Non Path-based Mutual Anonymity Approach with Secure Cipher Text to Image Encryption Message-Peer-to-Peer Systems

Abdul Majid, PhD
Research Scholar
Bhagwant University
Ajmer Rajasthan India

Amit Chaturvadi
HOD of MCA
Government Engineering College
Ajmer Rajasthan India

ABSTRACT
In Anonymous peer to peer system regularly incurred extra expenses if wants to do perfect transfer. Last node always tries to copy itself when they receive the information and privacy consideration for the entire user kept in consideration. The transmission of secure data in peer to peer system is major issue in current scenario. To ensure the security in the peer to peer system there are many techniques and algorithm were evolved his cryptograph techniques are most powerful. In the existing models the path based, unstructured with dummy traffic to confuse the attacker. The plain texts convert to cipher text in the existing models. The attackers are easy track the cipher text and this is not secure form. Propose Rumor Riding, a novel approach for nodes in P2P systems with a more secure data, cipher text to Image format which is more secure and protect data from unauthorized users. In this scheme block cipher using substitution method that encrypts the given text into blocks. In this paper, the user given plain text is dividing into blocks that are referred to the AES Rijndael Encryption process, converted to unreadable format. Each and every character of the block shifted into ASCII value and from this ASCII value formulated into equivalent color code. Finally this cipher text which encrypted is become the Image format this give the more enrichment to the data. After become image, now applying Random walk mechanism for lower overhead systems, by using the symmetric cryptographic algorithm. Dummy traffic generation will be used to hide the actual image encrypted data to confuse the attackers and accelerating query speed. Dummy traffic generates traffic in a similar message with Image encrypted format and key to confuse the attacker. Evaluation is done by using anonymity approaches AES Rijndael. show the effective by simulations driven this protocol is very effective and efficient than previous protocols and this is illustrated with the experimental and analytical results.

Keywords
Dummy traffic; Query Speed; non path based; random walk; peer-to-peer; Block cipher, Color Substitution, AES Rijndael Algorithm.

1. INTRODUCTION
Napster, Gnutella, and Bit Torrent are working on the Peer-To-Peer network which become very important media for information broadcasting and sharing over the Internet. There are number of methods that have been proposed to provide anonymity [1], [2], [3], [4].

Many methods reach anonymous message delivery through non traceable paths. These methods are called path-based approaches and users create a anonymous path before Transmission. These path based protocol had strong anonymity and it would pre-constructed which require collecting a large number of IP addresses and public keys by the initiator.

The initiator uses asymmetric key such as RSA[5],wrapping layer- encrypted packets. When a single node leave the peer , whole path will be failed then very difficult to identify by the initiator in the dynamic P2P system. Then again there are more attacker will try to attack the message which it encrypted in to cipher text. Considering the above issue propose anonymous P2P protocol called Rumor Riding on non-path based, here initiator initiate the encrypted message query by using asymmetric key and send along with image encrypted to different neighbors.

These two (Key and image encrypted) take random walks separately in the system and this separate walk is called a Rumor. The random walks by the image encrypted and key will meet at some peers together and this peer has authority to recover the original query message.its called Sower word for the agent peer. The same procedure using during the response, i.e. File Delivery process and Confirmation query.

Lets us discuss the cryptography techniques for example microdots, merging words with images, today's scenario, cryptography is most often associated with scrambling plaintext into cipher text (encryption) then back again (decryption). In the security issue the large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data [10, 2, and 4].

There are two types of operation used for converting plaintext to cipher text. Again all most all encryption algorithms having two general principals. First is substitution and transposition. In the substitution method plaintext such as bit, letter, group of bits of letters is mapped in to another element.

In the transposition all elements with plaintext are rearranged. This is called product systems which involve multiple stage of these substitution and transposition [6]. A cipher block put the input multiple blocks and each of this block which producing an output block for each input block. these convert into output block one at a time and its goes on.[3]

Encryption packet and path –based protocol provide strong anonymity and going to face following problems.

2. LITERATURE SURVEY
The Path-based anonymous delivery the message with multicast: Chaum[4] discuss with many approaches that support anonymous communications.

This approaches two categories: path-based anonymous

delivery and anonymous multicast. Onion Routing [7].Tor (Second generation)[8]. In this approach are most popular – based protocols with effective anonymity.

APFS[9] initiator anonymous protocols like Onion Routing to provide responder anonymity in P2P systems. Crowds [1] create random forwarding mechanism to intermediate nodes. Packet receives by the peer its have two option first one is packet forwarding randomly selected peer second is directly sending it to destination peer.

In the unstructured P2P systems, its search randomly and in this work attempt to search scalable and reduce the network traffic.

Gkantsidis et al[12] go thoroughly properties of random walk via statistical method and reveal some factor for improving the system performance.

Bisnik et al.[3] uses mathematical model to analyze the performance of ramdom walk and develop an adaptive algorithm to low the search overload.

Ahmed Abusukhon. Mohammad Talib and Maher A Nabulsi show the efficiency of text to image encryption algorithm analyses. And proposed a novel data encryption algorithm (TTIE), which give the text is encrypted into an image. every letter from the plaintext is encrypted into one pixel[2].

Sourabh Singh , anurag Jain, their use the new novel technique using RGB Substitution and AES algorithm. In this method Secret key is smartly sent along with cipher text in a single transmission and from this technique its solve the exchange problem that generally arises in most of the encryption models.

3. EXISTING SYSTEM

Napster, Guntella and Bit Torrent mandatory media for information sharing dissemination over the Internet this types of network called the P2P network. The plain-text query message and go along with direct downloading and this behavior facing the problem when it going to traced on non-anonymous P2P users.

In the present scenario of P2P applications it uses both content requests and providers the requirement of anonymity increasing. When sending the message via non-traceable path with several anonymous proxies or middle agent peers by most of them before transmission user usually need. This approach called as path-based approaches.

Initiator before sending the data to the other side , the data is pre-wrapped in layer-encryption packet and path –based protocol provide strong anonymity and going to face following problems.

Disadvantage

- Many addresses of IP with public Keys require in advance for the user who gong to create the pre-construction of paths. For to prepare and collection of both incur high cost.
- The initiators update periodically middle node for anonymous paths.

And for the creating of cipher text to image encrypted message there are several method all ready exist many algorithm and method now lets us discuss the some method with encryption and decryption procedure in Rumor Riding method.

Symmetric Key Encryption

A block cipher is uses as the input, a key and then the output block will be same in size in the symmetric key encryption. This will takes place in two modes one is block ciphers next is stream ciphers. In the block cipher mode ,Here whole data is divided into number of block. And based on the block length key is provided for encryption.

Substitution Algorithm

There exists two form of encryption namely first one substitution and the second transposition.

Substitution method where one character will be exchanged for the character, and vice versa at the decryption end.

Substitution algorithms have many formats example monoalphabetic substitution, polyalphabetic substitution, vigenere cipher, playfair cipher

etc.,

In a monoalphabetic cipher, substitution rule are same for every character position.

In a polyalphabetic cipher, the substitution rule changes continuously from one character position to the next according to the elements of the encryption key.

4. PROPOSED SYSTEM

Proposed RR system anonymous in which the paths automatically constructed through the rumors random walks. Initiator and responders should worry about the construction and maintenance of the paths.

Key rumor and image encryption are the two important point of this protocol to achieve mutual anonymity and meet the design objective.

4.1 The Proposed Algorithm and Example

The main intention of this proposed algorithm to present an innovative cryptographic Substitution method. can generate stronger cipher then the existing substitution algorithms.

Proposed Algorithm

The proposed algorithm works as follows:

Step1: input text will be read which is going to encrypted.

Step2: Use AES Rijndael encryption algorithm for this encrypted input text. From this output will obtain.

Step3: the cipher block will be divided into a length of 3 characters per block for encrypted unreadable format.

Step4: this block will be replace with 3 color codes R,G,B for each pixel within the block.

The procedure for block substitution.

Consider a block which is consisting of combination of three characters. Then it separate in to block again convert into corresponding color code through this get a single pixel. This process will be repeated till get full plaintext convert to pixel. Now get pixel to draw a 512 X 512 image.

Step1: draw row wise 512 pixel , then draw row wise pixel continuously until the final row of the block is reached. Now the final input text converted into unintelligible form image. This method called substitution method.. as shown in the figure. 1.

Example:

encryption – 101,110,99,114,121,112,116,105,111,110.

Convert into block cipher, 3 characters per block

101, 110, 99 - RGB (101, 110, 99) = 

114,121,112 - RGB (114,121,112) = 

116,105,111 - RGB (101, 0,0) = 

110, 0, 0 – RGB (110, 0, 0) = 

Figure 1: converting cipher block.

Process of text encrypted into image and decrypted the image into text file.

Encryption Algorithm

Hello Friends = Hel lo Fri end s

Step 1: Read each block and get the equivalent ASCII Value.

Hel =
72,101,108
. lo =
108,111,0.
Fri =
70,114,105
.
End=101,1
10,100. s =
115,0,0.

Now each block as pixel. In a block first value as Red, second value as Green and third value as Blue.

Step 3: Write it as an image.

Decryption Algorithm

Step 1: for first pixel if want to get Read the encrypted image.

Step 2: Read each pixel.

Example: First pixel has

Red = 72, Green = 101, Blue
= 108 72 = H, 101 =e, 108
=l.
Second Pixel.

Red = 108, Green = 110, Blue =
(Space) 32 108 = p, 110 =o, 32 =
(Space)

Third Pixel.

Red =70, Green = 114, Blue
= 114 70 = F, 114 = r , 105
=i.

Fourth Pixel.

Red = 101, Green = 110, Blue
= 100. 101 =e, 110= n, 100 =
d.

Fifth Pixel.

Red = 115, Green = 0,
Blue = 0 115 = s, 0 =
NULL, 0 = NULL

To combine all the characters get our original Plain text “Hello Friends”.

5. RUMOR GENERATION AND RECOVERY

Here, using the Rajindael AES algorithm to encrypt the original Image message. The size of key is 128-bits to take action on the pair of Image Encrypted message and key Rumor hits, and then apply a Cyclic Redundancy Check (CRC).

Now used the CRC value CRC (M) to the Image encrypted Message M.

The Sower, Sa ,who receive the Key and Image Encrypted Rumor to Decrypt by AES Rajindael algorithm Cryptosystem to recover the image encrypted Message MI and the checksum CRC (MI), then apply the CRC function to recover MI and compare the result with CRC (MI), if the result matched, the Sower, Sa ,now the Sower assume that the Message M Successfully Recovered.

Query Issuance:

The Initiator _I‘ desire to send the anonymous query, it will create content _q‘ to request for some services example for some file. The Initiator generates two pairs of asymmetric

keys:

- Private Key KI-
- Public key KI+

The query _q‘ create a requested service with Initiator public key KI+. The Initiator want the number of feedbacks, then tag the request before sending. By using the Rijndael AES

Algorithm cryptosystem the node _I‘ encrypt the query _q‘ and its public key KI+ into Image Encrypted pair (C1,C2). To decrypt the two Image Encrypted pair (C1,C2), the initiator prepare public value _p‘ and private key _K‘ as a key pair (p,x) into two query rumors, _qk‘ and _qc‘. IDqk and IDqc are the two random number strings used as two rumors labels. The rumor message forwarded to two randomly selected neighbors. After generating _I‘, they together start their own random walk

(Image encrypted rumor and key rumor).
RR would going to maintain Local Cache for each and every node to store the received rumors. It performed all the procedure for Image Encrypted Message in all cached when it receive the rumor. The Image Encrypted message and CRC value are matched and then it decrypt the rumor recovered successfully. First consider that its value matched or not, transitional node decrease the TTL value of received rumor. It store this evidence temporary which consisting the ID of rumor in local cache and move towards to a randomly selected neighbor. To confuse the attacker this process is used and no one will suspect that current node is a rumor.

TTL value of rumor become to zero the process is going up, and this process will be same when Image Encrypted rumor query received. If the rumor query pair reach not to exacting note now further node recover would be a unique _q' because there is no particular sequence.

The main issue is that they select at least one pair of rumor and its initial TTL value care fully along with key and Image encrypted Message meets. While sending in to Hops, first the RR initialized non-zero positive number w(1<w<127). The undersized number in between 7 and 10 is enough to confuse to

attacker who could try to determine the location of the initiator. For Example the length of rumor

walks is L and L + W is TTL value.

Sower

The Sower Sa randomly select its most trusted agent called subset St to the send the request. Here it will select one rumor pair, initial TTL values and number of rumors along with key and image encrypted Message meet. Now Sower agent change the value of TTL and Hop count and then prepare a query send to get feedback from a subset trusted agent St. Sower Sa now attach the original query Image Encrypted message qc plus _I' and public key KI+ called Image encrypted message pair (C1,C2). Qk (p,x) and tag request with a label IDsk and IDsk respectively plus its address in a cipher text and plaintext. This act is very useful to avoid invisible flooding.

Query Response

After request, now responding in a group which can hide their identities by sending all message to same address by using the Rijndael AES algorithm cryptosystem. When certain group of

Recipients agree on one value of _p'. these values to calculate their various secret generator _g' corresponding to their private key and this publishes a various multiple public keys using it. Sower and initiator will not having good responder with public key support

Target node St (Subset) has a copy of the file that requested from receiving node and it willing to responder to the node, called the responder. Query message that will copy that will release the message to continue its random walk.

Before its going to send the RR will going to create a non –zero positive number w(1<w<127) in the hops rumors fileds. Now the number 7 and 10 or 8 and 11, or 9 and 12 these value are enough to confuse the attacker who try to always looking into location of the initiator The marked Cr1 and Cr2 are two confirm numbers which will back Lsk and Lsc path to Sower Sa. This Sower will flood in group of two Image encrypted message. To decrypt the image encrypted message, only guinea responder will able to do this because it possesses the corresponding private key.

Now the value of _x' will be calculate by Responder with corresponding its private key to generator _g'.

Preparation for Response _R'as follows: Start with two responders:

- rk public key pair (p,g,x)
- rc image encrypted response with initiator public key KI+.

Through TCP connection It sends rk and rc back to Sower Agent Sa. The Responder will be

never show or revealing its identity due to most power of the generator _g'.

when sower agent will receive the reply rk and rc, then it will send to the original peers of _qc' and _qk'. The Lqk and Lqc reach at I, To confuse the attacker , the initiator _I' will copy the received one of rk and rc and vthat will added few count before sending them out randomly to two different recipients.

Using this private KI+, the two responder rumor _I' will going to get the original response message.

Query Confirm:

The Initiator _I' will provide to use the responder public key to encrypt the confirm message _C' forming two Image

Encrypted Message (C1,C2). Now the initialize by the initiator with positive number that is non zero W(1<W<127) in rumor hops field to confuse the attacker again a small number between 9 and 12.

E. File Delivery

Using the private key by the responder and _R' will encrypt the file with initiator public key t get data image encrypt message rumor divided in to to (C1,C2) and (e,y) and labeled Dc1 and Dc2 when the confirm message is received. There are number of Algorithm is there for example Raindae AES Cryptosystem. To perform for decryption the initiator keys are generator using above method form this the integrating check will be perform. Now the from this the TCP connection the _R'.will send two image encrypted message to Sower Sa.

6. CONCLUSIONS

New approach is employed with non –path –based mutual anonymity protocol for P2P systems, rumor riding (RR) ,in this paper try to create a Image encrypted message. through that a new approach can be emerge with more secure format from image to video encrypted message, attacker on initiator, sower, responder in the image encryption.

7. REFERENCES

[1] M.K. Reiter and A.D. Rubin, "Crowds: Anonymity for WebTransactions," ACM Trans. Information and System Security,vol.1, no. 1, pp. 66-92, Nov. 1998.

[2] L. Xiao, Z. Xu, and X. Zhang, "Low-Cost and Reliable MutualAnonymity Protocols in Peer-to-Peer Networks," IEEE Trans.

[3] D. Chaum, "Untraceable Electronic Mail Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-90, Feb. 1981.

[4] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[5] M.K. Wright, M. Adler, B.N. Levine, and C. Shields, "The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems," ACM Trans. Information and System Security, vol. 7, no. 4, pp. 489-522, Nov. 2004.

[6] D. Goldschlag, M. Reed, and P. Syverson, "Onion Routing,"Comm. ACM, vol. 42, no. 2, p. 39, 1999.

[7] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The Second-Generation Onion Router,"Proc. 13th

USENIX Security Symp., pp. 303-320, 2004.

[8] V. Scarlata, B.N. , B.N. Levine, and C. Shields, "Responder Anonymity and Anonymous Peer-to-Peer File Sharing," Proc. IEEE Int'l Conf. Network Protocols (ICNP), pp. 272-280, Nov. 2001.

[9] Q.Lv, P.Cao, E.Cohen, K.Li, and S. Shenker, "Search and Replication in Unstructured Peer-to-Peer Networks," Proc. 16thACM Int'l Conf. upercomputing, pp. 84-95, 2002.

[10] L.A.Adamic, R.M.Lukose, A.R.Puniyani, and B.A. Huberman, "Search in Power-Law Networks," Physical Rev. E., vol. 64,p. 046135, 2001.

[11] C.Gkantsidis, M.Mihail, and A.Saberi, "Random Walks in Peer-to-Peer Networks," Proc. IEEE INFOCOM, 2004.

[12] N. Bisnik and A. Abouzeid, "Modeling and Analysis of Random Walk Search Algorithms in P2P Networks," Proc. Second in p2p Systems, 2005.

[13] A.Abusukhon, and M. Talib, "A Novel network security algorithm based on Private Key Encryption". In Proceeding of The International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec12), 2012.

[14] Ahmad Abusukhon, Mohammad Talib and Maher A. Nabulsi, "Analysing the efficiency of Text to image encryption algorithm" , in International Journal of Advanced Computer Science and Applications, Vol. 3, No. 11, 2012, pp-35 – 38.

[15] Behrouz A. Forouzan, "Cryptography and Network Security", Tata McGraw-Hill, 2007.

[16] Jawad Ahmad and Fawad Ahmed "Efficiency Analysis and Security Evaluation of Image encryption Schemes", in International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04.

[17] Komal D.Patel and Sonal Belani," Image encryption Using Different Techniques:A Review", in International Journal of Emerging Technology and Advanced engineering, Volume 1, Issue 1, November 2011, pp: 30-34.

[18] Manoj Kumar, "Cryptography & Network Security", 3rd, Krishna Prakashan Media (P) Ltd, 2008.

[19] Mohammad Ali Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm", inIAENG International Journal of Computer Science, 35, 2008.