmetric encryption. Second, if an attacker determines a person's private key, his or her entire messages can be read.

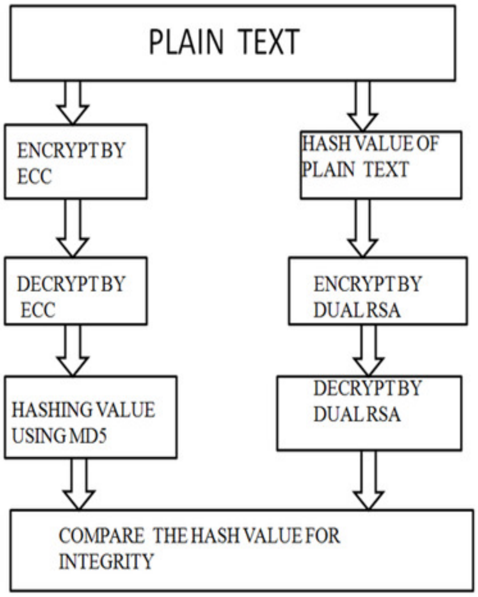

Fig: (SUBASREE) SECURITY PROTOCOL ARCHITECTURE [7]

2. (Kumar) Security Protocol Architecture [3]
The protocol architecture is shown in Fig. The given plain text is encrypted first with AES algorithm and then with ECC algorithm. The Hash value of this encrypted cipher text is taken through the MD5 algorithm. On the other side, the Hash value is first evaluated and integrated. Thereafter, the decryption of cipher text is done by AES and ECC decryption algorithms. Hence, the plaintext can be derived. This Protocol is a combination of both the Symmetric and Asymmetric Cryptographic Techniques. However, the execution time of this protocol is long because the plaintext is encrypted sequentially by both AES and ECC.

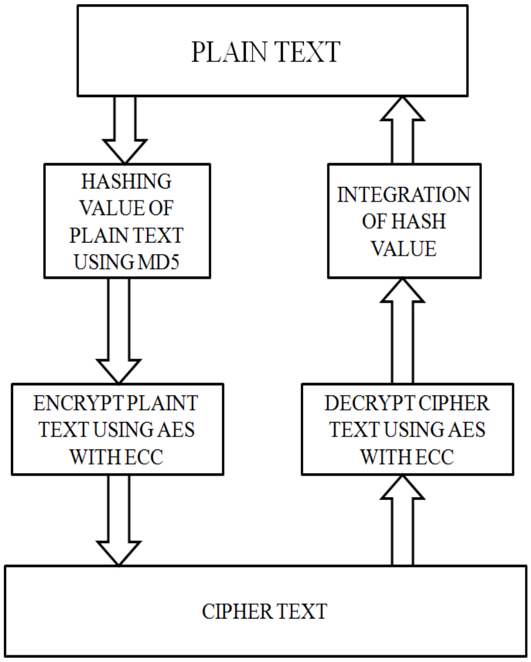
PLAIN TEXT
HASHING VALUE OF PLAIN TEXT USING MD5
INTEGRATION OF HASH VALUE
ENCRYPT PLAINT TEXT USING AES WITH ECC
DECRYPT CIPHER TEXT USING AES WITH ECC
CIPHER TEXT

Fig: (KUMAR) HYBRID PROTOCOL ARCHITECTURE [3]

III. Proposed System

A. Encryption Phase.

.

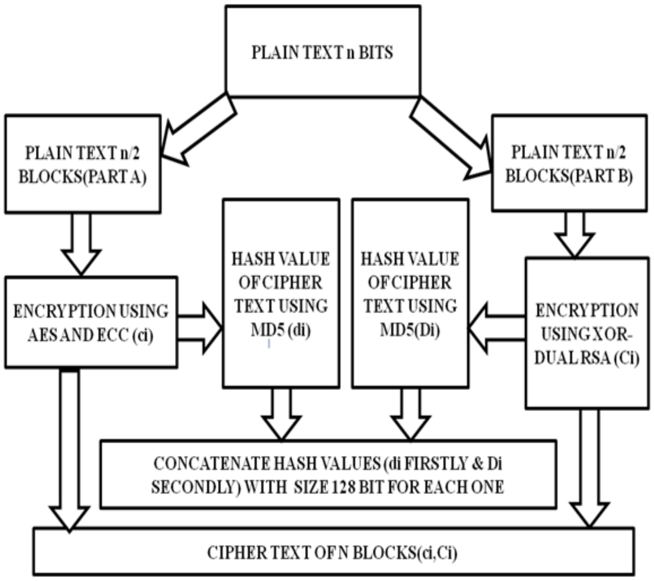
PLAIN TEXT n BITS
PLAIN TEXT n/2 BLOCKS(PART A)
PLAIN TEXT n/2 BLOCKS(PART B)
ENCRYPTION USING AES AND ECC (di)
HASH VALUE OF CIPHER TEXT USING MD5 (di)
HASH VALUE OF CIPHER TEXT USING MD5(Di)
ENCRYPTION USING XOR-DUAL RSA (Ci)
CONCATENATE HASH VALUES (di FIRSTLY & Di SECONDLY) WITH SIZE 128 BIT FOR EACH ONE
CIPHER TEXT OF N BLOCKS(di,Ci)

Fig: ENCRYPTION PHASE OF HCP

The plaintext is divided into n blocks. Each block consists of 128 bits. Then, it is divided into two parts P1 (0: n/2-1) blocks, and P2 (n/2: n-l) blocks.The first n/2 blocks are encrypted using (AES and ECC) hybrid encryption algorithm. ECC algorith m is used for protecting secret key which is highest secure public key algorithm. Moreover, according to the mathematical problem on which ECC can be solved by fully exponential rather than sub exponential for other public key systems, ECC needs smaller key size than other algorithms and that refers to less memory size [2] It allows the communication nodes to handle a larger number of requests with the smallest number of dropped packet. Since that ECC consumes more power than symmetric algorithm, using AES algorithm reduces the power consumption and raises the system performance [4] . When using AES with ECC, we are able to save power, and achieve speed up to 25% for encryption and nearly 20% for decryption [9].

The first n/2 blocks are encrypted as the following:

P1 will be encrypted using AES by the key *ki* which is the secret key of AES encryption algorithm with size 128 bits. *ki* is encrypted by ECC to produce *Kj.*

In parallel, the remaining n/2 blocks are encrypted using XOR-DUAL RSA algorithm. DUAL RSA allows for extremely fast encryption and decryption that is at most four times faster than standard RSA .The XOR Encryption algorithm is an example of a symmetric encryption algorithm. This means that the same key is used for both encryption and decryption.

MD5 is applied to the cipher texts. It is the best performance of hashing function security [4].

At the final stage of the encryption process, the two n/2 blocks are integrated to generate cipher text of n blocks and it is sent to the sink node. The corresponding Hash values (*di* and *Di*) with size 128 bits for each one are concatenated and sent to the sink node at the same time.

B. *Decryption Phase*

The Decryption phase is shown in Fig. The cipher text is divided into n blocks each block consists of 128 bits, Then it will be divided into two parts (0: n/2-1) blocks and (n/2: n-l) blocks.

Hashing is used in order to identify whether the sink node receive the same cipher text or not. In the proposed protocol, if the Hash values in both phases are compared. If they are the same, then the protocol will proceed the decryption phase. Else, it will discard the message.

In the case of the hash values are the same at the source and sink nodes, the first n/2 blocks are decrypted using AES and ECC algorithms.

Kj is decrypted by ECC to produce *ki* which is used to decrypt the cipher text using AES decryption scheme by *DAES* (AES decryption function).

The remaining n/2 blocks are decrypted using XNOR-DUAL RSA algorithm. Private Key (d, p, q) used for decryption.

At the final stage of the decryption process, the two n/2 blocks are integrated to produce plain text of n blocks.

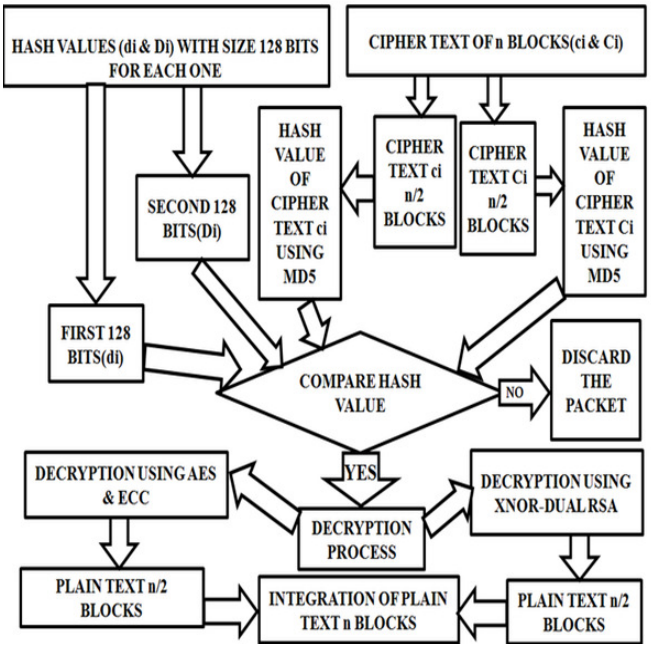
HASH VALUES (di & Di) WITH SIZE 128 BITS FOR EACH ONE
CIPHER TEXT OF n BLOCKS(ci & Ci)
HASH VALUE OF CIPHER TEXT ci USING MD5
CIPHER TEXT ci n/2 BLOCKS
CIPHER TEXT Ci n/2 BLOCKS
HASH VALUE OF CIPHER TEXT Ci USING MD5
SECOND 128 BITS(Di)
FIRST 128 BITS(di)
COMPARE HASH VALUE
NO
DISCARD THE PACKET
YES
DECRYPTION USING AES & ECC
DECRYPTION PROCESS
DECRYPTION USING XNOR-DUAL RSA
PLAIN TEXT n/2 BLOCKS
INTEGRATION OF PLAIN TEXT n BLOCKS
PLAIN TEXT n/2 BLOCKS

Fig: DECRYPTION PHASE OF HCP

C. *Strength Of HCP Protocol*

A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. A hybrid cryptosystem can be constructed using any two separate cryptosystems:

- a key encapsulation scheme, which is a public-key cryptosystem, and
- a data encapsulation scheme, which is a symmetric-key cryptosystem.

The hybrid cryptosystem is itself a public-key system, whose public and private keys are the same as in the key encapsulation scheme.

If both the key encapsulation and data encapsulation schemes are secure against adaptive chosen ciphertext attacks, then the hybrid scheme inherits that property as well.

The combination of encryption methods has various advantages. One is that a connection channel is established between two users' sets of equipment. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced. The result is the added security of the transmittal process along with overall improved system performance.

D. System Requirement

Hardware Requirement

- -Pentium IV processor
- -1 GB RAM
- -CD ROM
- -80 GB HARD DISK

Software Requirement:

- **-**WINDOWS 7
- **-**JAVA
- **-**MICROSOFT WINDOWS STUDIO,MS ACCESS
- **-**NETBEANS.

IV. RUN-TIME ANALYSIS

A. The Size Of The Cipher Text

Table I describes the output of the encryption process. It shows the size of the cipher text in bytes. It is shown that (Kumar) Protocol is the worst.

B. Time Of Encryption And Decryption Processes

The encryption time is the time that an encryption algorithm takes to produce a cipher text from a plaintext. The decryption time is the time that an decryption algorithm takes to produce a plaintext from a cipher text. Table II shows the time of encryption process for different sizes of plain text. It is shown that, (Zhu) protocol and the proposed hybrid protocol achieve the least time for encryption. Table III shows the time of decryption process for different sizes of plain text. As in the encryption, it is clear that (Zhu) protocol and the proposed hybrid protocol have the same results and the least time for
decryption.

C. Throughput

Enryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as:
Throughput of encryption = Tp (Bytes) / Et (Second)
where Tp is the total plain text (bytes) and Et is the encryption time (second). Table IV shows the throughput of the proposed hybrid protocol compared with the existing protocols for different sizes of plain text. It is shown that both (Zhu) protocol and the proposed protocol have the same results and they achieve the largest values.

TABLE I. SIZE OF CIPHER TEXT (BYTES)

Size Of The PlainText (Bytes)	**Subasree protocol**	**Kumar Protocol**	**Zhu Protocol**	**HCP**
609	609	846	609	641
25615	25615	35142	25615	25647
35080	35080	48226	35080	35112
61386	61386	84340	61386	61418
184162	184162	253008	184162	184194

TABLE II. TIME OF ENCRYPTTON (MS)

Size Of The PlainText	**Subasree protocol**	**Kumar Protocol**	**Zhu Protocol**	**HCP**
609	2063	1500	998	998
25615	3683	1518	1022	1022
35080	5651	1526	1059	1059
61386	15351	4219	3143	3143
184162	105889	5752	3814	3814

TABLE III. TIME OF DECRYPTION (MS)

Size Of The PlainText	**Subasree protocol**	**Kumar Protocol**	**Zhu Protocol**	**HCP**
609	1078	966	562	562
25615	1085	972	713	713
35080	1082	980	824	824
61386	1197	991	891	891
184162	2087	1099	907	907

TABLE IV. THROUGHPUT

Size Of The PlainText	**Subasree protocol**	**Kumar Protocol**	**Zhu Protocol**	**HCP**
609	295.20	406.00	610.2	610.2
25615	6954.93	6874.18	12063.6	12063.6
35080	6207.75	22988.2	33125.6	33125.6
61386	3998.83	14549.9	19531.0	19531.0
184162	1739.20	32017.0	48285.7	48285.8

CONCLUSION

In this paper, a robust hybrid security protocol for WSNs is proposed. It is designed in order to solve several problems as practical implementation, short response time, efficient computation and the strength of cryptosystem. The proposed hybrid protocol tries to trap the intruder by splitting the plaintext and then applies two different techniques. First, it takes the advantages of the combination of both Symmetric and Asymmetric cryptographic techniques using both AES and ECC algorithms. Second, XOR-DUAL RSA is used since it is more robust and cannot be easily attacked. In addition, Hashing is also used for data integrity using MD5 to be ensured that the original text is not being altered in the communication medium. The attractiveness of the proposed protocol, compared to other existing security protocols, is that it appears to offer better security for a shorter encryption and decryption time, and smallest cipher text size. There by, reducing processing overhead and achieving lower memory consumption that is appropriate for all WSN applications.

ACKNOWLEDGEMENT

I thank my guide Prof. (Mrs) Rachana Y Patil whose guidance, support and dedication is priceless. I especially thank to IEEE (Institute of Electrical and Electronics Engineers, Inc.) for providing recent information about my document.

It has been a challenging, yet rewarding journey which I couldn't have completed alone and I am grateful for my team member's support.

REFERENCES

[1] Dan Boneh and Glenn Durfee. Cryptanalysis of rsa with private key d less than n 0.292. *Information Theory, IEEE Transactions on*, 46(4):1339–1349, 2000.

[2] Ravi Kishore Kodali and NVS Narasimha Sarma. Energy efficient ecc encryption using ecdh. In *Emerging Research in Electronics, Computer Science and Technology*, volume248, pages 471–478. Springer, 2014.

[3] N. Kumar. A secure communication wireless sensor networks through hybrid (aes+ecc) algorithm. *von LAP LAMBERT Academic Publishing*, 386, 2012.

[4] Mewada, Shivlal, Pradeep Sharma, and S. S. Gautam. "*Classification of Efficient Symmetric Key Cryptography Algorithms*" International Journal of Computer Science and Information Security, Vol-14, No-2 (2016): 105-110.

[5] T. R. Mahesh M. J. Dubal and P. A. Ghosh. Design of a new security protocol using hybrid cryptography algorithms. *In Proceedings of 3rd International Conference on Electronics Computer Technology (ICECT)*, 5), year=2010**.**

[6] Wuling Ren and Zhiqian Miao. A hybrid encryption algorithm based on des and rsa in Bluetooth communication. In *Modeling, Simulation and Visualization Methods (WMSVM), 2010 Second International Conference on*, pages 221–225. IEEE, 2010.

[7] S Subasree and NK Sakthivel. Design of a new security protocol using hybrid cryptography.

[8] Hung-Min Sun, Mu-En Wu, Wei-Chi Ting, and M Jason Hinek. Dual rsa and its security analysis. *Information Theory, IEEE Transactions on*, 53(8):2922–2933, 2007.

[9] Stefan Tillich and Johann Großsch¨adl. Accelerating aes using instruction set extensions for elliptic curve cryptography. In *Computational Science and Its Applications–ICCSA 2005*, pages 665–675. Springer, 2005.

[10] Shi-hai Zhu. Research of hybrid cipher algorithm application to hydraulic information transmission. In *Electronics, Communications and Control (ICECC), 2011 International Conference on*, pages 3873–3876. IEEE, 2011.

AUTHORS PROFILE

Darshan Bhole: He is persuing the BE degree in Computer Engineering from A. C. Patil College of Engineering, Kharghar, Navi Mumbai, Mumbai University. His research interests includes Internet and Web Technology, Cyptography Alogorithms , and Intelligent Networks.

Aditi Mote: She is persuing the BE degree in Computer Engineering from A. C. Patil College of Engineering, Kharghar, Navi Mumbai, Mumbai University. His research interests includes Internet and Web Technology.

Rachana Patil: She has received the ME degree in computer engineering from Mumbai University, Mumbai, India, in 2012.She is currently working as an Assistant Professor with Computer Engineering Department, A. C. Patil College of Engineering, Kharghar, Navi Mumbai. Her research interests include Computer Network .Wireless network Security, Business intelligence systems. Mobile communication and systems