Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057 OPEN ACCESS 2017 12 (4): 125-131

To Achieve Source Anonymity in Wireless Network Using Network Coding

G. Michael, R. Kavitha

Received: 06 December 2016 ▪ Revised: 09 January 2017 ▪ Accepted: 08 February 2017

Abstract: Wireless networks have been widely deployed in the access network area due to their benefits such as convenience, mobility, and low cost. However, they still suffer from the main critical issues are lack of security and privacy threats. The Existing privacy-preserving techniques such as Onion Routing in which the attackers easy to attack the messages in intermediate nodes. We propose a Network coding based privacy-preserving scheme With homomorphic encryption on Global Encoding Vectors (GEVs). It offers two significant privacy preserving features such as packet flow untraceability and message content confidentiality. Our objective is to achieve source anonymity by preventing traffic analysis and flow tracing attacks. With the employment of HEFs (Homomorphic Encryption Function) to GEVs, the confidentiality of messages is effectively guaranteed which makes difficult for the attackers to recover the GEVs. Even when some intermediate nodes are compromised the adversaries still cannot decrypt the GEVs because we employ message recoding at intermediate nodes based on network coding.

Keywords: Network Coding, Homomorphic Encryption, Huffman Encoding.

INTRODUCTION

Wireless access network, such as Wi-Fi, have been widely deployed due to their convenience, portability and low cost. However, they still suffer inherent shortcomings such as limited radio coverage, poor system reliability, and the main critical issues of lack of security and privacy. Multi hop wireless networks have various kinds of attacks, such as data modification, node compromising, these attacks may have the security of MWNs. In some advanced attacks are traffic analysis and flow tracing, In this paper we focus on privacy issues, i.e., how to prevent the flow tracing and achieve source anonymity in MWNs. Consider the example of multicast communication in adhoc networks, where nodes can communicate with each other through multi hop packet forwarding.

In existing system for privacy preserving solution such as onion routing schemes [1]. Onion routing is the mechanism of the sender and the receiver nodes communicate with each other. The privacy issue from a brand new perspective using network coding to achieve security service.

Network coding was first introduced by Ahlswede. The two techniques are random coding and linear coding. The random coding makes network coding more practical, while the linear coding is proven to be sufficient and computationally efficient for network coding. Compared with conventional packet forwarding technologies, network coding offers by allowing and encouraging coding operation at intermediate forwarders. Some advantages such as potential throughput improvement, transmission energy minimization, and delay reduction.

The network coding in MWNs can not only bring the above performance benefits, but also provide a feasible way to efficiently thwart the traffic analysis/flow tracing attacks since the coding/mixing operation is encouraged at intermediate nodes.

Moreover, the unlink ability between incoming packets and out going packets, which is an important privacy property for preventing traffic analysis/flow tracing, can be achieved by mixing the incoming packets at intermediate nodes.

G. Michael, Associate Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai. E-mail: michaelcse@gmail.com

R. Kavitha, Associate Professor, Department of Computer Science and Engineering, BIST, BIHER, Bharath Institute of Higher Education & Research, Selaiyur, Chennai.

A simple deployment of network coding cannot prevent traffic analysis/flow tracing since the explicit Global Encoding Vectors (GEVs, also known as tags) prefixed to the encoded messages provide a back door for adversaries to compromise the privacy of users. Once enough coded packets are collected, adversaries can easily recover the original packets and then conduct the attacks based on packets. A naive solution to address this vulnerability is to employ link-to-link encryption. This solution can prevent traffic analysis to a certain degree, but it introduces heavy computational overhead and thus results in significant performance degradation of the whole network system. Additionally, it cannot protect the privacy of users once some intermediate nodes are compromised by adversaries. Such deficiencies motivate us to explore an efficient privacy-preserving scheme for MWNs.

In this paper, based on network coding and Homomorphic Encryption Functions (HEFs). we propose an efficient privacy-preserving scheme for MWNs. Our objective is to achieve source anonymity by preventing traffic analysis and flow tracing. The proposed scheme offers the following attractive features:

Efficiency

Due to the Homomorphism of HEFs, message recoding at intermediate nodes can be directly performed on encrypted GEVs and encoded messages, without knowing the decryption keys or performing expensive decryption operations on each incoming packet.

High Invertible Probability

Linear network coding with huffman encoding algorithm are invertible with high probability. Theoretical analysis demonstrates that the influence of HEFs on the invertible probability of GEVs is negligible. Thus the random coding feature can be kept in our network coding based privacy-preservation scheme.

PRELIMINARIES

A) Network Coding

Network coding allows intermediate nodes to perform computation on incoming messages, making outgoing messages be the mixture of incoming ones. Network coding is a techinique, where instead of simply relaying the packets of information they receive, the node of a network will take several packets and combine them together for transmission. This can be used to attain the maximum possible information flow in a network. Network coding is a field of information theory and coding theory.

B) Homomorphic Encryption Function

We used the homomorphic encryption function is highly efficiency and securable. In the Commander process, we using this for each packet encryption .Due to the Homomorphism of HEFs, message recoding at intermediate nodes can be directly performed on encrypted and encoded messages, without knowing the decryption keys or performing expensive decryption operations on each incoming packet. The performance evaluation on computational complexity demonstrates the efficiency of the proposed scheme.

Homomorphic Encryption Functions (HEFs) have the property of homomorphism, which means operations on plaintext can be performed by operating on corresponding cipher text. It allow the complex mathematical operation to be performed on encrypted data without compromising the encryption. To offer confidentiality for the tags employment of homomorphic Encryption functions (HEFs) is used for making it difficult for attackers to recover the plaintext.

C) Thread Models

We consider the following two attack models.

Outside attacker: An outside attacker can examine the tags and message content, and thus link outgoing packets with incoming packets. Further, even if end-to-end encryption is applied to messages at a higher layer, it is still possible for a global outside attacker to trace packets by analyzing and comparing the message ciphertext.

Inside attacker: An inside attacker may compromise several intermediate nodes. Link-to link encryption is vulnerable to inside attackers since they may already have obtained the decryption keys and thus the message plaintext can be easily recovered. Both inside and outside attackers may perform more advanced traffic analysis/flow tracing techniques, including size correlation, time correlation, and message content correlation. Adversaries can further explore these techniques to deduce the forwarding paths and thus to compromise user**.**

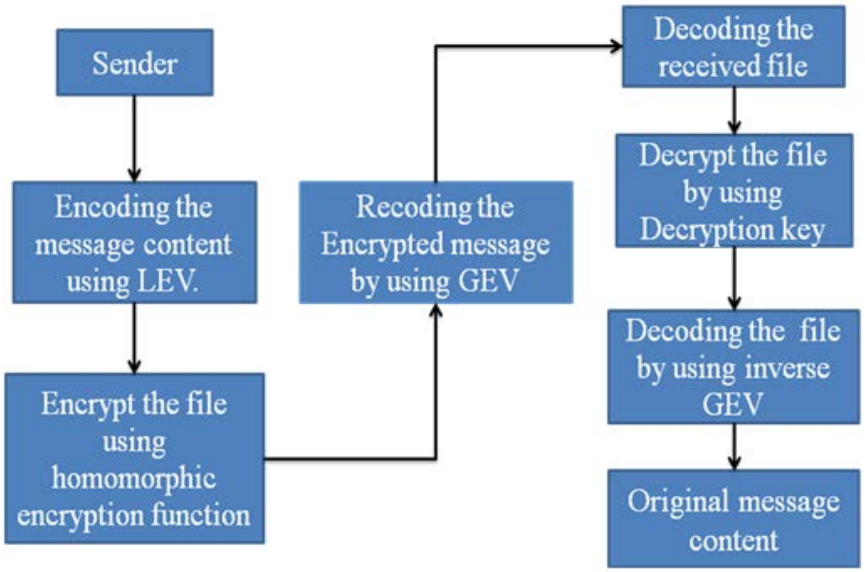
RELATED WORK

Several privacy-preserving schemes have been proposed, Onion-based schemes include Onion Routing and Onion Ring. The common feature of these schemes is to chain onion routers together to forward messages hop by hop to the intended recipient. Therefore, every intermediate onion router knows only about the router directly in front of and behind itself, respectively, which can protect user privacy if one or even several intermediate onion routers are compromised.

Network coding has privacy-preserving features, such as shaping, buffering, and mixing. However, network coding suffers from two primary types of attacks, pollution attacks and entropy attacks. Pollution attacks can be launched by un trusted nodes or adversaries through injecting faked messages or modifying authentic messages, which are fatal to the whole network due to the rapid propagation of pollution.

In entropy attacks, adversaries forge non-innovative packets that are linear combinations of "stale" ones, thus reducing the overall network throughput. A new network coding security model and a construction of secure linear network code with huffman encoding are proposed.

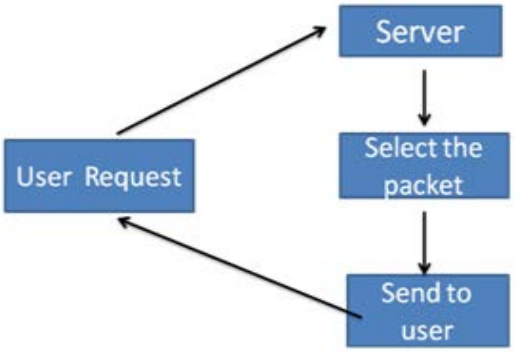
SYSTEM ARCHITECTURE



The Proposed Privacy Preservation Scheme

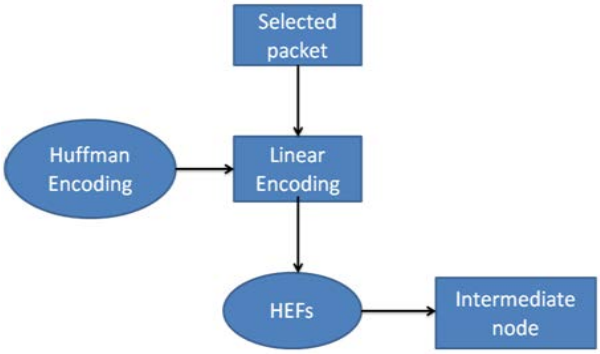
1) User Login

The user can send request to the server and the server can select the packet and send to the client.



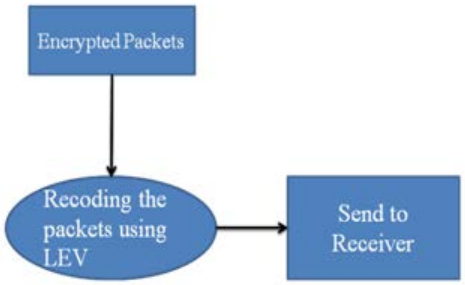
2) Homomorphic Encryption

In this module first perform the linear encoding by using Huffman Encoding algorithm. To offer confidentiality for the tags employment of homomorphic Encryption functions (HEFs) is used for making it difficult for attackers to recover the plaintext. We used the homomorphic encryption function is highly efficiency and securable. It allow the complex mathematical operation to be performed on encrypted data without compromising the encryption.



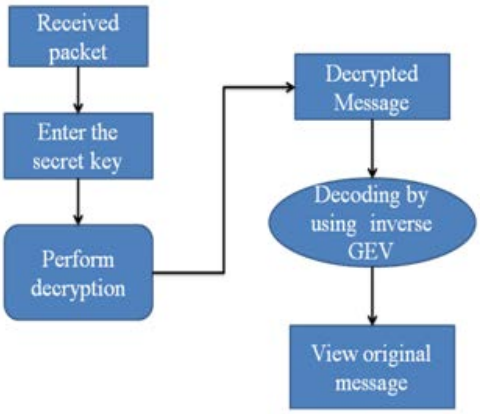
3) Intermediate Recoding

After receiving the number of packets an intermediate node can perform random linear coding using huffman encoding on this packets. Due to the Homomorphism of HEFs, message recoding at intermediate nodes can be directly performed on encrypted and encoded messages**.** Intermediate node has no knowledge of the corresponding decryption keys, it is difficult for the intermediate node to perform functions such as earliest decoding to get the original message content. However, due to the homomorphism of the encryption function, a linear transformation can be directly performed on the encrypted tags of the incoming packets to generate a new tag for the outgoing packet



4) Enhanced Privacy against Traffic Analysis and Flow Tracing

The confidentiality of GEVs further brings the implicative benefit of the confidentiality of message content. Message decoding is only possible by using inverse GEV. With the employment of HEFs, the confidentiality of GEVs is effectively guaranteed, making it difficult for attackers to recover the plaintext. Unlike other packet-forwarding systems, network coding allows intermediate nodes to perform computation on incoming messages, making outgoing messages be the mixture of incoming ones. Flow tracing in the sense of the report about the alerting sensor.



SECURITY ANALYSIS

The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis. Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or re-established for each new generation.

CONCULSION

In this paper, we have proposed an achieving security services for wireless network using network coding. With the light weight homomorphic encryption on Global Encoding Vector (GEVs), the proposed scheme offers two significant privacy-preserving features, packet flow untraceability and message content confidentiality. Moreover, the intermediate recoding further improve the privacy preservation and efficiency of the proposed scheme.

REFERENCES

[1] Das, J., Das, M. P., & Velusamy, P. (2013). Sesbania grandiflora leaf extract mediated green synthesis of antibacterial silver nanoparticles against selected human pathogens. *Spectrochimica Acta Part A: Molecular and Biomolecular Spectroscopy*, *104*, 265-270.

[2] Umanath, K.P.S.S.K., Palanikumar, K., & Selvamani, S. T. (2013). Analysis of dry sliding wear behaviour of Al6061/SiC/Al2O3 hybrid metal matrix composites. *Composites Part B: Engineering*, *53*, 159-168.

[3] Udayakumar, R., Khanaa, V., Saravanan, T., & Saritha, G. (1786). Cross layer optimization for wireless network (WIMAX). *Middle-East Journal of Scientific Research*, *16*(12), 1786-1789.

[4] Kumaravel, A., & Rangarajan, K. (2013). Algorithm for automaton specification for exploring dynamic labyrinths. *Indian Journal of Science and Technology*, *6*(5S), 4554-4559.

[5] Pieger, S., Salman, A., & Bidra, A.S. (2014). Clinical outcomes of lithium disilicate single crowns and partial fixed dental prostheses: a systematic review. *The Journal of prosthetic dentistry*, *112*(1), 22-30.

[6] Vijayaraghavan, K., Nalini, S.K., Prakash, N.U., & Madhankumar, D. (2012). One step green synthesis of silver nano/microparticles using extracts of Trachyspermum ammi and Papaver somniferum. *Colloids and Surfaces B: Biointerfaces*, *94*, 114-117.

[7] Khanaa, V., Mohanta, K., & Satheesh, B. (2013). Comparative study of uwb communications over fiber using direct and external modulations. *Indian Journal of Science and Technology*, *6*(6), 4845-4847.

[8] Khanaa, V., Thooyamani, K. P., & Udayakumar, R. (1798). Cognitive radio based network for ISM band real time embedded system. *Middle-East Journal of Scientific Research*, *16*(12), 1798-1800.

[9] Vijayaraghavan, K., Nalini, S.K., Prakash, N.U., & Madhankumar, D. (2012). Biomimetic synthesis of silver nanoparticles by aqueous extract of Syzygium aromaticum. *Materials Letters*, *75*, 33-35

[10] Caroline, M.L., Sankar, R., Indirani, R.M., & Vasudevan, S. (2009). Growth, optical, thermal and dielectric studies of an amino acid organic nonlinear optical material: l-Alanine. *Materials Chemistry and Physics*, *114*(1), 490-494.

[11] Kumaravel, A., & Pradeepa, R. (2013). Efficient molecule reduction for drug design by intelligent search methods. *International Journal of Pharma and Bio Sciences*, *4*(2), B1023-B1029.

[12] Kaviyarasu, K., Manikandan, E., Kennedy, J., Jayachandran, M., Ladchumananandasiivam, R., De Gomes, U. U., & Maaza, M. (2016). Synthesis and characterization studies of NiO nanorods for enhancing solar cell efficiency using photon upconversion materials. *Ceramics International*, *42*(7), 8385-8394.

[13] Sengottuvel, P., Satishkumar, S., & Dinakaran, D. (2013). Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling. *Procedia Engineering*, *64*, 1069-1078.

[14] Anbuselvi S., Chellaram, C., Jonesh S., Jayanthi L., & Edward J.K.P. (2009). Bioactive potential of coral associated gastropod, Trochus tentorium of Gulf of Mannar, Southeastern India. *J. Med. Sci,* 9(5), 240-244.

[15] Kaviyarasu, K., Ayeshamariam, A., Manikandan, E., Kennedy, J., Ladchumananandasivam, R., Gomes, U. U., & Maaza, M. (2016). Solution processing of CuSe quantum dots: Photocatalytic activity under RhB for UV and visible-light solar irradiation. *Materials Science and Engineering: B*, *210*, 1-9.

[16] Kumaravel, A., & Udayakumar, R. (2013). Web portal visits patterns predicted by intuitionistic fuzzy approach. *Indian Journal of Science and Technology*, *6*(5S), 4549-4553.

[17] Srinivasan, V., & Saravanan, T. (2013). Reformation and market design of power sector. *Middle-East Journal of Scientific Research*, *16*(12), 1763-1767.

[18] Kaviyarasu, K., Manikandan, E., Kennedy, J., & Maaza, M. (2015). A comparative study on the morphological features of highly ordered MgO: AgO nanocube arrays prepared via a hydrothermal method. *RSC Advances*, *5*(100), 82421-82428.

[19] Kumaravel, A., & Udhayakumarapandian, D. (2013). Consruction of meta classifiers for apple scab infections. *International Journal of Pharma and Bio Sciences*, *4*(4), B1207-B1213.

[20] Sankari, S. L., Masthan, K. M. K., Babu, N. A., Bhattacharjee, T., & Elumalai, M. (2012). Apoptosis in cancer-an update. *Asian Pacific journal of cancer prevention*, *13*(10), 4873-4878

[21] Harish, B. N., & Menezes, G. A. (2011). Antimicrobial resistance in typhoidal salmonellae. *Indian journal of medical microbiology*, *29*(3), 223-229.

[22] Manikandan, A., Manikandan, E., Meenatchi, B., Vadivel, S., Jaganathan, S. K., Ladchumanananandasivam, R., & Aanand, J. S. (2017). Rare earth element (REE) lanthanum doped zinc oxide (La: ZnO) nanomaterials: synthesis structural optical and antibacterial studies. *Journal of Alloys and Compounds*, *723*, 1155-1161.

[23] Caroline, M. L., & Vasudevan, S. (2008). Growth and characterization of an organic nonlinear optical material: L-alanine alaninium nitrate. *Materials Letters*, *62*(15), 2245-2248.

[24] Saravanan T., Srinivasan V., Udayakumar R. (2013). A approach for visualization of atherosclerosis in coronary artery, Middle - East Journal of Scientific Research, 18(12), 1713-1717.

[25] Poongothai, S., Ilavarasan, R., & Karrunakaran, C.M. (2010). Simultaneous and accurate determination of vitamins B1, B6, B12 and alpha-lipoic acid in multivitamin capsule by reverse-phase high performance liquid chromatographic method. *International Journal of Pharmacy and Pharmaceutical Sciences*, *2*(4), 133-139.

[26] Udayakumar, R., Khanaa, V., & Saravanan, T. (2013). Synthesis and structural characterization of thin films of SnO 2 prepared by spray pyrolysis technique. *Indian Journal of Science and Technology*, *6*(6), 4754-4757

[27] Anbazhagan, R., Satheesh, B., & Gopalakrishnan, K. (2013). Mathematical modeling and simulation of modern cars in the role of stability analysis. *Indian Journal of Science and Technology*, *6*(5S), 4633-4641.

[28] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of bis thiourea cadmium iodide: A semiorganic single crystal. *Materials Chemistry and Physics*, *113*(2-3), 670-674.

[29] Sharmila, S., Jeyanthi Rebecca, L., & Das, M. P. (2012). Production of Biodiesel from Chaetomorpha antennina and Gracilaria corticata. *Journal of Chemical and Pharmaceutical Research*, *4*(11), 4870-4874.

[30] Thooyamani, K.P., Khanaa, V., & Udayakumar, R. (2013). An integrated agent system for e-mail coordination using jade. *Indian Journal of Science and Technology*, *6*(6), 4758-4761.

[31] Caroline, M. L., Kandasamy, A., Mohan, R., & Vasudevan, S. (2009). Growth and characterization of dichlorobis l-proline Zn (II): A semiorganic nonlinear optical single crystal. *Journal of Crystal Growth*, *311*(4), 1161-1165.

[32] Caroline, M.L., & Vasudevan, S. (2009). Growth and characterization of L-phenylalanine nitric acid, a new organic nonlinear optical material. *Materials Letters*, *63*(1), 41-44.

[33] Kaviyarasu, K., Xolile Fuku, Genene T. Mola, E. Manikandan, J. Kennedy, and M. Maaza. Photoluminescence of well-aligned ZnO doped CeO2 nanoplatelets by a solvothermal route. *Materials Letters*, *183*(2016), 351-354.

[34] Saravanan, T., & Saritha, G. (2013). Buck converter with a variable number of predictive current distributing method. *Indian Journal of Science and Technology*, *6*(5S), 4583-4588.

[35] Parthasarathy, R., Ilavarasan, R., & Karrunakaran, C. M. (2009). Antidiabetic activity of Thespesia Populnea bark and leaf extract against streptozotocin induced diabetic rats. *International Journal of PharmTech Research*, *1*(4), 1069-1072.

[36] Hanirex, D. K., & Kaliyamurthie, K. P. (2013). Multi-classification approach for detecting thyroid attacks. *International Journal of Pharma and Bio Sciences,* 4(3), B1246-B1251

[37] Kandasamy, A., Mohan, R., Lydia Caroline, M., & Vasudevan, S. (2008). Nucleation kinetics, growth, solubility and dielectric studies of L-proline cadmium chloride monohydrate semi organic nonlinear optical single crystal. *Crystal Research and Technology: Journal of Experimental and Industrial Crystallography*, *43*(2), 186-192.

[38] Srinivasan, V., Saravanan, T., Udayakumar, R., & Saritha, G. (2013). Specific absorption rate in the cell phone user's head. *Middle-East Journal of Scientific Research*, *16*(12), 1748-50.

[39] Udayakumar R., Khanaa V., & Saravanan T. (2013). Chromatic dispersion compensation in optical fiber communication system and its simulation, Indian Journal of Science and Technology, 6(6), 4762-4766.

[40] Vijayaragavan, S.P., Karthik, B., Kiran, T.V.U., & Sundar Raj, M. (1990). Robotic surveillance for patient care in hospitals. *Middle-East Journal of Scientific Research*, *16*(12), 1820-1824.

[41] Priyambiga, R., & Shanthi, D. (2014). Diverse Relevance Ranking in Web Scrapping for Multimedia Answering. *International Journal of System Design and Information Processing, 2*(2), 34-39.

[42] Rasool, Z., Tariq, W., Ir. Dr. Othman, M.L., & Dr.Jasni, J.bt. (2019). What Building Management System Can Offer to Reduce Power Wastage both Social and Economical: Brief Discussion by Taking Malaysian Power Infrastructure as a Sample. *The SIJ Transactions on Advances in Space Research & Earth Exploration, 7*(1), 1-5.

[43] Taylor and Jin, B. (2016). A Complete Review on Various Noises and Recent Developments in Denoising Filters. *Bonfring International Journal of Power Systems and Integrated Circuits, 6*(4), 22-29.

[44] Sethi, G., Shaw, S., Jyothi, B., & Chakravorty, C. (2014). Performance Analysis of Wi-MAX Networking Modulation Scheme. *International Scientific Journal on Science Engineering & Technology, 17*(9), 882-885.

[45] Achar, R.K., SwagathBabu, M., & Dr.Arun, M. (2014). Border Gateway Protocol Performance and Its Protection against Disturbed Denial of Service Attack. *Bonfring International Journal of Research in Communication Engineering, 4*(1), 5-9.

[46] Phadke, S. (2013). The Importance of a Biometric Authentication System. *The SIJ Transactions on Computer Science Engineering & its Applications, 1*(4), 18-22.

[47] Sangeetha, N., Dr.Gopinath, B., Muthulakshmi, S., Dr.Kalayanasundram, M., & Suriya, G. (2018). A New Approach to Single Phase AC Microgrid System Using UPQC Device. *Bonfring International Journal of Software Engineering and Soft Computing, 8*(2), 26-34.

[48] Sonam Vohra, R., & Dr. Sawhney, R.S. (2014).Dynamic Routing Protocols Analysis based on Dissimilar Number of Packets. *The SIJ Transactions on Computer Networks & Communication Engineering (CNCE), 2*(3), 1-6.

[49] Prabhakar, E., & Sugashini, K. (2018).New Ensemble Approach to Analyze User Sentiments from Social Media Twitter Data. *The SIJ Transactions on Industrial, Financial & Business Management (IFBM), 6*(3), 7-11.

[50] Aruna, K.B., LallithaShri, A., Aravindh, Jayakumar& Jayasurya, (2017). Protection for Multi Owner Data Sharing Scheme. *Bonfring International Journal of Advances in Image Processing, 7*(1), 01-05.