iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** VII **Month of publication:** July 2019

DOI: http://doi.org/10.22214/ijraset.2019.7012

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

Implementation of Encoding and Decoding in Delay Tolerant Networking

Sarita Malik[1], Sudesh Kumari Nandal[2]
[1,2]*Department of Electronics and Communication Engineering, BPS Women University Khanpur Kalan, India*

Abstract: ***The research work focused on delay tolerant networking that has been considered as mechanism of computer network system. It has been observed that there is requirement to enhance the features of delay-tolerant networking. This up gradation could be performed by reducing the size of packet at the time of transmission. Main aim of proposed work is to secure DTN content from active and passive attack. System should be capable to providing security at multiple layer. Research focused on designing and implementation of secure and fast mechanism to save information from attackers in DTN environment. The contents need to compress during cooperative sharing and security should be provided to them at the time of transmission. Research work has used RSA mechanism in order to encrypt the contents stored in packets. Moreover a compression technique has been used to reduce the packet size. After simulating the transmission the comparative analysis of time consumption and error rates found during is simulated using MATLAB.***
Keywords: DTN, ENCODING, DECODING, MATLAB, TCP/IP

I. INTRODUCTION

DTN [1] stands for Delay-tolerant networking that has been considered as suitable approach to transfer data over network system. Delay Tolerance Network in present scenario is facing lot of technical challenges. Many challenges have been faced due to presence of heterogeneous networks. Due to such challenges the performance of existing DTN system gets degraded. In recent times, the term disruption-tolerant networking is popular in the United States. The reason is that it has been supported by the DARPA. In several time, DARPA has donated to DTN based projects [2]. But there is occurrence of Disturbance due to limited range of wireless radio. Mobile nodes sparsely, attack, and noise also influences the performance of DTN.

It has been observed that mobile appliances are frequently used by several user in their daily life. These applications are very helpful in performing the operation such as remote access to IOT based devices and social communication. It has been investigated that the user feel requirement of fast and secure data transmission. However there are many issues during data transmission due to weak connectivity of network[3]. Some of existing researches described Network coded cooperation in delay tolerant networks. Several tradition approaches are providing comparable error rates with DF. Research has opted to improving spectral and energy efficiency of the target network [4].

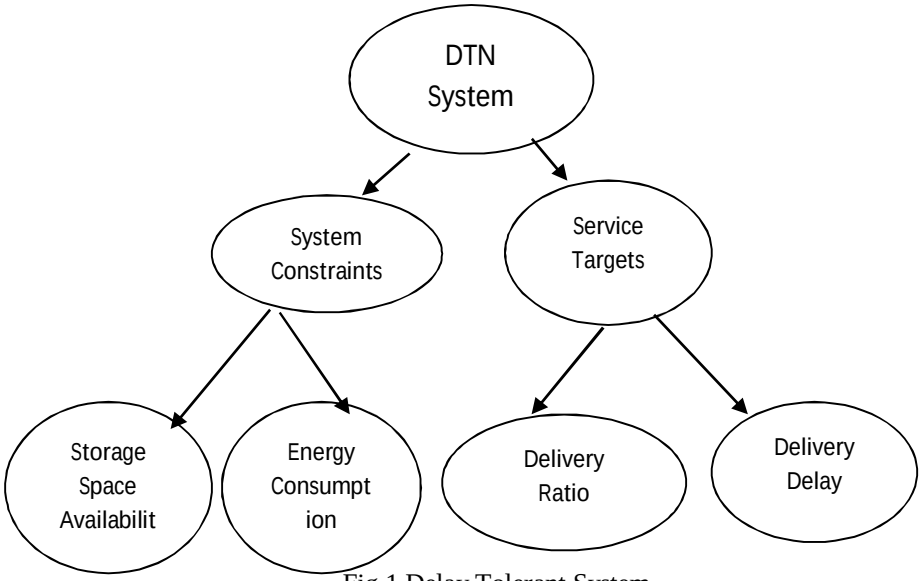


Fig 1 Delay Tolerant System

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue VII, July 2019- Available at www.ijraset.com

There are many challenges with mobile DTNs such as security issue and performance issues. There is also a challenge to route the information in perfect manner. If nodes are mobile, the tables of static routing may be unsuitable. As several apps includes the transmission to the known destination node. The existing researches have highlighted several such issues related to transmission. Routing issues have been resolved using routing table in DTN [5] many researches. But the objective of research is to study the need and scope after resolving performance and security issues in DTN. In the research work the perform analysis of existing researches has been proposed. The loopholes of existing researches are highlighted. Research would propose efficient and secure model to enhance the performance of DTN [6]. The comparative study of traditional and proposed DTN model representing hacking probability, packet size and error rate would be simulated in this research.

II. PROPOSED WORK

Some of existing researches described Network coded cooperation in delay tolerant networks. Several tradition approaches are providing comparable error rates with DF and at same time improving spectral and energy efficiency of the target network. But there is need to upgrade the Delay-tolerant networking by enhancing its performance by file size reduction during transmission and cooperative sharing. The security of data travelling on DTN is also mandatory.

The proposed model would consist of two additional layers of file compressor and file encoder. The data received from file server would be compressed by file server that would be connected to database server to compress and decompress data. The step would reduce size of file and reduces the delay in transmission. Then compressed data would be encoded by file encoder in order to make it secure. In DTN the all nodes that would receive data would decode and decompress the file in order to make it understandable and usable.

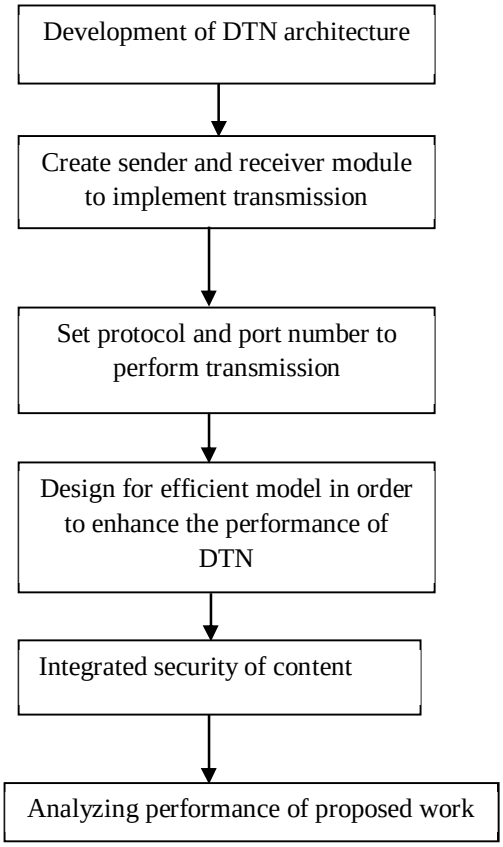


Fig 2 Process Flow

A. Packet size Reduction Logic

The packet size has been reduced using packet replacement mechanism. The packet replacement mechanism would hit two targets with single arrow. It would reduce the size of packet in order to increase the speed of data transmission. As the size of packet decreased the error rate during transmission get reduced automatically. In order to reduce the content size the frequency of repeated large words would be considered. The words that are repeating again and again in same text would be replaced by small keys before transmission.

©IJRASET: All Rights are Reserved

B. Security Integration In Work

1) Encryption and Decryption Algorithm of RSA: Two keys, d and e are used in RSA algorithm. It has been used to for decryption and encryption, respectively. The actual data P has been encrypted into decoded form that is referred as cipher text C.

2) Algorithm of RSA for Encryption

Following step are include in order to RSA encryption in text

a) STEP1: Take plane text P
b) STEP2: Take two keys d and e
c) STEP3: Take n constant
d) STEP4: Get cipher text using equation $C = P^e \bmod n$

3) Algorithm of RSA for decryption

Following step are include in order to RSA decryption in text

a) STEP1: Take Cipher text C
b) STEP2: Take two keys d and e
c) STEP3: Take n constant
d) STEP4: Get plain text using following equation $P = C^d \bmod n$

C. Flow chart for RSA Encryption

The following are flow chart describe in the function. In following flow chart the plan text p has been taken and two keys d and e with n constant are considered. Then the cipher text has been generated using equation $C=P^e \bmod n$.

D. Flowchart for RSA Decryption

The following are flow chart describe in the decryption function. In following flow chart the cipher text C has been taken and two keys d and e with n constant are considered. Then the cipher text has been converted to plane text using equation $P=C^d \bmod n$.

The RSA based encryption would protect data from external attack in DTN network. The content after compression would be encrypted using RSA mechanism. This would reduce the chances of external attack from cracker end. The algorithm applied during encryption would convert the contents to cipher form that would be non understandable. On receiving end the reverse algorithm would convert the cipher text to plain text that would make content transferred over DTN easy to understand.

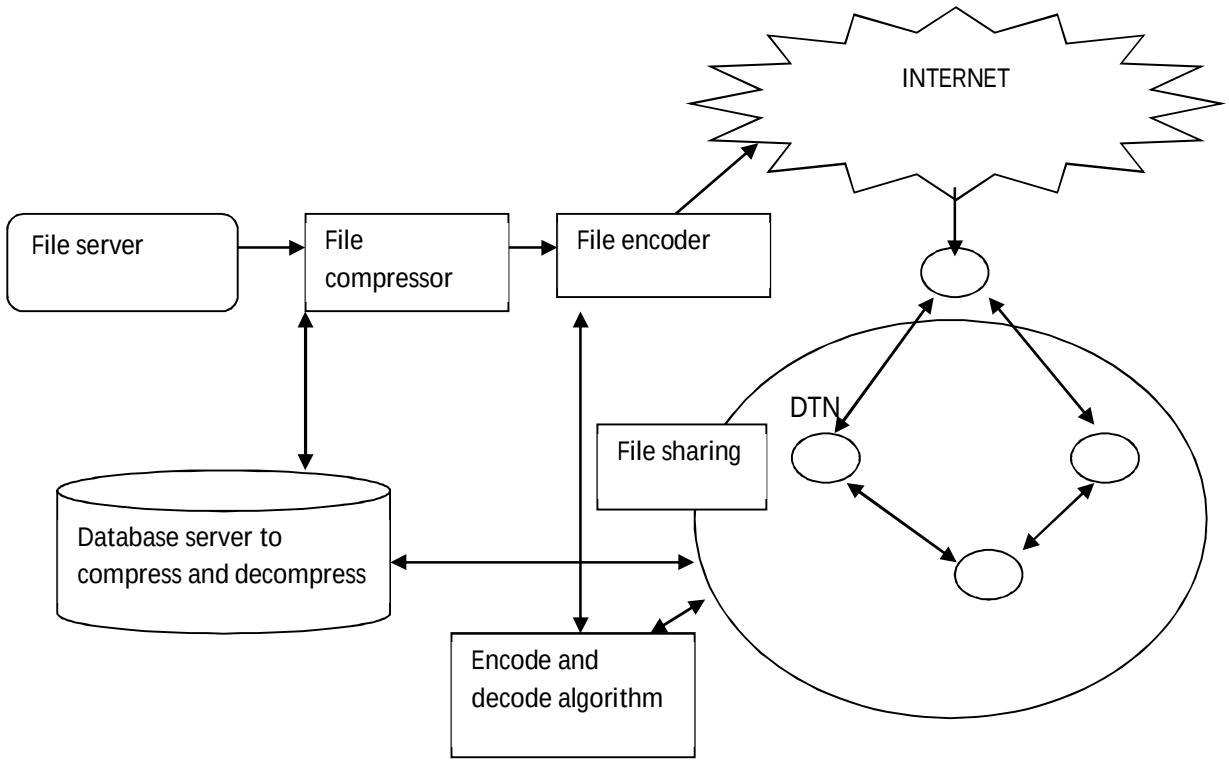


Fig 3 The Proposed model

©IJRASET: All Rights are Reserved

III. RESULT AND DISCUSSION

The results of the proposed work are stated below

A. Time Consumption

This simulation is representing the difference between time taken in case of traditional security system and proposed system. Following chart shows the existing work in red colour line and proposed work by blue colour line. Proposed work has been found less time consuming.

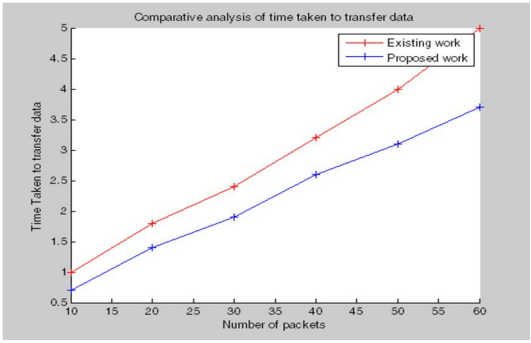


Fig 4 Comparative analysis of time taken during transmission

B. Error Rate

As there will be small size packet of data, there will be less probability of error. Therefore proposed work is capable to decrease the less error as compare to traditional work. Following figure represent the comparative analysis of error rate in case existing and proposed work. The proposed work is showing less errors as compare to traditional.

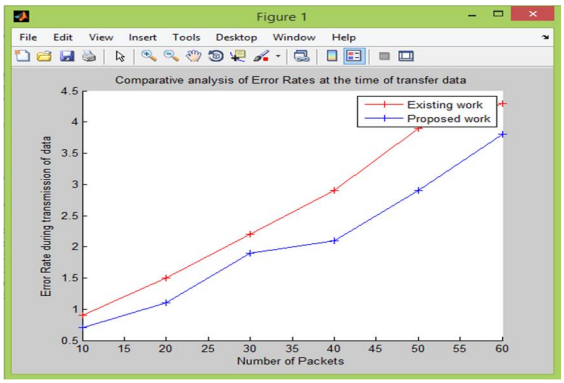


Fig 5 Comparative analysis of error rates at time of transfer data

C. Packet Size Reduction

In proposed work, Due to reduction in size of data the packet size get reduced. Thus proposed work use small data in packets as compare to traditional work. Following figure represent the comparative analysis of packet size in case existing and proposed work.

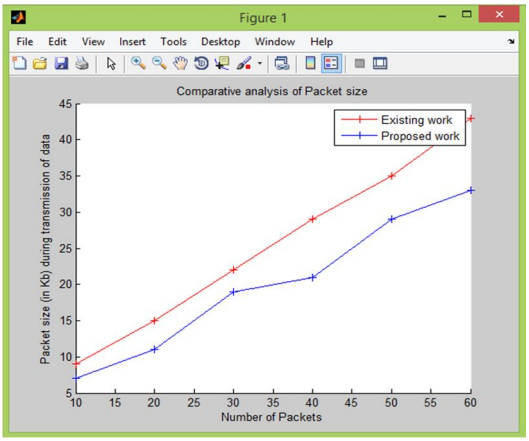


Fig 6 Comparative analysis of packet size

©IJRASET: All Rights are Reserved

Table 1 Comparison Chart of Existing and Proposed Work

	Existing work	Proposed work
Hacking probability[23]	0.56	0.23
Congestion control[2]	0.52	0.9
Transmission error control in [5]	0.42	0.86
Compression factor[4]	0.89	0.5
Reliability[11]	0.45	0.87

IV. CONCLUSION

The results show that the proposed DTN model has achieved the objective of research. This work has reduced the packet size in order to increase the performance. Moreover the RSA based security mechanism has been applied over the content in order to increase protection during data transmission. Error rates, packet size, probability of security cracking in tradition work and proposed work has been compared in this research. Comparative analysis of time and error rates and packet size been simulated using MATLAB. SCOPE OF RESEARCH

The research work has provided the study of need and scope of DTN. It would perform the analysis of existing researches and their proposals. It is capable to investigate the loop of existing researches. The steps are followed to reduce size of file and reduce the delay in transmission. Then compressed data would be encoded by file encoder in order to secure the transmission. In DTN all nodes that would receive data would decode and decompress the file. It would propose the efficient and secure model in order to enhance the performance of DTN. Along with this the comparative study of traditional and proposed work is also provided by the research work.

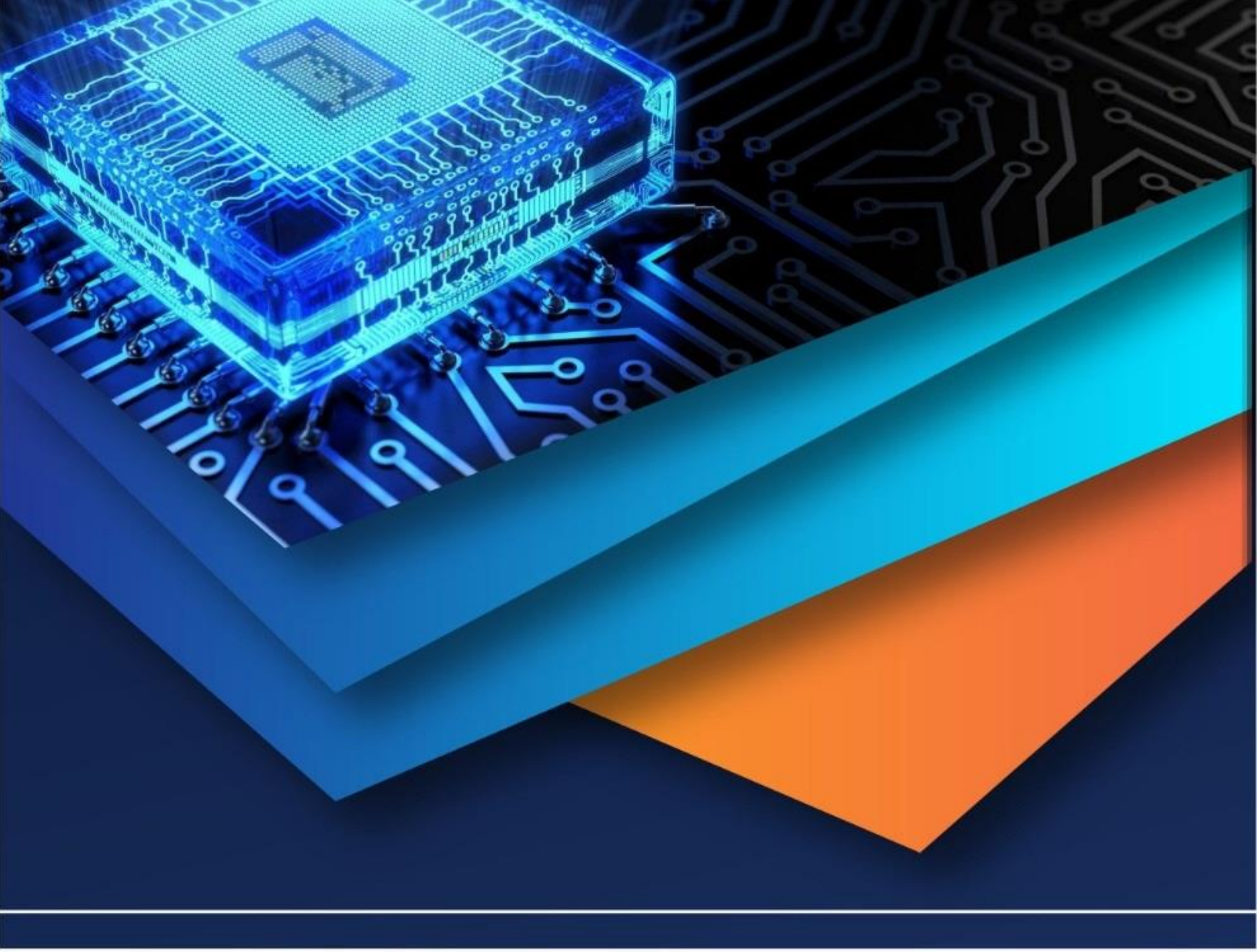
REFERENCE

[1] Janani Vijayanathan, ,"Delay Tolerant Social Networking (DTSN): Dual architecture for DTN based social networking"2011 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA).Year: 2011.Page s: 55 - 58 .
[2] Chuan Zhou, ,"Adaptive fault-tolerant control for a class of networked control system with random time delay based on neural network"Proceedings of the 30th Chinese Control Conference. Year: 2011. Page s: 4217 - 4222
[3] Onur Çalık , ,"Network coded cooperation in delay tolerant networks"2016 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE). Year: 2016. Page s: 155 - 157
[4] Madhavi Gholap "Information Sharing in Delay Tolerant Mobile Networks with Some Incentive and Fewest Transmissions" 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN). Year: 2016. Page s: 119 - 123
[5] YoungSang Yun , , "Distributed Algorithm for Lifetime Maximization in a Delay-Tolerant Wireless Sensor Network with a Mobile Sink" . IEEE Transactions on Mobile Computing. Year: 2013 , Volume: 12 , Issue: 10. Page s: 1920 - 1930
[6] Anh-Minh Nguyen,"SOCIAL-DTN: Why Social Networking Services is more fruitful to Mobile Delay-Tolerant Networks?", 2009 International Conference on Ultra Modern Telecommunications & Workshops.Year: 2009.Page s: 1 - 2
[7] Azadeh Omidvar, ,"Intelligent routing in delay tolerant networks" 2014 22nd Iranian Conference on Electrical Engineering (ICEE).Year: 2014.Page s: 846 - 849
[8] Ana Barroso ,"Performance evaluation of delay-tolerant wireless friend-to-friend networks for undetectable communication"2015 IEEE 40th Conference on Local Computer Networks (LCN). Year: 2015.Page s: 474 - 477
[9] Depeng Chen, ”On the Applicability of Onion Routing on Predictable Delay-Tolerant Networks" 2017 IEEE 42nd Conference on Local Computer Networks (LCN). Year: 2017. Page s: 575 - 578
[10] Zhongjiang Yan "Optimal Traffic Scheduling in Vehicular Delay Tolerant Networks" IEEE Communications Letters.Year: 2012, Volume: 16 , Issue: 1.Page s: 50 – 53.
[11] Sharmin Rashid, “Proposed Methods of IP Spoofing Detection & Prevention, International”, Journal of Science & Research (IJSR), Volume 2, Issue 8, August 2013, pp.438-444.
[12] Amandeep Kaur, “A Review on Security Attacks in Mobile Ad-hoc Networks”, International Journal of Science & Research, Volume 3 Issue 5, May 2014, pp.1295-1299
[13] P. Kiruthika Devi, “Spoofing attack detection & localization in wireless sensor network”, International Journal of Computer Science & Engineering Technology, Vol. 5, No. 09, Sep 2014, pp.877-886.
[14] Barleen Shinh, “A Review Paper on Collaborative Black Hole Attack in MANET”, International Journal of Engineering & Computer Science, Volume 3, Issue 12, December 2014, pp. 9547-9551.

©IJRASET: All Rights are Reserved

[15] Blessy Rajra M B, "A Survey on Security of network Attacks & Prevention Mechanism", Journal of Current Computer Science & Technology, Volume 5, No. 2, February 2015, pp.1-5.
[16] Md. Waliullah, Diane Gan, "Wireless LAN Security Threats & Vulnerabilities", International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2014, pp.176-183.
[17] P. Kiruthika Devi, Dr. R. Manavalan "Spoofing attack detection & localization in wireless sensor network", International Journal of Computer Science & Engineering Technology, Vol. 5, No. 09, Sep 2014, pp.877-886.
[18] Barleen Shinh, Manwinder Singh, "A Review Paper on Collaborative Black Hole Attack in MANET", International Journal of Engineering & Computer Science, Volume 3, Issue 12, December 2014, pp. 9547-9551.
[19] Ms. Vidya Vijayan, Ms. Josna P Joy, Mrs. Suchithra M S, "A Review on Password Cracking Strategies", international Journal of Research in Computer & Communication Technology, 2014, pp.8-15.
[20] Blessy Rajra M B, A J Deepa ME, "A Survey on Security of network Attacks & Prevention Mechanism", Journal of Current Computer Science & Technology, Volume 5, No. 2, February 2015, pp.1-5.
[21] Venkadesh .S, K.Palanivel , "A Survey on Password Stealing Attacks & Its Protecting Mechanism", International Journal of Engineering Trends & Technology (IJETT) , Volume 19, Number 4 , Jan 2015, pp.223-226.
[22] Tuhin Das, "A Study on Identity Based Attack Detection and Localization by the Clustering in Wireless Sensor Network, International Journal of Computer Sciences and EngineeringOpen Access, Volume-04, Issue-02, Feb 2016, pp. 96-99 .
[23] Amandeep Kaur, Sandeep Singh Kang, "Attacks in Wireless Sensor Network- A Review", International Journal of Computer Sciences & Engineering, Vol.04, Issue 05, May 2016, pp.157-162.
[24] Shahriar Mohammadi, Reza Ebrahimi Atani, Hossein Jadidoleslamy, "A Comparison of Link Layer Attacks on Wireless Sensor Networks", Journal of Information Security, April 2011, pp. 69-84.
[25] Hani Alshamrani, "Internet Protocol Security (IPSec) Mechanisms", International Journal of Scientific & Engineering Research, Volume 5, Issue 5, May-2014, pp. 85-87.
[26] Chander Diwakar, Sandeep Kumar, Amit Chaudhary, "SECURITY THREATS IN PEER TO PEER NETWORKS", Journal of Global Research in Computer Science, Volume 2, No. 4, April 2011, pp. 81-84.
[27] Haroon Shakirat Oluwatosin, "Client-Server Model", Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 1, Feb. 2014, pp. 67-71.
[28] Ms. Jasmin Bhambure, Ms. Dhanashri Chavan, Ms. Pallavi Band, Mrs.Lakshmi Madhuri, "Secure Authentication Protocol in Client – Server Application using Visual Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014, pp. 556-560.
[29] Mohan V. Pawar, Anuradha J, "Security of network and Types of Attacks in Network", International Conference on Intelligent Computing, Communication & Convergence, 2015, pp. 503 – 506.
[30] MANJIRI N. MULEY, "ANALYSIS FOR EXPLORING THE SCOPE OF NETWORK SECURITY TECHNIQUES IN DIFFERENT ERA: A STUDY", International Journal of Advanced Computational Engineering and Networking, Volume-3, Issue-12, Dec.-2015, pp. 33-36.
[31] E Bertino, "Data Security – Challenges and Research Opportunities", Springer International Publishing Switzerland, 2014, pp. 9–13.
[32] Bhawan Bhardwaj,Ankur Mittal, "Advanced Mechanisms to Secure Wireless ad hoc Network with Performance Analysis", Volume 08, Issue 08 ,October - December 2017.
[33] Jaclynn J. Stubbs, Gabriel C. Birch, Bryana L. Woo and Camron G. Kouhestani"Physical Security Assessment with Convolutional Neural Network Transfer Learning" 2017 International Carnahan Conference on Security Technology (ICCST)
[34] ZHAO Lei1, REN Xiangyu, LIU Mengleng, WANG Lina, ZHANG Hao, ZHANG Huanguo, "Collaborative Reversing of Input Formats and Program Data Structures for Security Applications"China Communications (Volume: 11, Issue: 9, Sept. 2014)
[35] Wu Wei "The Application Research of Airport Security Information Management System on the Field of Civil Aviation Security"43rd Annual 2009 International Carnahan Conference on Security Technology
[36] Prof. Mukund R. Joshi, Renuka Avinash Karkade"Network Security with Cryptography Network Security with Cryptography "Renuka Avinash Karkade et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 201-204
[37] Albandari Mishal Alotaibi, Bedour Fahaad Alrashidi, Samina Naz Zahida Parveen, "Security issues in Protocols of TCP/IP Model at Layers Level", International Journal of Computer Networks Communications Security, VOL. 5, NO. 5, MAY 2017, pp. 96-104.
[38] J.M. Sierra , J.C. Hernandez , A. Ribagorda , N. Jayaram, "Migration of Internet security protocols to the IPSEC framework"36th Annual 2002 International Carnahan Conference on Security Technology
[39] Chang-Chun Cheng , Wei-Ming Chen ,Han-Chieh Chao , Yao-Po Wang, "FPGA authentication header (AH) implementation for Internet appliances"11th Pacific Rim International Symposium on Dependable Computing (PRDC'05)
[40] Manjiri N. Muley, "Analysis for Exploring the Scope of Network Security Techniques in Different era: A Study", International Journal of Advanced Computational Engineering and Networking, Volume-3, Issue-12, Dec.-2015, pp. 33-36

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)