



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Identity based secure communication over wireless network using NTEA

Amishi Aggarwal¹, Pradeep Kumar²

^{1,2} Computer Science and Engg, Mahamaya Technical University
Sector 62, Noida, UP, INDIA

Abstract: As Wireless links are more vulnerable to attacks they are considered to be "un-trusted" in terms of security, i.e. they are relatively simple to be hacked. One can easily gain access to confidential information. In this paper we propose a secure transmission of information in wireless network by generating the key using Lagrange interpolation and polynomial equation through which only the shares will be transmitted over the network not the key. That key will be generated by the receiver by using those shares and node id known to the users and that generated key will be used in the algorithm known as New Tiny Encryption Algorithm (NTEA) which is a cryptographic efficient algorithm designed to minimize memory and maximize speed. TEA suffers from differential cryptanalysis most notably from equivalent keys and related-key attacks. We tried to remove its weaknesses by securing the key used in our proposed NTEA algorithm.

Keywords: NTEA , ID based cryptography , Lagrange interpolation , Multi Agent Model , Threshold Cryptography

I. Introduction:

Security during transmission of data is an important issue as in decentralized wireless networks there is no information available between the existing nodes and these networks are much weak to be attacked. The elements necessary for secure communication over the insecure wireless channel, are privacy, confidentiality, key exchange, authentication, and non-repudiation. Security threats cause continual patching in wireless networks. Therefore, enhancing security of wireless networks has become one of the most important problem in the area of wireless network. . Main areas of exploration of security concerns will be the encrypting of data transmissions and protection against attacks. The attacks on security may be of either passive attack or active attack. Passive attacks threaten confidentiality of data.[2] The attacker does not modify the data, but only captures and monitors the traffic. Availability can be compromised when the data is not encrypted. Active attacks occur when the attacker actively captures the data and attempts to modify, delete, add or redirect the data. This threat violates the security of the data.

The strength of its infrastructure (wireless nature) also becomes the point of its greatest susceptibility. Thus decreasing the confidence level of the system as it pertains to availability, reliability, data integrity and privacy concerns. Authentication is the basis of any secure communication. This can only be realized by means of verifying something known to be associated with an identity.

The **Tiny Encryption Algorithm** (TEA) [1] is a block cipher symmetric (private) key encryption algorithm. *Symmetric key encryption* use same key for encryption and decryption whereas in asymmetric key encryption (public key encryption) different keys are used. **Symmetric** encryption uses either stream or block cipher.

Block cipher take no of bits and encrypt them as a single unit. A *block cipher* consists of two paired algorithms, one for encryption and the other for decryption. Both algorithms accept two inputs: an input block of size n bits and a key of size k bits, yielding an n -bit output block. For any one fixed key, decryption is the inverse function of encryption. The Tiny Encryption Algorithm (TEA) is a cryptographic algorithm designed to *minimize* memory footprint and maximize speed. The TEA is a feistel structure used to satisfy the confusion and the diffusion properties to hide the statistical characteristics of the plaintext.

This paper is prepared in sections. Section - I explained about the Introduction. Section - II deals with background that includes related work with reference to present problem and the proposed architecture is discussed in section - III under heads of proposed work the conclusion of this paper is mentioned in section - IV. The proposed work may extended further with reference to different situation are mentioned in section - V under future Aspect, References included in section – VI that's used in this paper.

II. BACKGROUND

Identity-based cryptography specifies a cryptosystem in which keys(both public and private) are based on the identities of the users.[3,6] This idea of IBC was first proposed by Shamir in 1984.[7]. This scheme has the property that a user's public key is easily obtained from his identity, while a user's private key can be calculated for him by any trusted authority, called a Private Key Generator (PKG). It saves storage and transmission of public keys and certificates, as compared to traditional PKI used in earlier times for key generation purpose.

In Shamir's idea of identity-based cryptosystem [3], the recipient's identity i is used to generate the key for encryption, and the key for decryption is derived from i and a random seed k . In signature scheme, the signature

key is generated from sender identity i and a random seed k , and the verification key is obtained by using sender's identity i .

Many IBC schemes [6] uses the concept of threshold cryptography which was originated from Shamir. Shamir gives a solution to the problem of sharing a secret among different users. In his paper, he provides the solution of how to divide data D into n pieces in such a way that D is easily recreate able from any t pieces, but even complete knowledge of $t - 1$ pieces provides absolutely no information about D .

Distributed pair wise key establishment scheme based on the concept of bivariate polynomials is discussed in [8]. In this method, any mobile node by knowing corresponding IDs of other nodes in an ad hoc network can securely communicate with them. The shares of the bivariate polynomial depend on the coefficient matrix of the polynomial, the requesting node's ID and the ID of the nodes that respond to the request.

The identity based cryptosystem [9,13] shared the session key among the nodes. Identity based cryptosystem provides a new but safe strategy for communication in MANET, it uses Lagrange interpolation to share the session key among the nodes of MANET. This paper provides the safe communication in the MANET.

The Agent based information retrieval model [10] techniques get back the information from the server to user. The problem is secure information retrieval from server to user. This model provides the security of information retrieval.

Modified tiny encryption algorithm in [1,11] tried to remove the weaknesses of TEA as TEA is suffered form equivalent keys and related-key attacks. Tiny Encryption Algorithm (TEA) is a light weight cryptographic symmetric block cipher and a very simple algorithm which makes it suitable for systems that require high performance; ease of implementation, high speed, low power consumption and low cost. TEA met these requirements and has a resistance towards differential cryptanalysis; however, it has a easy key schedule which makes it weak against the key attacks. MTEA uses the Linear Feedback Shift Register (LFSR) in the key schedule of TEA to overcome its security weakness.

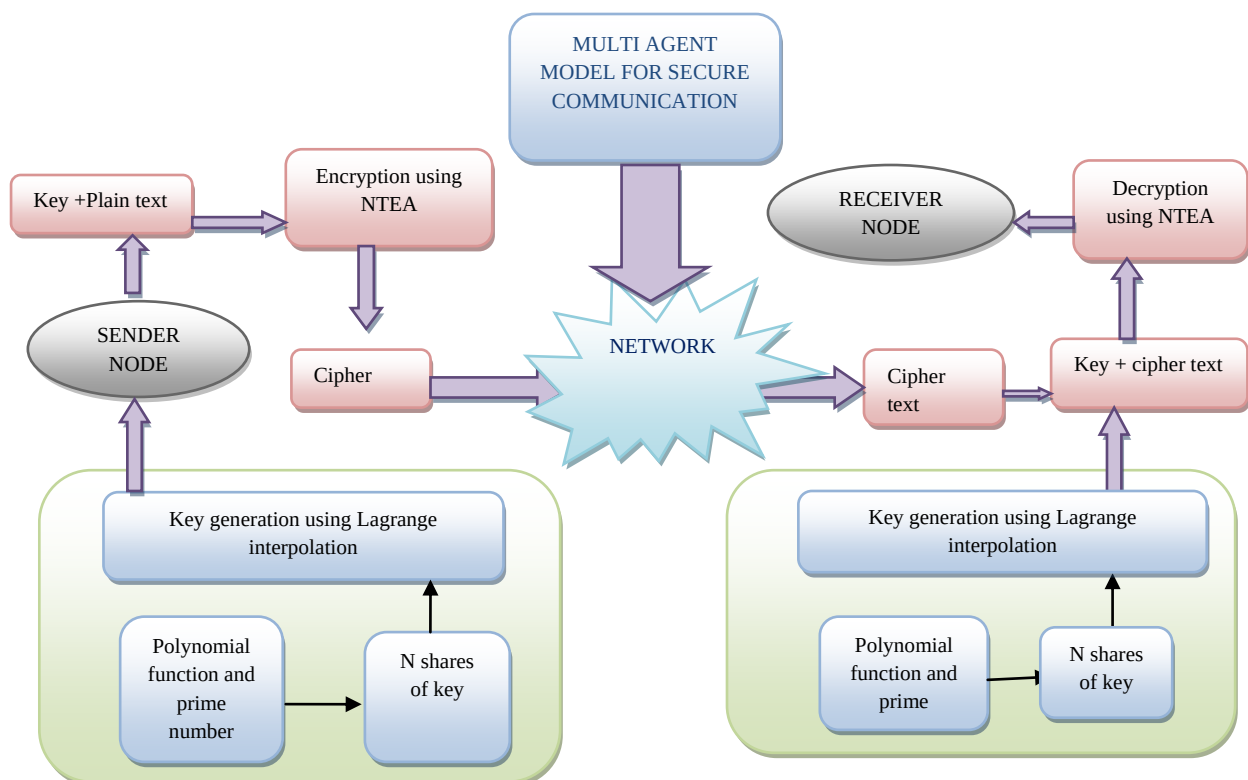
III. Proposed Security Architecture and Mechanism for wireless Information Transmission:

The proposed architecture and its detailed mechanism is presented in section A and B respectively.

A. Security Architecture :

Figure-1 illustrates the working architecture based on threshold cryptography and Lagrange interpolation. The proposed architecture is divided into modules like Generate session key using node id at both sender and receiver site, Multi Agent model for secure information retrieval among nodes, and NTEA for encrypting and decrypting the data.

Figure 1 Architecture for Identity based secure communication over network using NTEA



Steps to be followed are-

- Secret share is generated using the polynomial equation and lagrange interpolation.

- The generated secret is converted into binary form.
- Data is encrypted using NTEA which we will explain later in the paper.
- At receiver site the inverse operation will be performed as data will be decrypted by the same key which receiver will also generate through lagrange interpolation.

B. Detailed mechanism of modules of architecture

In the first Module which is of key generation, we generate the session key by using threshold cryptography and Lagrange interpolation with modular arithmetic. t_{Th} (**Threshold value**) is the minimum threshold value ie number of id and share pairs required to generate a session key. Consider a Polynomial equation GF (p) is Finite field $p > n$

Choose $b_0, b_1, b_2, \dots, b_{k-1} \in GF(p)$ $F(x) = (b_0 x^0 + b_1 x^1 + b_2 x^2 + \dots + b_{t-1} x^{t-1}) \bmod p$
 $F(0) = b_0 = \text{secret key}$ and p is a large prime number and $b_1, b_2, \dots$, and b_{k-1} are arbitrarily chosen from Z/PZ . Then each receiver of identity will have partial keys $S_i = f(\text{id}_i)$. Those shares provide t distinct points $(s, r) = (i, S_i)$ calculate polynomial by using lagrange interpolation [5]

$$F(x) = \sum_{i=1}^k Y_i \prod_{1 \leq j \leq k, j \neq i} \frac{x - x_j}{x_i - x_j} \quad \text{Eq-1}$$

Since $f(0) = b_0 = S$, the shared secret can be expressed as

$$S = \sum_{i=1}^k P_i Y_i \quad \text{Where}$$

$$P_i = \prod_{1 \leq j \leq k, j \neq i} \frac{x_j}{x_j - x_i} \quad \text{Eq-2}$$

Secret key is generated by t pairs (minimum no of threshold) by using $F(0) = b_0 \bmod p$

Example: $p = 24151$. Let the threshold be $t = 3$, and the secret be $21567 \in Z/24151Z$. We choose elements at random $b_1 = 198$ and $b_2 = 21$ in $Z/24151Z$, and set

$f(x) = 21567 + 198x + 21x^2$. As the trusted party, we can now generate as many shares as we like,

$(1, f(1)) = (1, 21607)$ $(5, f(5)) = (5, 22187)$

$(2, f(2)) = (2, 21689)$ $(6, f(6)) = (6, 22437)$

$(3, f(3)) = (3, 21813)$ $(7, f(7)) = (7, 22729)$

$(4, f(4)) = (4, 21979)$

which are distributed to the holders of the share recipients, and the original polynomial $f(x)$ is destroyed. The secret can be recovered from the formula in eq 1 using any t shares $(x_1, y_1), \dots, (x_t, y_t)$. If we take the first three shares $(1, 21607), (2, 21689), (3, 21813)$, we compute $f(0) = 21567$.

C. Secret Key Generation for encryption and decryption using lagrange interpolation and threshold cryptography concept

To generate session key required t_{Th} (**Threshold value**) no of minimum nodes required to generate the session key. Consider a Polynomial equation GF (p) is Finite field $p > n$

Choose $b_0, b_1, b_2, \dots, b_{k-1} \in GF(p)$

$F(x) = (b_0 x^0 + b_1 x^1 + b_2 x^2 + \dots + b_{t-1} x^{t-1}) \bmod p$

Total No of Node = N;

for($q=0$; $q < t$; $q++$)

{

NodeId[q];

}

for($q=0$; $q < t$; $q++$)

{

nr=1;

dr=1;

for($j=0$; $j < t$; $j++$)

{

If($j \neq q$)

{

nr=nr*($x - \text{NodeId}[j]$);

dr=dr*($\text{NodeId}[q] - \text{NodeId}[j]$);

$F(x) = (nr/dr) * F(\text{NodeId}[q]);$ /*Polynomial Equation

}

Sk= $F(x) \bmod p$; /*Session Key*/

D. New Tiny Encryption Algorithm

We will use the above concept of key generation in new tiny encryption algorithm by generating the key through Lagrange interpolation on receiver side. This generated key is used in the algorithm so that the attacks on the keys could be minimized as the key is secured already. NTEA is a block cipher with block length of 64

bits and its key length is of 128 bits. It is a Feistel type structure as shown in Figure 2 which uses operations from orthogonal algebraic groups. A dual shift in the algorithm causes all bits of the data and key to be blend repeatedly. The key schedule of the algorithm is ; the 128-bit key K is split into four 32-bit blocks (K[0], K[1], K[2], K[3]) and the 64-bit plaintext is split into two 32-bit blocks (Z_i and Y_i)

The operations on the algorithm depends on the alternate use of XOR and ADD to provide nonlinearity. Addition and subtraction are used as the reversible operators for encryption and decryption rather than XOR. 16 cycles (32-iterations) or 32 cycles (64-iterations) rounds can be used in the algorithm. The constant number, delta, a constant which is effective in “hiding” weak keys is derived from the golden number ratio[12]:

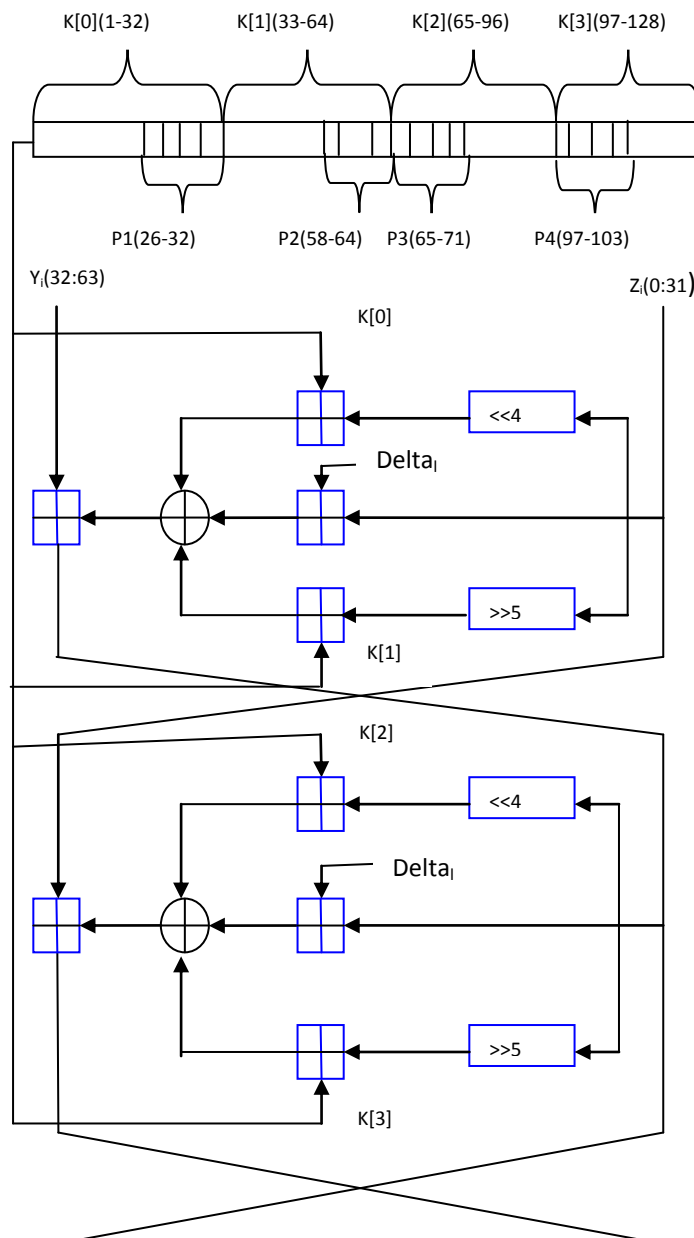
$$\text{delta} = (\sqrt{5} - 1) * 2^{31} = 9\text{E}3779\text{B}9\text{h}$$

$$\text{delta}[l] = (l + 1) * \text{delta}, l = 0, 1, 2, \dots, 31$$

delta is used to ensure that the sub keys are distinct.

As there is a need of 128 bit **key** so we will fixed the 128 bits in the algorithm as all 1's then the key generated through above process is used which is explained below.

Figure 2 New Tiny Encryption Algorithm block diagram



Steps to be followed are:

- The 28 bit (fixed) key which is generated through the process explained above is being converted in binary form. I.e. for above example the decimal number used as key is 21567 whose binary in 28 bit will be 0000000000000101010000111111
- This binary number of 28 bit is divided into four equal halves i.e. P1, P2, P3, P4 (7 bit each).

- P1 and P2 is used in the least significant bit of K1 and K2 and P3 and P4 in the most significant bit of K3 and K4.
- **For example:** K1 part is 32 bit 1's. ie 11111111111111111111111111111111
and we will use P1 as the LSB for K1 then the K1 will be 1111111111111111111111111100111111
- The resulted key blocks of 32 bit is passed and the whole processing of encrypting is done as shown in figure 2.

IV. Conclusion

The main issue in security of data is security of a key .The tiny encryption algorithm also had this weakness regarding security of key. It suffers with the problem of various attacks on key. Our proposed mechanism provides the security of key and hence secures the algorithm by providing different key blocks.

V. Future Work

It can be further extended on heterogeneous network as the above one we proposed is based on homogeneous network.

VI. References

- [1] M. B. Abdelhalim , M. El-Mahallawy , M. Ayyad , A. Elhennawy , Design & Implementation of an Encryption Algorithm for use in RFID System , International Journal of RFID Security and Cryptography (IJRFIDSC), Volume 1, Issues 1/2, March/June 2012
- [2] Mamatha. T , Network Security for MANETS International Journal of Soft Computing and Engineering (IJSCE) , Volume-2, Issue-2, May 2012
- [3] Shushan Zhao, Akshai Aggarwal , Richard Frost, Xiaole Bai , A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks , IEEE communications surveys & tutorials, vol. 14, No. 2, Second Quarter 2012
- [4] Lu Li, Ze Wang, Wenju Liu and Yunlong , A Certificate less Key Management Scheme in Mobile Ad Hoc Networks , 2011 IEEE
- [5] A.Rajaram , Dr.S.Palaniswam, A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks , International Journal of Computer Science Issues, Vol. 7, Issue 4, No 5, July 2010
- [6] Eduardo Da Silva , Aldri L. Dos Santos, Andluz Carlos P. Albini , Identity based key management in mobile adhoc networks and applications, IEEE Wireless Communications • October 2008
- [7] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," CRYPTO'84, LNCS, 1985,
- [8] Anindo Mukherjee, Hongmei Deng, Dharma Agrawal , Distributed Pair wise Key Generation Using Shared Polynomials for Wireless Ad Hoc Networks , Centre of Distributed And Mobile Computing, University Of Cincinnati, Cincinnati
- [9] Li Wang, Jiu Hui Zhang " Security Strategy of MANET Based on Identity- Based Cryptosystems" 2010 IEEE
- [10] XU Xiao-long XIONG Jing-Yi, CHENG Chun-Ling "The Model and the Security Mechanism of the Information Retrieval System based on Mobile Multi- Agent" 2010 IEEE
- [11] Derek Williams , The Tiny Encryption Algorithm (TEA) CPSC 6128 – Network Security Columbus State University April 26, 2008
- [12] A. V. Reddy, "A Cryptanalysis of the Tiny Encryption Algorithm", Master of Science, Department of Computer Science in the Graduate School, The university of Alabama, 2003.
- [13] Pradeep Kumar, A. K. Vatsa, (2011) "Novel Security Architecture and Mechanism for Identity based Information Retrieval System in MANET", International Journal of Mobile Adhoc Network, Vol.1,No.3.