DOI 10.29042/2018-3971-3975

Helix Vol. 8(5): 3971- 3975

High Speed Network Anonymity Protocol Using Compression Based Face Change

[1]Aparna S. Jaiswal, [2]Rashmi R. Welekar
[1, 2]Shri Ramdeobaba College of Engineering and Management, Nagpur
Email: aparna.jaiswal90@gmail.com

Received: 09th July 2018, Accepted: 14th August 2018, Published: 31st August 2018

Abstract
The major objective of any data communication system is to securely transmit their digital data between two or more computers in the network. Delay Tolerant Networks were proposed to enable communication by leveraging the store-carry-and-forward mechanism of message transfer. The proposed approach selects the path according to the feasible number of hops needed to reach the corresponding node. The architecture anonymise every node of the network by giving them fake ids which will be their FaceChange_id's. This FaceChange_id is used for communication in the network which enhances the data forwarding security. The data is compressed so as to increase the speed of the system and reduce delay and throughput rate.

Keywords: Face Change, Anonymity, Compression, Unicast, Multicast

Introduction

A Network is a continuously self-configuring, infrastructure network of systems connected to each other with wires. A special form of delay tolerant networks (DTNs). Where nodes side by side communicate with each other via FaceChange_id's generated by hiding their original ID's, a malicious node in system can easily find attack targets from FaceChange_id and launch attacks to decrease the system performance without any loss of data. Then, for ensuring privacy, attacker's nodes can also easily find the transmitting path between nodes for attacks. To generalize this process as useful applications in opportunistic social networks to Face Change logically. Face Change can provide Security extended from the Internet gateway into the whole network. Face Change assigning fake id from its original id. We generate a FaceChange_id with gold code random number generator to hide its original id to transmitting and receiving data in network with correct nodes. Compression is process of reducing the data size. We use for reducing the data transmission speed in network, as data compressed it take less time while data transmission. For secure data transmission, though we use AES algorithm which is a stronger and a more secure encryption standard, which is standard and more likely used. We use AES because it also supports zipping that we use in our system for compression.

Although, in existing anonymous routing system generate a high cost, less data transmission speed in network, loss in data packet during sending and receiving, this type of service in data transmission due to low quality resources may lead to delay in taking operations performing on that data. A system we generate is proposed by the following steps.

1. *File Transfer:* First is transferring file or data in network without packet loss and with security. For providing security we use AES, to safely transmit data in network with encryption while sending and decrypting while receiving data. This is done in network.
2. *Compressing data:* Second in advance we compress the data while transmitting in network so that there is no delay in data transmission, no more throughputs, no data loss, due to which data transmitting speed is increased hence, no delay while transmitting data.
3. *Zipping:* Third, we apply zipping, that is zipEncrypt for data compression, which compress the original data and unzip for decompression the data which decompresses the data in its original form. The use of zipping is to increase the data transmitting speed in network, for no delay in transmission.
4. *Fake attack:* We have also launched a fake attack to ensure the security of our system and also to identify if there are any loopholes in the system.

Our main task is to provide security and privacy for user data. The issue is handling the information of single user and group user securely. In case of loss in any small amount of loss in personal information may increase number of legal and illegal issue regarding privacy. Now a days data is updated, collected daily which is electronically directly on server so it cannot exchange the information of one user to other, so our main task is to provide privacy, In case of FREECHARGE safety example the FREECHARGE (server) has a database with user information and summary of their ordered recharges with FREECHARGE wallet that linked with user account and amount balance, where client poses queries correspond to data where our main block is Provide privacy and security to their data. The paper is structured as follows; we introduce the literature review in section 2. We describe how we do the implementation and proposed work which algorithms we use in our proposed system in section 3. Results of the implemented work in section 4. Conclusion in section 5.

Literature Survey

FaceChange Attaining Neighbor Node Anonymity in Mobile

In this paper work is done on face change, where we change node id with face change id which is in the form of pattern. Face change id is done so that the third party cannot access the confidential information sending from one node to another node in a network. Only the node which has face change id will retrieve the information send from other node. The receiving node identifies the sender node by classifying the pattern. Face change in this used to provide privacy and security to the node. [1]

Dissent Numbers: Making Strong Anonymity Scale

In this paper work done is to making the scale anonymity strong. This works on current prototype, local area network web browsing and wide area network group messaging. To show the use of dissent they use WiNoN system which is virtual machine to identify user browsing OS environment which uniquely identifying the user. For that they use one anonymous micro blogging application and work is done. The micro-blogging prototype system runs on PlanetLab and DeterLab having capacity of managing 2000 to 5000 node. The short messages are send in Dissent protocol with use of HTTP API [2].

Anonymous Communication: Peer-to-Peer Networks

In this paper work done is to provide more privacy and security because main issue in peer-to-peer networks is anonymity. The main purpose is to find attacker. Peer-to-peer network is very important, because it gives vital information about the system to attacker to compromise the networks. Where some common types of attack are *Time-to-Live Attacks, Denial of Service Attacks, Statistical Attacks and Traffic analysis.* The work done is based on dual path paradigm where one is request path and another is response path [3] and one private key use which provides more efficiency.

Privacy and anonymity:

Anonymity is present in the concept of privacy. Anonymity refers to the matters related to the identity. This ensures that the user may use resources and services without leaking their identity. Privacy concerns with user protection against discovery and misuse of identity by other user. First work is done by analyzing threats using all layers of OSI model [5]. The level of privacy is linked with type of encryption method algorithm used. Some algorithm of encryption might use are Public-key cryptography and algorithms such as RSA [6] and DSA [7]. Proxy server, Onion Routing, TOR which are the solutions to protect privacy and anonymity on the web [4].

Proposed Method

System Design of FaceChange

A. System Setup:

As per the system we have to design, the trusted node first generate the parameter that is FaceChange_id used to communicate. Trusted node select the data, encrypt with AES () and apply ZIPPING to compress the data, which is use speedup the transmission securely with encryption and decryption. In addition trusted node has the private key that is Real IDs and public key FaceChange_id's use for the securely transmitting the data. Finally the transmission done securely with the generated parameters and done with following steps:

• Trusted node creates a pair of public/private key (Real_id's, FaceChange_id's) by the same method used by nodes and their Real_id's to other node.

• Trusted node fetches the system parameter and its Real_id and FaceChange_id from other trusted node.

B. Neighbor Node Anonymity in FaceChange:

The node that does not know the Real_id's of the other nodes in the network. To transmit the data from the node to node we generate FaceChange_id for every node. While sending data if any node disconnects and not able to receive the files because of the not proper parameter to receive the data such as real IDs and FaceChange_id's, then the data files are not transferred to receiver node. We cannot able to change the IP address and PORT number through the software, we have to change it every time while the transmission. Therefore, for that we change the node behavior which can further generate it automatically. We later design the FaceChange_id's using FaceChange algorithm to ensure that neighbor node anonymity is preserve in these processes.

Advanced Encryption Standards:

- Compared to DES, AES is stronger encryption algorithm because in AES 128 bits is applied. The process model of AES is shown in Fig. 1.

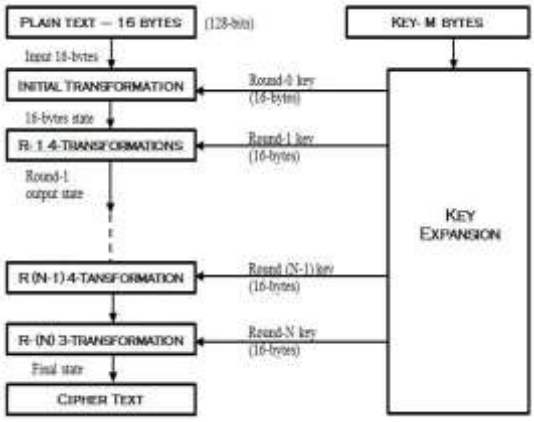

Fig. 1 Process Model of AES

Rounds – In AES the number of rounds is not fixed, it depends on the size of the key i.e. if we are applying a key of 16-bytes then the total number of rounds will be 10; for 24-bytes key there will be 12 rounds whereas for 32-bytes key there will be 14 rounds. One extra round is added i.e. for 16-bytes key there will be total 11 rounds because the rounds starts with round-0.

Key Expansion – In this block key expansion takes place in which the key is divided into 16-bytes before it is applied. Division of key takes place in a block which is of 16-bytes size.

Block – The block consist of 16-bytes and one particular column represents group of words i.e. one column represents one word. So, in one round we apply 4 words. As we said before that we have 11 rounds for 16- bytes of plain text and we are applying 4 words in one round, so our key is totally divided into 44 words. Similarly, if we have 12 rounds then our key will be divided into 52 words.

Transformation – In round-0 the transformation takes place by only applying the key. From round-1 to round (N-1) 4 transformations takes place viz.

(i) Substitution – Here S-box is applied. Suppose we have 4*4 matrixes and having a value $S_{1,1}$ in it. So for substitution of $S_{1,1}$ the algorithm will check co-ordinate value of (x, y) i.e. (1, 1) in S-box and replace the original value $S_{1,1}$ with $S'_{1,1}$ in the new matrix. Hence all the values are substituted by this method and a new Matrix is formed;

(ii) Shifting of Rows – Consider the example of 4*4 matrixes. Here, the 1st row is kept as it is. The 2nd row is shifted by 1 byte. The 3rd row is shifted by 2 bytes, and the 4th row is shifted by 3 bytes;

(iii) Mixing Columns – Here, one particular column is multiplied with a fix value and the resultant values are put in the column. In the same way all the 4 columns are multiplied and we get a new 4*4 matrix;

(iv) Add round key – This is same as explained above for rounds. At the end of every round this step is performed. If this step is not done before the starting of next round then we will not get the security in that particular round. In last round (N) only 3 transformations take place, here, mixing of columns is not used.

After all the process is done, lastly we get the cipher text which is also of 16-bytes.

The decryption process in AES: The rounds which we have applied during the encryption process in the same format we have to go in the reverse direction for decrypting the cipher text.

Results and Discussions

In current methods, when data is send through the network where each node is able to access the data and able to find the node who is sending that data. Here to ensure the privacy, security and high speed transmission of data we are using the keys: Public key and Private key where the node sending the data share information in the network with his private key by applying it publicly so that it can travel among every node in the network and only the node who has that private key can access the data or shared information in the network.

In our system the task we have done is id assignment to the node for exchanging messages or information from one node to another node. For that we are assigning a new id to each node in a network which we called FaceChange_id which is of 20 digit anonymous key generated using gold code random number generator algorithm, FaceChange_id used to anonymise the real id of the node, the only node having correct FaceChange_id is able to send and receive the data travel in the network. While we are sending a data or information from one node to another node, first we have to start the server in the receiving position, when server is on and connection is established using the face change id generated then only the data received at the server side which is other node.

While sending the data from one node to another node the key is generated which contains first eight digit of both the sending node FaceChange_id followed by eight digit of receiving node FaceChange_id for sending the data between sender and receiver, after generating this key only data send in network in encrypted form from one node to another node in the network with the help of this key. For data encryption we use the AES algorithm to encrypt the original data and sending via network to the receiver. Where the receiver node is only able to receive the data if the receiving node has generate a key of its own eight digit FaceChange_id followed by eight digit of sending node FaceChange_id, which gives access for receiver node to receive the data.

The table below shows the result and comparison between the factors that we calculate to show how our system is more efficient than the other. In table below we send the data in the form of byte that is small message, then we send a paragraph in the form of message, then we send image .png file, .docx file, .pdf file and check the efficiency. Then we get the result how efficiently our system generated that output than the previous one. The table below is shown with the parameter's data length, delay and throughput.

Parameters	Data Length		Delay in ms		Throughput in bps	
	Existing System	Proposed System	Existing System	Proposed System	Existing System	Proposed System
Short Message	43	29	2	1	21500	29000
Long Message	241	161	3	1	80333	161000
Image (.png file)	546	386	47	22	11617	17545
Word Document	66	44	19	4	3473	11000
PDF File	297	182	33	9	9000	20222

TABLE I Effectiveness of the Proposed System

The above table shows the Effective results of our proposed system. It shows the comparison between the existing system and the proposed system. The data length is reduced because the data is been send in the compressed form. The delay time is also reduced because of compression and data transmission speed is increased. Due to this decrease in delay time, the throughput rate is increased. This leads to an improved privacy security system.

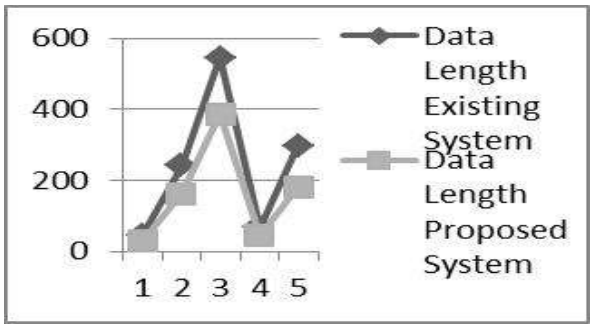

Fig. 2 Analysis of Data Length

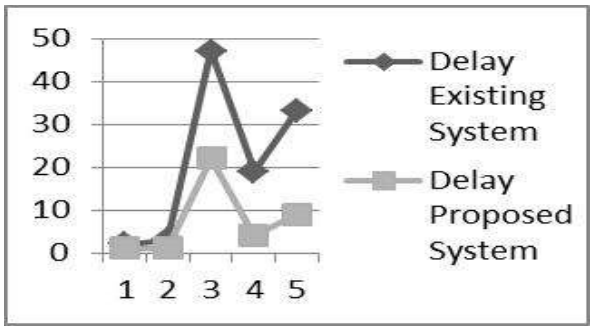

Fig. 3 Analysis of Delay in receiving the data

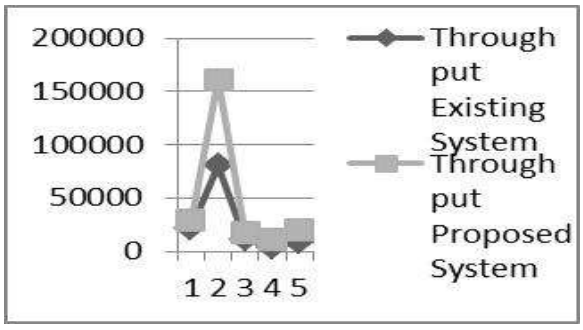

Fig. 4 Analysis of Throughput Rate

Data compression is important. It storage requirements and improve transfer speed over standard connections. Data compression algorithms are capable of breaking down longer string data into shorter ones. And assembling them later using what they retain. The test results of data compression are shown in Fig. 2.

Due to data compression the transferring speed of data is increased. This leads to reduction in delay time. The delay time is calculated by using the below equation and the test results of delay is shown in Fig. 3.

$$Delay = Receveing\ time - Transmission\ time \quad (1)$$

The reduction in delay time leads to the increase in throughput rate. Throughput is calculated using the equation below and the test results are shown in Fig. 4.

$$Throughput = \frac{Data\ Length}{Delay} \quad (2)$$

Conclusion

In this paper, we propose High Speed Network Anonymity Protocol Using Compression Based Face Change, which enables every node to send their confidential information to other nodes without revealing their real ids. The communication takes place with their FaceChange_id's only. Here only the sender node knows the real id of the receiver node to which the data is to be sent and also only the receiver node knows the real id of the owner of the data. We have compressed the data which increases the data forwarding speed and reduces delay and throughput rate.

References

[1] Kang Chen, Member and Haiying Shen, "Face Change: Attaining Neighbor Node Anonymity in Mobile Opportunistic Social Networks With Fine-Grained Control" in *IEEE/ACM Transactions on Networking(TON), vol. 25 issue 2, April 2017.*

[2] David Isaac Wolinsky, Henry Corrigan-Gibbs, and Bryan Ford, "Dissent in Numbers: Making Strong Anonymity Scale" in *10th USENIX Symposium on Operating Systems Design and Implementation (OSDI '12), 2016-04-10.*

[3] Ehsan Saboori and Shahriar Mohammadi, "Anonymous Communication in Peer-to-Peer Networks for Providing more Privacy and Security" in International Journal of Modeling and Optimization, Vol. 2, No. 3, June 2012.

[4] Adrian Yanes, "Privacy and Anonymity" in arXiv preprint arXiv: 1407.0423, 2014

[5] Opportunistic Mobile Networks: Advances and Applications: By Sudip Misra, Barun Kumar Saha, Sujata Pal, Chapter 8.

[6] J. Jonsson and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications", Version 2.1. RFC 3447 (Informational), February 2003.

[7] National Institute of Standards and Technology. FIPS PUB 180-1: Secure Hash Standard. April 1995. Supersedes FIPS PUB 180 1993 May 11.

[8] K. Chen and H. Shen, "Fine-grained encountering information collection under neighbor anonymity in mobile opportunistic social

networks," in Proc. IEEE ICNP, Nov. 2015, pp. 179–188.

[9] K. Chen, H. Shen, and H. Zhang, "Leveraging social networks for p2p content-based file sharing in disconnected MANETs," in IEEE Trans. Mobile Comput., vol. 13, no. 2, pp. 235–249, Feb. 2014.

[10] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on opportunistic forwarding algorithms" IEEE Trans. Mobile Comput., vol. 6, no. 6, pp. 606–620, Jun. 2007.

[11] M. C. Chuah, "Social network aided multicast delivery scheme for human contact-based networks," in Proc.1st Simplex, vol.1, issue 3, Feb. 2009.

[12] V. Conan, J. Leguay, and T. Friedman, "Characterizing pairwise inter-contact patterns in delay tolerant networks," in Proc. 1st Int. Conf. Autonomic Comput. Commun. Syst., Article no. 19, Oct. 2007.

[13] P. Costa, C. Mascolo, M. Musolesi, and G. Picco, "Socially-aware routing for publish-subscribe in delay-tolerant mobile ad-hoc networks" in IEEE J. Sel. Areas Commun., vol. 26, no. 5, pp. 748–760, Jun.2008

[14] Junggab Son, Donghyun Kim, Rahman Tashakkori, Alade O, Tokuta, Heekuck Oh, "A New Mobile Online Social Network Based Location Sharing with Enhanced Privacy Protection" in IEEE Computer Communication and Networks (ICCCN), 25th International Conference, Aug. 2016.

[15] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in delay tolerant networks: A social network perspective," in Proc. ACM MobiHoc, 2009, pp. 299–308.

[16] N. Eagle and A. Pentland, "Reality mining: Sensing complex social systems," in Pers. Ubiquitous Comput., vol. 10, no. 4, pp. 255–268, 2006.

[17] E. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant MANETs," in Proc. ACM MobiHoc, 2007, pp.32–40.

[18] V. Erramilli, A. Chaintreau, M. Crovella, and C. Diot, "Delegation for-warding," in Proc. ACM MobiHoc, 2008, pp. 251–260.

[19] K. Fall, "Delay tolerant network architecture for challenged internets," in *Proc. ACM SIGCOMM, 2003, pp. 27–34.*

[20] L. Freeman, "A set of measures of centrality based on betweenness, Sociometry", in *IEEE vol. 40, no. 1, pp. 35–41, 1977.*

