J. Sustain. Wireless Syst.
Vol.01/ No. 01
Pages: 62-68
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.1.005

SECURE MULTIMEDIA DATA TRANSMISSION IN MOBILE AD-HOC NETWORKS

S. Balaji
Department of Computer Science and Engineering,
Francis Xavier Engineering College, Tirunelveli., India
E-mail: sbalajiphd@gmail.com

Y. Harold Robinson
Department of Computer Science and Engineering,
SCAD College of Engineering and Technology, Tirunelveli, India
E-mail: yhrbinphd@gmail.com.

E. Golden Julie
Department of Computer Science and Engineering,
Anna University Regional Campus, Tirunelveli, India
E-mail :goldenjuliephd@gmail.com

Abstract. Multimedia file transmission with quality of service is the important issue in Mobile Ad-hoc Networks. The real-time data is in the form of audio file and the video file. These kinds of files can be divided into several data packets and the data packet is delivered from the begining node to the recipient node within the limited amount of time. The increase of throughput is possible only by means of secure data transmission. So, the secure data transmission methodology is used to implement the quality delivery of the multimedia files. The sequence of data packets are encoded and decoded using the encryption and the decryption process. The simulation results proved that the proposed method has the highest amount of throughput, delivery ratio and also improving the quality of service compared to all the other related methods.

Keywords: MANET, multimedia file, data packets, throughput, .

1 Introduction

The MANET does not depend on an infrastructure which is fixed in prior and the mobile nodes could dynamically communicate with other nodes within a communication range [1]. The topology of MANET dynamically changes and every mobile node acts a host as well as a router to transmit the data packets. MANET has the important properties of without any fixed infrastructure, Dynamic topology, Autonomous terminal, Energy constrained operation, Limited Bandwidth, Interoperation with the Internet, Multi-hop Routing, and Auto-configurable [2]. MANET faces certain challenges due to the wireless network medium and mobility. As MANET is a wireless network the traditional problem associated with wireless networking is inherited. Asymmetric propagation with time varying properties may affect the channel and the wired media is more reliable compared to the wireless media [3]. Scalability is an important feature required in MANET because the size of the network grows according

J. Sustain. Wireless Syst.
Vol.01/ No. 01
Pages: 62-68
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.1.005

to the purpose, so every mobile node must adapt to handle the augmentation of network to implement the task assigned [4]. Another challenge in MANET arises due to distributed environment where it is difficult task to detect and handle the flaws in communication due to absence of central administration [5]. Complexities like packet losses, recurrent partitions in network and route fluctuation possibly occurs due to random movement of autonomous nodes [6]. There is a great demand for real-time communication to be established in critical applications such as disaster recovery, search and rescue affair, battle field management in a mobile network [7]. Dissemination of data such as video and audio need to satisfy specific time constraints based on deadline or priority of the data. The communication services disseminated may be a voice, graphics, video, images. Images related to map of urban area, position of soldier, maps of defense area etc. The messages are encrypted between sender and receiver based on algorithm to enhance security [8].

2 Related Work

Trust, security and encryption are the process of rendering message in practice of mobile peer-to-peer network. There are various applications becoming a ground for exchanging digital data where many sensors, laptops,

smart-phone, notebooks etc exchange high speed data to perform coherently. Moreover, these units carry out data exchange on the move emphasizing on flexibility and mobility [9]. Audio or video transmission must be guaranteed for emergency applications domains in MANET. File streaming services with dynamic topology must be promising and in reliable. Multimedia images must be secured by means of encryption in prior to be transferred over the network. There are two main features to enhance communication are secure key management system and the secure data exchange with data encryption. This paper is associated with real-time data corresponding to any kind of data format, exchanged in an encrypted form at the sender side and decrypted format receiver side. This technique of sending and receiving images using public key in encrypted and decrypted form assures good security standard for data transmission [10]. Enhanced resource key generation algorithm (ESKGA) [11] helps to avoid the brute force attack by using an efficient algorithm in wireless sensor network. And the key generation scheme implemented in RSA approach for the effective and efficient results [12]. Chinese reminder algorithm [13] uses the adopted approach for encryption and decryption process. For more security, another key generation technique [14] has been implemented and it will used the letters for public key generation algorithm. The same has been implemented in the private key generation algorithm [15]. Chinese reminder approach mostly concentrate in the arithmetic operations and modulo functions [16]. This type of algorithms [17-18] improves the execution time as faster compared to the previous existing security algorithms.

3 Proposed Work

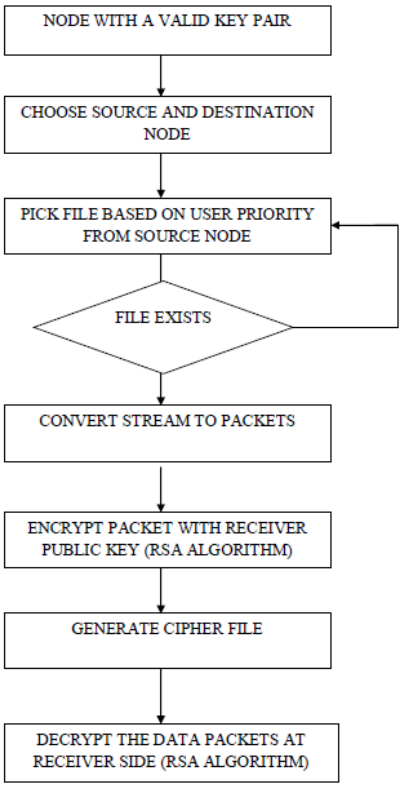
File sharing has become a popular feature in MANET. This methodology focuses on multimedia transmission in MANET. The proposed work is fully related on Distributed hash table and did not take into consideration about the real-time requirements to meet the deadline. Moreover they are much focused on secure data transmission.

ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 01
Pages: 62-68
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.1.005

The proposed algorithm is used to find a deadline is assigned to each task that streams a video and tasks are scheduled based on increasing order of their deadline. With a slight variation, RMS algorithm assumes that all the tasks are monotonic, and a priority is assigned to all the tasks in order of request rate. The tasks with high request rate obtain high priority and they are executed first. This system is based on BitTorrent, with more enhanced features to support social network usage and live video streaming. This works out greatly for Internet but does not adapt to the network. Fig 1 describes the architecture of encryption and decryption of multimedia files using public key pair. Encryption and decryption is an important concern in today's era to transmit the data from one place to another to prevent unauthorized access. The original message must be difficult to break depending on the computational hardness of the key. Here RSA algorithm is used to enhance the security to encrypt and decrypt, thus making it complex to break the key and retrieve the original data. An image file /audio file is selected encrypted decrypted of the receiver to transfer the data from one destination to another.

Every node has its own public/private keys. The key as it name suggests must be distributed to other nodes in the network to establish communication. The key is basically long random number and this key has be securely handled and managed. The size of the key is taken as 128 bits and key format is hexadecimal. RSA signature algorithm is adopted to generate unique key pair for every node. Once the key is generated, every node looks for trusted one-hop neighbor to obtain a certificate ensuring that the key generated is a valid key.



ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 01
Pages: 62-68
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.1.005

Fig. 1: Architecture Diagram

4 Performance Evaluation

The simulation parameters are described in Table 1.

Table 1: Throughput corresponding to audio files

PARAMETERS	VALUE
CHANNEL	WIRELESS CHANNEL
NETWORK TOPOLOGY	1000*1000
NUMBER OF NODES	25
INITIAL ENERGY	100W
TRANSMISSION RANGE	200
TRUST-THREHSOLD	0.3 to 0.5

Generally the transfer speed depends on time taken for encryption and decryption. The time is taken to encrypt and decrypt increases especially when the file size increases.

$$\text{Transfer speed} = \frac{\text{Input File size}}{(\text{EET} + \text{DET})} \quad (1)$$

Here, Input File size is in KB

EET is Encryption Execution Time

DET is Decryption Execution Time

The risk exposed by using an invalid key to send messages is given by equation

$$R = Tg\ LT\ \Sigma Tg\ LT\ t = 0\Sigma\ LT\ j \in C\ \Sigma\ R\ i, (t)\ i \in M \quad (2)$$

Table 2 demonstrates the transfer speed and the throughput values.

Table 2: Transfer speed and throughput

SNO	FILE NAME	FILE SIZE	TRANSFER SPEED	THROUGHPUT
1	NEPAL.jpg	858.4KB	3342ms	398.852184 kbps
2	PICTURE.jpg	118.8KB	605ms	196.36363 kbps
3	Img1.jpg	126.6KB	339ms	216.55162 kbps

ISSN: 2582-3167 (online)

J. Sustain. Wireless Syst.
Vol.01/ No. 01
Pages: 62-68
http://irojournals.com/irosws/
DOI: https://doi.org/10.36548/jsws.2019.1.005

Figure 2 illustrates the selected audio files format. Figure 3 demonstrates the comparison of throughput to the related works. The simulation results proved that the proposed work has the improved performance compared to its related methods for the security enhancements.

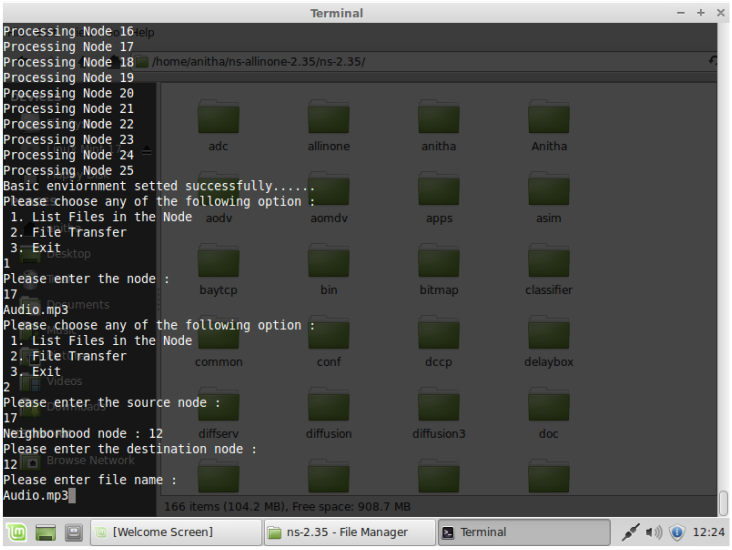


Fig. 2: Encryption Process

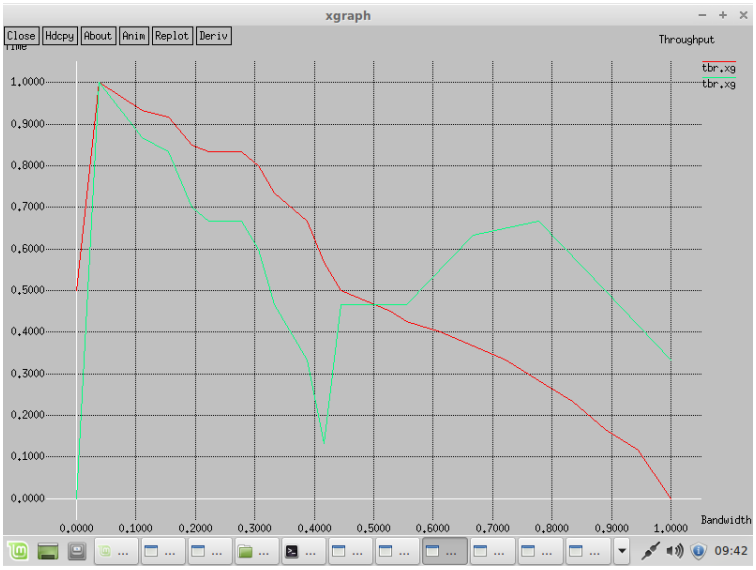


Fig. 3: Comparison of the throughput

5 Conclusion

In this paper, the issue of data transmission of multimedia files in the mobile ad-hoc network has been resolved. The distribution of multimedia files has been thoroughly monitored. By using the encryption and decryption

ISSN: 2582-3167 (online)

process, the multimedia file has been transferred from the source node to the destination node without any disturbance. The secured data transmission algorithm is proposed to improve the quality of service and it completely provides the security between the source node to the destination node. The proposed secure data transmission algorithm deliver the packets without any loss in a specific particular time and that leads to improving the throughput and network performance and reduces the delay. And this security algorithm provides efficient performance compared to similar security based algorithms. In future, this work has been tested with more number of nodes with high mobility conditions in a different scenario. Then, during the data transmission multimedia files supports all type of image format, video format and audio format.

References

[1] Jin-Hee Cho, Ing-Ray Chen and Kevin S. Chan, " Trust threshold based public key management in mobile adhoc networks" Adhoc Networks, Vol 44, pp 58–75, 1 July 2016.

[2] Bui, B.D., Pellizzoni, R., Caccamo, M., Cheah, C.F., and Tzakis, A, "Soft real-time chains for multi-hop wireless ad-hoc networks" 13th IEEE Real Time and Embedded Technology and Applications Symposium, RTAS'07 ,pp. 69–80, 2007.

[3] Robinson, Y., & Rajaram, M. (2015). Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks. The Scientific World Journal, 2015, 1–9.

[4] G.A.V.Rama ,Chanra Rao, P.V.Lakshmi and N.Ravi Shankar, "A Novel Modular Multiplication Algorithm and its Application to RSA Decryption", International journal of Computer Science Issues Vol.9 No.6 pp.303-309, 2012.

[5] Ravi Shankar Dhakar , Amit Kumar Gupta and Prashant Sharma, "Modified RSA Encryption Algorithm", Second International Conference on Advanced Computing & Communication pp.426-429, 2012.

[6] Robinson, Y.H., & Rajaram, M. (2016). A Memory Aided Broadcast Mechanism with Fuzzy Classification on a Device-to-Device Mobile Ad Hoc Network. Wireless Personal Communications, vol. 90, no.2, pp. 769-791.

[7] Thangavel M, Varalakshmi P, Murali M and Nithya K, " An enhanced and secured RSA key generation scheme" Journal of Information security and Applications, Vol.20, pp.3-10, 2015.

[8] Yunfei Li, Qing Liu, Tong Li, "Design and Implementation of an improved RSA Algorithm" International Conference on E-health Networking, Digital Ecosystems and Technologies, pp.390-393, 2010.

[9] Harold Robinson, Y, Golden Julie, E., Krishnan Saravanan, Raghvendra Kumar & Le Hoang Son, (2018), FD-AOMDV: fault-tolerant disjoint ad-hoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks, Journal of Ambient Intelligence and Humanized Computing, 1-18.

[10] Zulkarnain Md Ali and Jassim Mohammed Ahmed, "New Computation Technique for encryption and decryption based on RSA and elgamal cryptosystems", Journal of Theoretical and Applied Information Technology, Vol 47 No 1 pp.73-79, 2013.

[11] Sonal Sharma and Alshamma S, "High speed implementation of RSA algorithm with modified keys exchange", Sciences Electronics", Technologies of Information and Telecommunications, pp.639-642, 2012.

[12] Harold Robinson, Y., Balaji, S., & Golden Julie, E., (2018). Design of a Buffer Enabled Ad hoc on-demand Multipath Distance Vector Routing Protocol for Improving Throughput in Mobile Ad Hoc Networks, Wireless Personal Communications, 1-26.

[13] Peltotalo, J., Harju, J., Saukko, M., Vaatamoinen, L., Bouazizi, I., Curcio, I.D.D and Van Gassel, J, April "A real-

time PEER-TO-PEER streaming system for mobile PEER-TO-PEER system". Concurrency and Computation: Practice and Experience, Vol 20, 127–138, April 2009.

[14] Noh J., Baccichet P., Hartung F., Mavlankar and Girod B "Stanford PEER-TO-PEER multicast (SPPM)-overview and recent extensions" Picture Coding Symposium, IEEE, pp. 1–4, 2009.

[15] Harold Robinson, Y., Balaji, S., & Golden Julie, E., (2018). PSOBLAP: Particle Swarm Optimization-Based Bandwidth and Link Availability Prediction Algorithm for Multipath Routing in Mobile Ad Hoc Networks, Wireless Personal Communications, 1-29.

[16] Hwang, R.J, Su, F.F., and Shiau, S.H, "An Efficient Decryption Method for RSA Cryptosystem, International Conference on Advanced Information Networking and Applications", pp. 585-590, 2009.

[17] Ding G. and Bhargava, B., "March. PEER-TO-PEER file-sharing over mobile ad hoc Networks" Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp. 104–108, 2004.

[18] Harold Robinson, Y & Golden Julie, E (2018). SMR: A Synchronized Multipath Rebroadcasting Mechanism for Improving the Quality of Conversational Video Service, Wireless Personal Communications,1-25.