International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 6, December 2016, pp. 2962~2970
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i6.11264

A Hybrid Cryptographic System for Secured Device to Device Communication

A. Rama Krishna[1], A. S. N. Chakravarthy[2], A. S. C. S. Sastry[3]
[1,3]Dept. of ECE, K L University, Guntur A.P., India
[2]Dept. of CSE, J N T U. K -UCEV, A.P., India

Article Info

Article history:

Received May 15, 2016
Revised Oct 15, 2016
Accepted Oct 29, 2016

Keyword:

Binary coding
Cryptography
D2D communication
Huffman coding
Wireless communication

ABSTRACT

It is general fact that even after enormous expansion of wireless communication there are still dead regions that hampers the effective communication. With exponential rise in the smart phones, a new layer of communication has evolved that could address the concerns of dead regions and capacity barriers. D2D is the evolving communication technology which focuses on short distance hops between the public devices to reach the destination. The major drawback of this technology is that most of the devices are public hence trustworthiness of the entire channel needs to be addressed in order to make it a viable solution. In this paper, we introduce a novel hybrid cryptographic approach that could address multiple eavesdroppers' scenario. This approach incorporates both Huffman coding and Binary coding to enhance the crypto benefits for the information transmitted over D2D channel that consists of several public devices. The dual-crypto nature of the proposed algorithm offers higher efficiency, better security and improved key transmission. Thus, the proposed hybrid cryptographic approach is robust in nature while easy and simple to operate. In addition, the proposed approach could recover the original information without any distortion from the encrypted data making the approach lossless in nature. Further simulation results prove that the proposed offers confidentiality to the transmitted to data while addressing the network capacity crunch.

Corresponding Author:

A. Rama Krishna,
Department of Electronics and Communication Engineering,
K L University,
Vaddeswaram, Guntur, A.P, 522502, India.
Email: ramakrishna.a@kluniversity.in

1. INTRODUCTION

In this digital era, wireless has become the major backdrop for cheap and high speed data transfer and several advance technologies are constantly evolving that are ensure wireless approachwould be the primary communication channel. It is evident that to ensure an effective communication channel that is capable of transferring significantamount of data between two authorized personnel requires a wide spread infrastructure [1]. With the advancements in the technology the corresponding requirement of the communication channel varies significantly. For example, smaller packets drop with more coverage for transmission, high data rates, secured and robust communication to name few [2]. The major drawback of the existing communication channels are complex network architecture and high power requirement for processing and transmission of the data packets.

Thus to effective address the above concerns of the existing wireless networks, a novel open-public channel is require that offers significantly high number of possible paths and energy at each node but requires low energy for transmission. Since, device-to-device (D2D) communication is independent of existing

wireless network architecture but can operate in tandem with the systemhas recently emerged as a promising technique that can significantly boost the performance of existing wireless networks [1]. The prime ideaof incorporating D2D communication along with the existing infrastructure was to employ the public channel rather than the licensed band.In addition, the operators expect that D2D communication would offer high data rates as its operation distance is small based on availableneighborhood-user equipmentswhile existing communication is infrastructure-based which has high operational distance [2]. Therefore, significant amount of research is focused on improving various factors associated with D2D communicationto ensure a holistic development of this technology.This communication channel is offers simple architecture, high data rates, and precise transmission with authorized clients. Unfortunately, as the means of communication is focused on the maximization of public nodes rather than private nodes and also the number of nodes would also be increased drastically, the security of information being transmitted plays a vital role in the feasibility of D2D communication system. Even though it addresses the factors of energy requirement, infrastructure security / safety, packet drops and data rates in an effective manner in comparison with existing systems [3]. Furthermore, with ever increasing rise in the smart device users (phones, pads, and etc) there is a significantly rise in the possibility of locating an optimal energy path with high data rate and improved coverage can be found to engage in communication.

Therefore it has become a vital task to provide effective data security and integrity approach so as to ensure the feasibility of D2D communication channel. In this paper, we focus on improved spectral utilization of the data being transmitted in a secured manner over public D2D communication channels. The major focus of this research was to design and develop an innovative novel framework that exploits various factors to provide reliable and robust D2D communication based on the existing network constraints and improve packetstransfer rate while minimizing the load existing communication infrastructure. Even though several approaches for optimized D2D communication have been proposed but still it has evolved into a research topicwith its scope expanding into various fields. Unfortunately, with significant rise in the research much of the focus was contributed towards securing the physical layer rather than the D2D communicationschannel layer. With the growing market of smart devices with secure physical layer are difficult to design and market due to shear high price and complex operation while usingdevices [1]. This led to design a framework that could secure the channel (i.e. means of communication) rather than the device; it has been evolving into an active research area.

1.1. Cryptography

Cryptography (as name indicates secret writing) is an art of transforming the information into noise like or unreadable data to any unauthorized individual or eavesdropper. Digital cryptography offers protection to information and authenticates the personnel accessing the information. It has become a high focused research area within the area of information security and assurance field [4].The digital cryptography has received significant attention in the current digital era, due to rapid developments and escalation in the amount of information transferred on the public channels such as D2D communication. We focus on the crypto systems that could offer a means of secured communication over unencrypted channels and/or protect the integrity of transmitted information. It is evident that any crypto system works on as presented in the Figure 1, one of the basic ideas as described below [5].

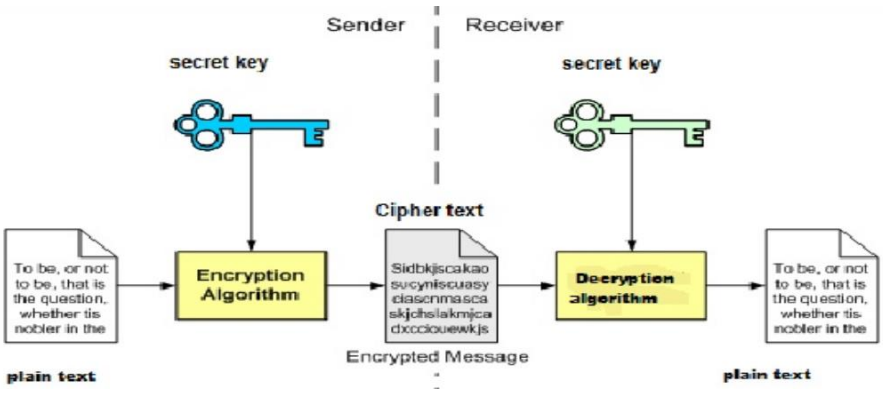


Figure 1. General Model of Cryptographic System

DataManipulation: This framework alters the original information based on a transform / code or look-up tableinto corresponding crypto information. These techniques are most commonly used approaches as their reverse-transformation would simple. The information could be recovered with minimal or no distortion in comparison with original information.

Data Location permutation: This framework proposes that the original information could be protected by means of changing the location of information bits based on a transform / code or look-up table into corresponding crypto information. The information could be recovered with no distortion in comparison with original information. The original information could be recovered from encrypted data by inverse permutation.

It is a well known fact that each of the above approaches has several advantages and corresponding limitations. Currently significant focus is incorporating in combining both the approaches to generate a hybrid model as discussed in this paper.

In brief, the proposed algorithm uses a combination of Huffman coding and Binary algorithm to securely transmit the information packets via D2D communication between two or more public devices. The Huffman algorithm offers higher efficiency in block encryption, while the Binary securely codesthe key management advantages. Thus the dual protection makes the data transmission secure. The remaining paper is structured as the Section 2 deals with background on various existing hybrid algorithms. The Section 3 introduces the coding concepts of Huffman and binary in detail. Section 4 deals with the proposed algorithm and Section 5 illustrates various phases of computer simulation that were carried out to test and analyze the proposed algorithm. Finally the conclusion is presented in the Section 6.

2. BACKGROUND

With the rapid advancements in the network technology and signal processing the corresponding requirement of the communication channel varies significantly in terms of security constraints. Commonly the word security means an environment that is danger free from malicious intent individuals/organizations. Most of the existing communication systems focus on physical security that protects infrastructure, physical data from unauthorized intrusionor destruction [6]. In this paper, we focus on transmission security that focuses on information that being transmitted between authorized personnel through a chain of physical devices (mostly public devices).

Nesterenko, A. Y. E., et al., [7] proposed a new hybrid encryption scheme based on ElGamal asymmetric encryption scheme with distributed secret keys. The keys were used as defense against unauthorized intrusion of encrypted messages. This scheme views the problem asdiscrete logarithm and incorporates the security that uses elliptic curve as the basis. The main feature of the scheme is the fact that plain message is not represented as a point of elliptic curve, hence, can encrypt a long messages. The cryptographic properties of the scheme were validated with practical evaluations. Persichetti, E., [8] introduces an encryption algorithm that incorporates coding theory in a post-quantum scenario. The hybrid concept of the algorithm uses Niederreiter construction which offers a random model focuses of IND-CCA security approach.

Shen, W., et al., [9] investigates various factors and limitations of the D2D communications channel existing protocols and proposed a new secure and robust key exchange concept that enables any two smart communicative devices to launch a D2D communications without prior public covert key information.This protocol was designed based on the Diffie-Hellman key exchange protocol and assuranceframework. The proposed schemewas developed on Android platform based devices and simulation using the Wi-Fi communication channel proves the robustness and protocol successful implementation.

Abd-Elrahman, E. et.al [10] analyzed various security factors surrounding the D2D communications' in both Proximity Services and transmission stages. Initially, existing limitations and requirements were considered by the authors in design and development of the Group Key Management (GKM) concept that would covertly and efficiently exchange messages over D2D processing, transmission and receiving stages of the communication system. The proposed solution was analyzed in depth and simulated with detailcomparison with existing approaches that focus on near field communication similar D2D (i.e. ad-hoc) [11]. Furthermore, the simulation results prove that the Group Key Management (GKM) concept is an efficient key management system for D2D communication. Rege, K., et al., [12] presented a hybrid encryption approachthat incorporate AES and RSA to improve the level of protection for the information being transmitted between two or more public devices that were using Bluetooth communication to transmit the information.

Lu, X., et al., [13] proves if an cryptotext is secured with KEM (i.e. Key Encapsulation Mechanism) and offers key flexibility and authentication then Tag-DEM (i.e. Tag Data Encapsulation Mechanism) that secures the authentic cryptotext from earlier phase is immune to key related attacks. The simulation results

show that the proposed hybrid encryption scheme is secured and robust against RKA. In addition, existing KEM approaches were also simulated only to prove that they satisfy these two properties.

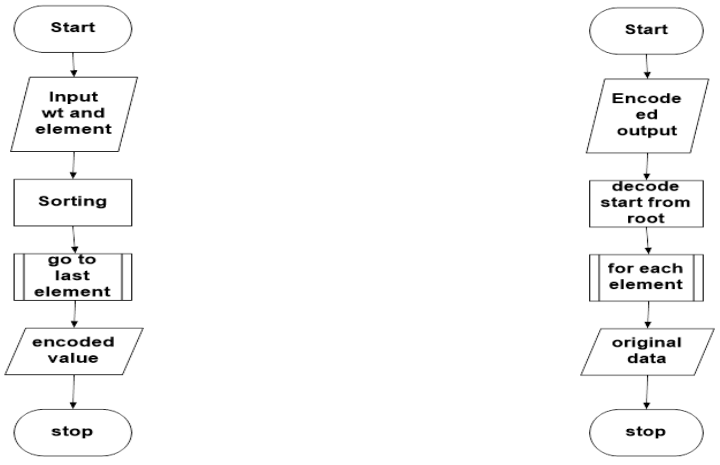
Kwon, H., [14] proposed a new D2D certificationprocess that incorporates a covert key determining stage using cipher text-policy attribute-based encryption (CP-ABE). By leveraging CP-ABE, this approach offers a agreement protocol and exchange the key information between the communicating parties in a multi-hop network system (i.e. similar to D2D communication). In addition, several deviations of the protocolswere introduced for different scenarios in a multi-hop networks without network infrastructure. Simulation results show that the scheme gains rational computation cost and are immune to MITM and replay attack in D2D mobile multi-hop networks.

3. CODING TECHNIQUES

Huffman coding: It is entropybased coding technique that is commonly used for compression of the data in a lossless manner. This technique uses the frequency of occurrence as reference to design a variable-length key based lookup-table for coding that original information. The success of the coding largely depends on the lookup-table determined from the original information which is obtained based on the frequency of occurrence for each possible value. Figure 2(a) and 2(b) shows the flow chart for Huffman encoding and decoding process respectively.

Huffman coding exploitsa generalized approach for the selection of each possible value and establishes a corresponding prefix code that can comprehend all the possible values existing in the original information in consideration. The coding starts with smaller prefix code employed for values that are having higher frequency and as the frequency of the value decreases the coding string increases [15]. This approach was able to devisea most efficient coding framework in which no two possible values will have the same prefix code determined from the look-up table. These unique codes of bits will produce a data which is of the smaller size and completely different from the original information, when the actual value frequencies comprehend with the prefix-codes in the look-up table the code can be decoded [16-17].

The encoding process of Huffman's method is fairly efficient; it takes $O(n \log n)$ operations to code the complete original information [18-19]. In general, this approach offers the optimal manner to take benefit of the changing frequencies values in an information stream. It is evident that this approach operates on the range of 10% to 30% compression ratio but the encryption largely depends on distribution of the information. The prime concept that drives this coding technique is based on mapping the less frequency values with a larger prefix code from the determined look-up table and smaller prefix code for high frequency values. In addition, the entire coding is mapped based on the look-up table which has unique code for each value. This property about the code is crucial with respect to easily deciphering the code [20-21].

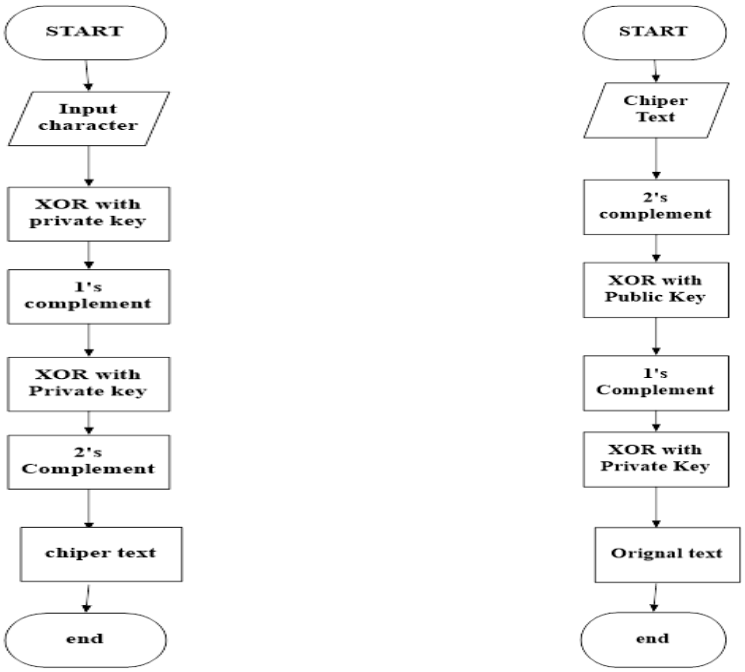


(a) (b)

Figure 2. (a) The Flow Chart of Huffman Encoding (b) The Flow Chart of Huffman Decoding

Binary Coding: Binary encryption is an algorithm which is used to code and decode the secured data using asymmetric encryption algorithm where it uses both private and public key. It is easy to read for system

while decrease with the complexity. Binary encoding and decoding flow charts are shown in Figure 3(a) and 3(b) respectively.



(a) (b)

Figure 3. (a) The Flow Chart of Binary Encoding (b) The Flow Chart of Binary Decoding

4. PROPOSED ALGORITHM

The major focus of this Section was to design and develop an innovative novel framework that exploits various factors to provide reliable and robust D2D communication based on the existing network constraints and improve packets transfer rate while minimizing the load existing communication infrastructure. The basic procedure for encoding and decoding the digital information using proposed algorithm is presented in the Figure 4 and Figure 5 respectively. In addition, the approach generates a binary code using the particular defined input factors.

HYBRID ENCRYPTION ALGORITHM
Step: 1 Enter the input data.
Step: 2 Input data goes to binary mode.
Step: 3 In binary first is xor private key.
Step: 4 find the 2's complement.
Step: 5 find the 1's complement.
Step: 6 find the xor with public key .
Step: 7 chipper text .
Step: 8 Now applying Huffman on chipper text.
Step: 9 Read character from database
Step: 10 Replace the character match in data base.
Step: 11 Save that in file.
Step: 12 chipper text got.

HYBRID DECRYPTION ALGORITHM
Step: 1 input the chipper text.
Step: 2 search the encode from database.
Step: 3 match the code and paste in place of that character and put required character.
Step: 4 find the xor with public key.

Step: 5 find the 1's complement.
Step: 6 find the 2's complement.
Step: 7 find the xor with private key.
Step: 8 Original texts found.

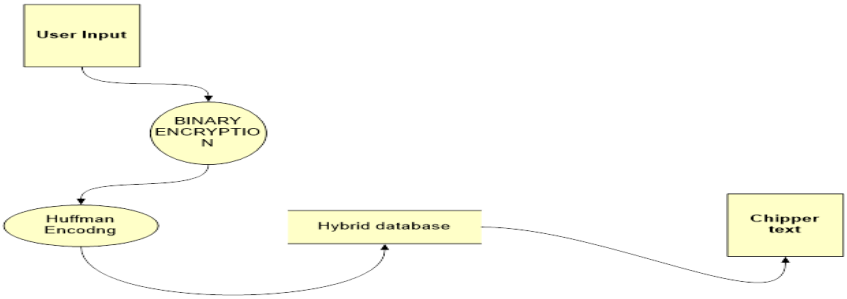


Figure 4. Encoding Process of the Hybrid Cryptographic System

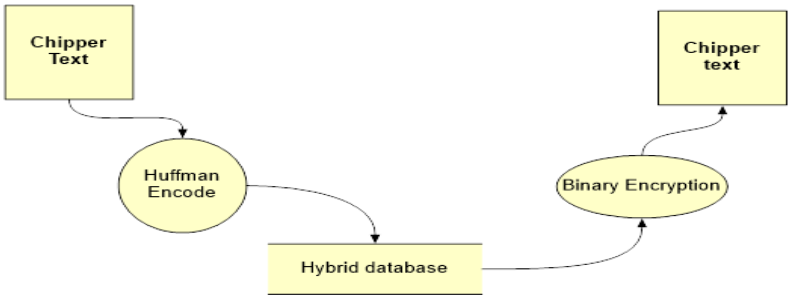


Figure 5. Decoding Process of the Hybrid Cryptographic System

5. SIMULATION AND RESULTS

This Section presents with the experimentation analysis and corresponding test results of proposed Hybrid encryption system. These simulations were replicated using JAVA programming based development environment. Analysis and testing was done in a phased manner using text data of varying sizes and classes of features. They were analyzed for robustness of the proposed algorithm.

5.1. Phase-1 Class Diagram

The class diagram is considered as the prime building block of any object oriented modeling. It is primarily employed for both conceptual and detailed modeling of the application wherein the diagram translates the operations into corresponding programming code. Further, they could be effectively employed for conceptual data modeling based applications. A relationship of the proposed hybrid encryption algorithm using the class diagram is illustrated in the Figure 6, the specific attributes and operation connection are found on class and objects diagrams. Moreover, the classes in a class diagram represent both the main objects, interactions in the application and the classes to be programmed.

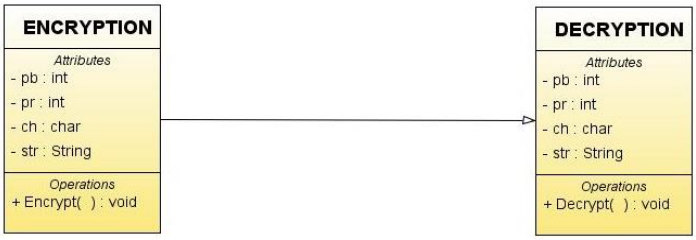


Figure 6. Class Diagram of the Hybrid Encryption Algorithm

5.2. Phase 2 Snap Shots

The results of simulation is represented in this phase as snap shots. Figure 7 represents the initial step of simulation, which requires name and password of an authenticated user to encode and decode the information using proposed algorithm. Next step in simulation is the selection of encoding or decoding stage as shown in Figure 8. The final step is to apply the proposed hybrid cryptographic algorithm for encoding or decoding as shown in Figure 9 or Figure 10 respectively.

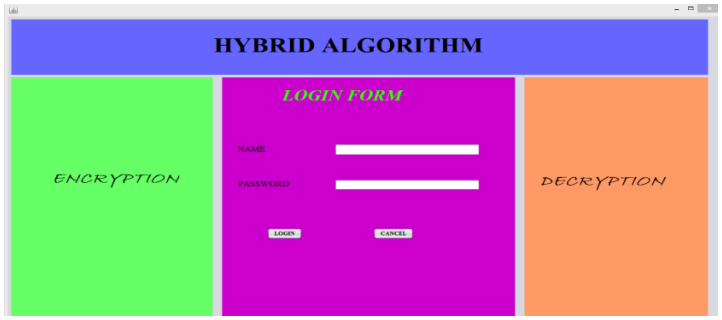


Figure 7. GUI of Hybrid Cryptographic System

Figure 8. Basic GUI of Selection of Sender and Receiver Algorithm

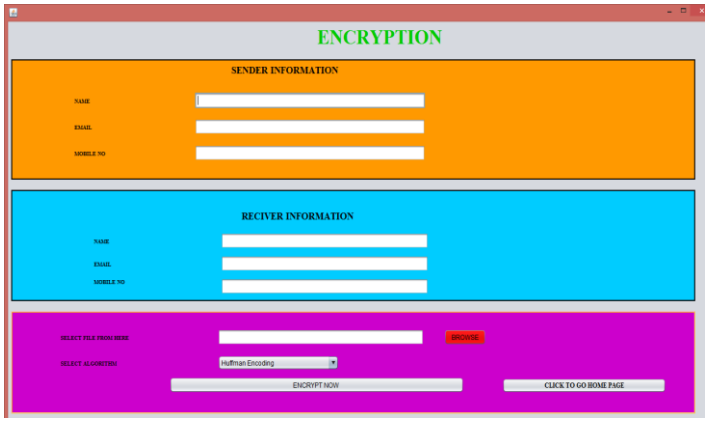


Figure 9. GUI of Encoding Process for Hybrid Cryptographic System

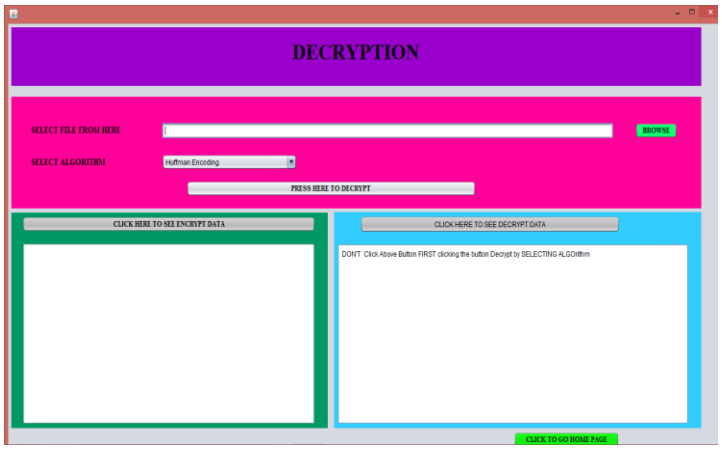


Figure 10. GUI of Decoding Process for Hybrid Cryptographic System

5.3. Phase 3 Numerical analysis

Table 1 shows the comparative analysis of the proposed algorithm with well-known RMSE algorithm for information containing: only characters, only numbers or both.

Table 1. Comparison of RMSE of the Color Images between Binary Coding and Proposed Hybrid Algorithm

File Size	RMSE Encrypt			RMSE Decrypt			Binary Encrypt
	Numbers	Char	Both	Numbers	Char	Both	
2KB	11.7150	11.2900	10.7950	0	0	0	9.7709
5KB	12.0010	11.4710	11.1560	0	0	0	10.1848
10KB	11.6590	11.4720	11.2560	0	0	0	9.6624
20KB	13.2430	13.4360	13.2440	0	0	0	10.1311
36KB	13.4140	13.7040	13.5670	0	0	0	10.3210
50KB	12.5470	12.5590	12.2390	0	0	0	8.6801

6. CONCLUSION

In this paper, we presented a new hybrid cryptographic system based on Huffman coding and Binary that could improve the security of the information being transmitted over multi-hop D2D communication channel. The proposed systems used a combination Huffman algorithm and Binary algorithm for higher efficiency in block encryption and covertkey agreement protocols. Henceforth, the significant advantages of using Huffman coding and Binary algorithm will ensure that the information transmitted in more covertly manner over the D2D channel. Experimental results prove that the proposed approach is robust, lossless in nature, and can effectively manage the network's traffic issues. Moreover the proposed algorithm proves that the D2D communication is feasible to operate independently or in collaboration with the existing infrastructure based communication system.

In addition, encryption on media file convert it into a binary format and it is easy to understand by system and both algorithm based on these binary number it take less time to encrypt and decrypt from another algorithm. Further, the proposed system is lossless in nature i.e., the decrypted information and original information would same with no distortion.

REFERENCES

[1] F. C. Cheng and S. Tatesh. "Secure Device-to-Device (D2d) Communication," U.S. Patent No. 20,150,326,537, 2015.
[2] L. Goratti, *et al.*, "Connectivity and security in a D2D communication protocol for public safety applications," in *Wireless Communications Systems (ISWCS), 2014 11th International Symposium on*, pp. 548-552, 2014.
[3] J. L. Massey, "Some applications of source coding in cryptography," *Euopean Transaction on Telecommunication*, vol. 5, pp. 421–429, 1994.
[4] J. Knudsen, "Java Cryptography," O'Reilly and Associates, Inc., 1998.
[5] H. Delfs and H. Knebl, "Introduction to Cryptography," Springer, 2007.
[6] "Huffman coding and encryptions methods," *International Journal of Computer Science and Information Security*, vol/issue: 8(9), pp. 195–199, 2010.

[7] A. Y. E. Nesterenko and A. V. E. Pugachev, "A new hybrid encryption scheme," *Prikladnaya Diskretnaya Matematika*, vol. 4, pp. 56-71, 2015.
[8] E. Persichetti, "Secure and anonymous hybrid encryption from coding theory," in *Post-Quantum Cryptography*, Springer Berlin Heidelberg, pp. 174-187, 2011.
[9] W. Shen, *et al.*, "Secure key establishment for device-to-device communications," in *Global Communications Conference (GLOBECOM), 2014 IEEE*, pp. 336-340, 2014.
[10] E. A. Elrahman, *et al.*, "D2D group communications security," in *Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015 International Conference on*, pp. 1-6, 2015.
[11] E. A. Elrahman, *et al.*, "Fast group discovery and non-repudiation in D2D communications using IBE," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International*, pp. 616-621, 2015.
[12] K. Rege, *et al.*, "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA," *International Journal of Computer Applications*, vol/issue: 71(22), 2013.
[13] X. Lu, *et al.*, "Related-key security for hybrid encryption. InInformation Security, Springer International Publishing, pp. 19-32, 2014.
[14] H. Kwon, *et al.*, "Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks," *Multimedia Tools and Applications*, pp. 1-15, 2016.
[15] R. L. Rivest, *et al.*, "On breaking a huffman code," in *Proc. IEEE Transactions on Information Theory*, vol/issue: 42(3), 1996.
[16] N. Lee, *et al.*, "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," *Selected Areas in Communications, IEEE Journal on*, vol/issue: 33(1), pp. 1-13, 2015.
[17] Y. Liu, *et al.*, "Secure D2D communication in large-scale cognitive cellular networks with wireless power transfer," in *Communications (ICC), 2015 IEEE International Conference on*, pp. 4309-4314, 2015.
[18] H. Kwon, *et al.*, "Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks," *Multimedia Tools and Applications*, pp. 1-15, 2016.
[19] S. Nagaraj, *et al.*, "A Bio-Crypto Protocol for Password Protection Using ECC," *Bulletin of Electrical Engineering and Informatics*, vol/issue: 4(1), pp. 67-72, 2015.
[20] C. Meshram, "Discrete Logarithm and Integer Factorization using ID-based Encryption," *Bulletin of Electrical Engineering and Informatics*, vol/issue: 4(2), pp. 160-168, 2015.
[21] T. N. Babu, *et al.*, "Ortho Linear Feedback Shift Register Cryptographic System," *Journal of Telematics and Informatics*, vol/issue: 3(2), 2015.