Available online @ https://jjem.jnnce.ac.in
https:www.doi.org/10.37314/JJEM.2022.060109
Indexed in International Scientific Indexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 31July 2022

Securing D2D Communication using Lightweight Cryptography

Ajith Kumar V[1]*, K Satyanarayan Reddy[2]

[1*]Research Scholar VTU RRC Belgaum, [2]Professor & Head ISE Department Cambridge Institute of Technology, Bangalore

ajith.it@gmail.com, ksatyanreddy@gmail.com

Abstract

D2D communication is going to be a path breaking technology. D2D communication can help in many scenarios including Emergency Service. The D2D communication is having a lot of potential to serve community either through emergency services and commercial or paid services. Security and privacy are two important issues in D2D communication. The Objective of this paper is to explore security challenges in D2D communication and suggest remediation with lightweight cryptography. Evaluation of wireless network leads to massive load on the service provider network. The D2D communication can be the choice for offloading the traffic from the service provider network. Security should not become overhead, lightweight cryptography techniques can be explored to support resource constrained devices. Enough care is to be taken for not compromising security and by using lightweight cryptographic techniques. As we know some attacks such as Denial of Service (DoS) cannot be completely prevented but can be mitigated. In this paper we compared existing work on providing security for D2D communication. There is no single solution which can address security for various D2D communication scenarios such as full coverage, partial coverage, and no coverage. This gives a clear indication that a set of security solutions is required to address different D2D scenarios, each D2D scenario come with its own challenges. In this work we are proposing encryption mechanism using lightweight cryptographic approach. Proposed encryption mechanism is targeted for low-end resource constrained devices. Although Bluetooth and Wi-Fi technology provides minimum security, our scheme can be used to provide additional security for data transmission. We extend our work by breaking different D2D scenarios and proposing appropriate solution for each scenario.

Keywords: *D2D communication security, Lightweight cryptography, Resource constrained devices*

1. Introduction

D2D communication will be a path breaking technology. D2D communication can help us in situations such as Emergency Service. D2D connectivity has many opportunities to help the community through emergency services and commercial or paid services. The outbreak of Mobile Communication, where users are no longer tied to Public Switched Telephone Network (PSTN) line services provided provides many opportunities for service providers. Evolution for Wireless Technology starting from 2G, 3G, 4G and now the world is moving towards 5G.

The D2D network attracted researchers and academics. One can find many books related to D2D communication. Most of the research focused on resource allocation, mode selection, QOS verification. However, more focus is needed on the management of D2D communication features. D2D connectivity is wireless, benefiting most of the security challenges common to this sector. Additionally, D2D connectivity has both local features as a node in the Mobile Adhoc Network (MANET) while simultaneously a D2D node can be a node in a Service Provider network. Security challenges in D2D connectivity can be considered with major security challenges in the wireless network and security challenges in MANET.

Key challenges in wireless communication. In a wireless network of communication, most of these activities will be handled by the service provider. These services are paid for by end users as well as a major source of revenue for the service provider. In this case most of the difficulties handled by the Service Provider and User Equipment will be relieved of all such overhead. However, in the case of the Mobile Adhoc Network all these activities are performed in an infrastructural manner, where there is no service provider. MANN sites are complex to handle issues of acquisition, registration, authentication and routing Technologies like D2D communication can only be accepted by the general public if it is not expensive. The economy plays a major role. The cost of the device is equal to the difficulty it can handle. At the same time Government regulations mandate the adoption of technology. Technology is often viewed as a two-edged sword, as it can be used for good or for bad. MANET receives most of its applications in the Military or Defense Forces. For the successful adoption of D2D communications, vendors must maintain a complex and legitimate use as per the practices set by the Public Authorities.

D2D communication paradigm opens several new avenues for data sharing between devices which are directly communicating with each other. The advantages of D2D communication are traffic offloading, high data rate and efficient use of spectrum and besides enhancing spatial efficiency. It also improves throughput, efficiency, and delay [1]. Evolution of 2G, 3G wireless networks lead to revolution, which resulted in increased usage of mobile phone. Vendors started offering new services to capture the market. Data sharing became a very common phenomenon, Bluetooth, Wi-Fi already exist to support such requirement. If we look at the evaluation of wireless networks, First generation supported analog telephone service without any support for data communication. Second generation supported data rate up to 250 kbps with voice, text, and data services. Third generation technology marked the beginning of Smart Phones, and this technology provided high data at lower rate. Fourth generation technology offered high speed, high quality, and higher capacity services such as IP Telephony, high definition mobile TV. Fifth generation is expected to support higher connectivity, and support for connecting heterogeneous devices. As we move higher up in technology ladder, security challenges also increase.

D2D communication got Industry and Academia attention long back. Qualcomm has introduced effective D2D communication with FlashLinQ (FLQ) in Orthogonal Frequency Division Multiplexing (OFDM) based wireless networks. Lot of research work is being carried out in some specific areas like resource allocation, mode selection, QoS, bandwidth allocation and related parameters. Several research papers are available in literature. We are not attempting for another survey on D2D communication but the effort is focused on presenting an overview of security challenges in D2D communication. One distinct difference between D2D and MANETs is the communication spectrum. MANETs work mainly on an unlicensed spectrum making spectrum control difficult and interference a major issue [8]. In contrast, D2D can use both a licensed and an unlicensed spectrum depending on the usage. The control mode is also different. In MANETs each node performs system operations autonomously, whereas in D2D the operations can be performed through the cooperation between D2D nodes or using cellular infrastructure. In addition, the routing patterns vary. D2D uses mainly single hop transmission, instead of multi-hop routing commonly used in MANETs [8].

Standards play important role for the development of communication technologies.

ETSI standards are helping extensively for the development of communication standards, such as Internet Of Things(IOT), Wireless Communication, Machine to Machine Communication and Cyber Physical Systems. ETSI 3rd Generation Partnership Project (3GPP) published Technical Specification for Evolved Packer System (EPS) based Release 13 which added support for other D2D functions and unveiled the first set of specifications covering mission critical services. Release 14, brought about a series of Mission Critical enhancements, LTE support for V2x services, eLAA, 4 band Carrier Aggregation, inter band Carrier Aggregation and more Release 15 includes work on 5G System-Phase 1, Machine-Type Communications (MTC) and Internet of Things(IoT),Vehicle-to-Everything Communication (V2X) improvements Release 16 includes work on the work on 5G System Phase 2, V2X Phase 3, Industrial IoT, Satellite Access in 5G Release 17 more 5G system enhancements are set to follow in Release 17, scheduled for delivery in 2021.

3GPP specification release 12 which laid down basic functionalities for D2D communication such as Proximity services (Prosec) was not only for public safety, also covers D2D extension of conventional cellular services [6]. 3GPP standard release and their features are shown in table 1.

Table 1: 3GPP Standard Release

Release	Features
Release 12	Proximity Services Device to Device Communication (D2D)
Release 13	Enhanced ProSec
Release 14	LTE support for V2X services
Release 15	5G System - Phase 1, MTC, IoT and V2X improvements
Release 16	5G System - Phase 2, V2X Phase 3, Industrial IoT
Release 17	5G System Enhancements

1.1 D2D Scenarios

D2D communication can be categorized into single hop D2D communication and multihop D2D communication. In case of the single hop D2D communication two devices such as User Equipments (UEs) directly communicate with each other. In this kind of scenario message routing is not required. However mutual authentication and key exchange is required before starting any data communication. In case of multi-hop D2D communication, message has to be relayed between source and destination devices with the help of intermediate devices. In this kind of scenario, message routing may be required. Most popular way of handling multi-hop D2D communication is using techniques like Cluster formation and cluster head will be responsible for handling communication on behalf of the cluster. D2D communication being a wireless communication, inherits most of the security challenges prevalent in this field.

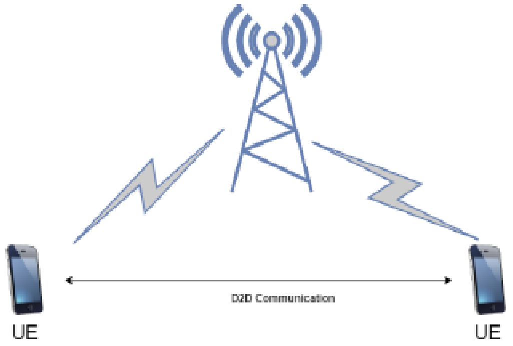


Figure 1: Cellular and D2D communication

Additionally, D2D communication has characteristics of both autonomous node like node in Mobile Adhoc Network (MANET) at the same time D2D node can be node in Service Provider network. Security challenges in D2D communication can be thought of as a super set of security challenges in wireless network and security challenges in MANET. D2D communication is vulnerable to various attacks; primarily it lacks centralized control, and D2D communication also inherits all security risks which exist in wireless networks [11].

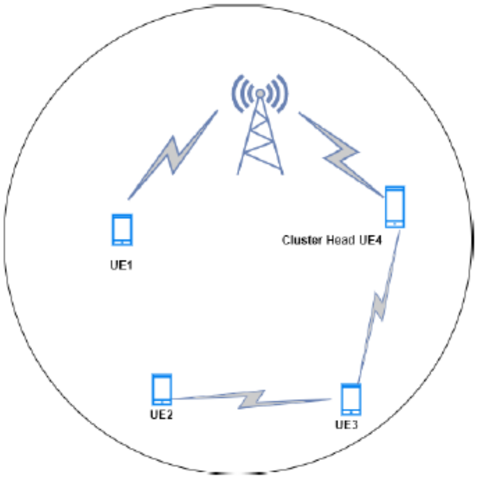


Figure 2: Cellular and D2D communication

As shown in Figure 1 D2D Communication and Cellular communication can happen between two UEs, in this case UE1 can directly communicate with UE2 using D2D communication, which results in offloading the traffic from the service provider core network. However, in Figure 2 UE2 is communicating with UE4 using D2D communication, in this scenario UE2 is under partial coverage, hence it requires an intermediate node UE3 which relays messages between UE2 and UE4.

1.2 Security Challenges in D2D Communication

Confidentiality, Integrity and Availability are main the ingredients for secure communication. Confidentiality is breached when sensitive information is disclosed to an unauthorized entity. Integrity is breached when original message is modified by an unauthorized entity. Finally, Availability is impacted when resources are not available to authorized entities due to Denial of Service (DoS) [7] attack by an intruder. Security threats can be different, based on D2D scenarios, such as single-hop D2D communication or multi-hop D2D communication.

As shown in figure 3 Confidentiality, Integrity and Availability are important factors for securing the communication.

Confidentiality
Integrity
Security Goals
Availability

Figure 3: CIA Triad.

In case of multi-hop D2D communication, an intermediate node can launch data injection attack, by forwarding false data. This type of attack is insider attack [10], which compromises with message integrity. In such cases security can be ensured by authenticating each message by all the intermediate UEs. The Cryptographic Key agreement is very important requirement for achieving authentication and confidentiality in scenarios like D2D communication. Several cryptographic key algorithms were proposed for securing D2D communication, some research focused on usage of asymmetric key algorithms such as RSA, whereas some research focused on combination of asymmetric and symmetric key algorithms, where asymmetric key algorithms were initially used to exchange symmetric keys between D2D nodes. The latter approach is an attempt to make use of the advantage of both symmetric and asymmetric key cryptography. Such combination includes RSA, DH with other combination of protocols. In some research work ECC which is a public key cryptosystem is used for secure exchange of symmetric key.

2. Literature Survey

Some novel approaches have also been taken for securing D2D communication, where public key-based signature and symmetric encryption algorithms are used together [2] to ensure security. Major security challenges in

D2D communication include device discovery, identification and authentication of the device or user. Identification and authentication always occur together as a single two-step process. Identification and authentication are very important decisive factor for accepting or rejecting communication request from another entity. The Interesting factor about D2D communication is security scope. As we can see from the different findings, some work focuses only on secure exchange of key which can be used for encryption and decryption of the messages, while some other work focusses only on user authentication. But there are only a few works which focus on end-to-end encryption. In this way we can say that some solutions are partial and not complete.

Sedidi R. et al., proposed key exchanged protocol suitable for D2D communication in 5G wireless network. The proposed protocol is based on the standard Diffie-Hellman (DH) based key exchange and other cryptographic functions. Proposed protocol is resilient against Man-in-the-middle attack. Although simulation results show that proposed protocol is having less communication overhead in terms of communication cost and computing time [9]. However, this protocol does not address other aspects of security.

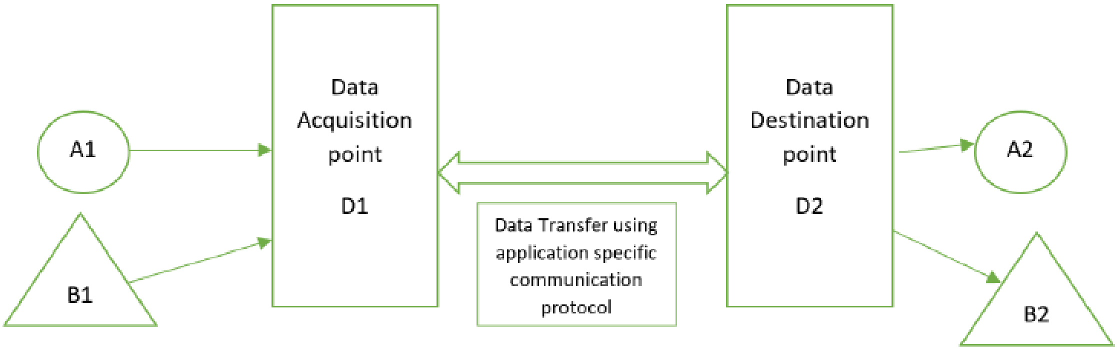

A1
B1
Data Acquisition point
D1
Data Transfer using application specific communication protocol
Data Destination point
D2
A2
B2

Figure 4: Device-to-Device Communication

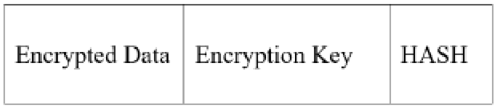
Zhang et al., [2] focus on providing security against free-riding attack. But this algorithm suffers from a lot of overhead such as keeping a track of communicating entities. Here the data is signed first by the provider and then by the sender to achieve transmission non-repudiation, for ensuring receiver non-repudiation, receiver has to send hint for decryption algorithm. Free-riding attack is tied with system availability. Mutual data sharing is good; however, this cannot be the sole criteria or pre-condition for any data sharing algorithm. Additionally, for secure data exchange this protocol involves eNB and Gateway (GW) which defeats the objective of offloading the cellular network. Effect of mobility on security in D2D communication is not explored. In this work, Computational overhead and Communication overhead are used as parameters. Data can be shared on need basis, importance of data, also could be based on circumstances such as emergency service.

User Equipment (UEs) play major role in securing D2D Communication. UEs are high end devices with sufficient computational and storage capabilities. UEs are responsible for registration, initial key exchange, mutual authentication, and secure key exchange phases of D2D communication. The new network paradigm, 5G network supports communication with heterogeneous devices. In 5G network, which supports connecting heterogeneous devices, additional security challenges can be anticipated. Some devices might be constrained by resources such as computation and storage space. On such low-end devices providing security could be a challenge.

As shown in Figure 4, a system is proposed where Data can be aggregated from several low-end devices. UE can act like an aggregation point. Some scenarios could be data generated by wrist band can be collected by UE. Some smart devices which can collect and transmit heartbeat, temperature can be pushed to UE. This use case is similar to Wireless Body Network(WBNs).

3. System Design

Some low-end devices could support only simplex communication, in such scenarios, key exchange is a big challenge. In such scenarios, encrypting the data should be carried out at the source, key can be generated using some trivial techniques, however key should be transferred along with the data. Typical data packet format for such communication could be given in this format.



Encrypted Data	Encryption Key	HASH

Figure 5: Data Frame format for simple encryption.

As shown in Figure 5, for a simple encryption, we can use a frame format which carry Encrypted data, encryption key and hash for message integrity in the same frame. In above sample scenario, data which is being encrypted by the sender is encrypted using a key which is also generated by the transmitting device. However, there is no concept of key exchange between sender and receiver devices. Key is sent along with the encrypted data. Receiving device should extract the key from the data packet itself. Such arrangements are justifiable when sender is using a low-end device and can support only simple communication. If we send key along with the data, there are two options. The first option would be sending the encryption key in control field such as header and the second option would be sending the encryption key in the payload. If the encryption key is sent in control field, more processing is required on the receiving side, receiving device must extract encryption key from the control field and then the same can be used for decrypting the payload. As per the second option, if encryption key is sent in payload along with the data, some additional protection can be used such as generating the Hash for the encrypted data and encryption key. This Hash can be appended at the end of data frame, receiver can compute the hash function locally and proceed with extracting encryption key and decrypt the message if and only if there is a match in hash function.

Chien-Ming Chen et al., [5] proposed human verifiable protocol for securing communication for mobile devices. This protocol is aimed at defending against Man-in-the-middle attack. However, this cannot be directly used in D2D scenarios. Keyless encryption is another paradigm where encryption key is not at all used. Akhil et al., [4] proposed keyless encryption scheme, which was implemented for character level, block level and binary level. This scheme could be useful for ensuring secure communication for low-end devices, which are constrained by the computational and storage capabilities. However, additional investigation needs to be done to check whether proposed scheme can withstand against brute force attack. There are some key challenges in adopting keyless encryption. As per the established principles of cryptography encryption algorithm is made public so that it will be subjected to security analysis by various researchers working in this area.

As shown in Figure 6, Data acquisition and data distribution can happen with multiple devices. In this case A1 is generating the data, data is acquired by the system, however on the other hand B1 is receiving the data from the device.

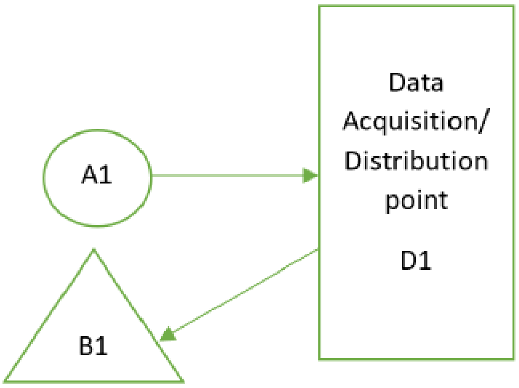


Figure 6: Data acquisition and distribution point.

However, strength of the encryption algorithm lies with the encryption key. The Algorithm is public, and the key is private, however in key-less encryption, there is no concept of encryption key. If the algorithm is published then it will be difficult to maintain the secrecy. Secrecy is to be handled in such a way that the published algorithm does not compromise on security.

4. Security Requirements

There are devices constrained with power, memory, and computing power. These devices generate continuous data such as wrist bands, medical sensor devices Data is collected and transmitted from these devices lacks security Example applications file sharing over Blue-tooth, Wi-Fi interfaces. There are many low-end devices lacks security. Our aim is to provide Security for the data collected from the end devices. This can be achieved by following certain methodologies, where Data is collected and aggregated at the first point.

After collecting such data, raw data is being processed. This processing could be something like enhance the strength of the binary information contained in the data. Raw data is then encrypted using lightweight cryptographic techniques. As in case of any standard encryption, encryption is done at the source, encrypted data is transmitted based on the target applications - Blue tooth, Wi-Fi and so on. Our algorithm is based on maintaining code book at source as well as destination.

Encryption is done character by character using X-OR operation with the encryption key. At the receiving end Data is being decrypted using the same X-OR operation. After the Data is being decrypted, it is fed to the respective application. High level system design for our implementation is shown in Figure 7.

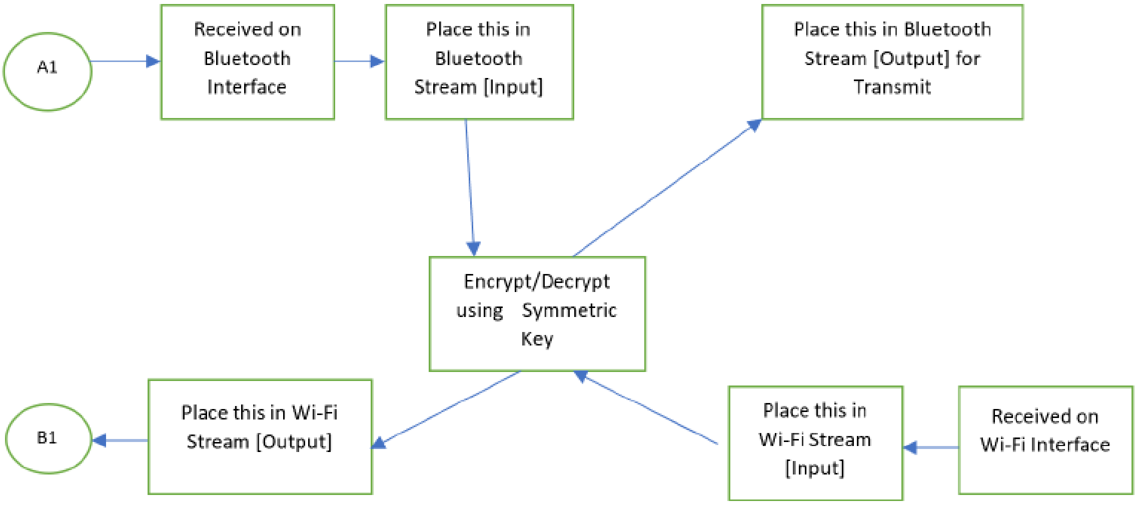

A1
Received on Bluetooth Interface
Place this in Bluetooth Stream [Input]
Place this in Bluetooth Stream [Output] for Transmit
Encrypt/Decrypt using Symmetric Key
B1
Place this in Wi-Fi Stream [Output]
Place this in Wi-Fi Stream [Input]
Received on Wi-Fi Interface

Figure 7: High Level System Design.

A1 is a data generating device connected to Bluetooth interface, hence data will be placed in a stream dedicated for Bluetooth, similarly B1 is a target device connected via Wi-Fi network, receives data sent from anther device connected to Wi-Fi network. Irrespective of whether device is connected to Bluetooth or Wi-Fi, encryption and decryption is taken care by the UE itself, in this way end devices are relieved from the overhead of mathematical computation required for encryption and decryption, storage space required for storing encryption and decryption keys. Symmetric key encryption is ideal for such situation as same key is being used for both encryption and decryption.

Lightweight protocol for securing D2D communication should be capable of detecting whether the data is altered by attackers, should be able to achieve mutual authentication between the sender and receiver, the computational and communication cost should be low, and the protocol should be robust enough to face the threat when part of the keys are exposed [3].

4.1 Proposed Algorithm

a. Data will be identified as different streams based on the communication interface
b. Data received from A1 intended for Bluetooth communication will be treated
c. as one stream, whereas data destined from B1 over Wi-Fi channel will be treated as different stream
d. Since we are using symmetric key encryption, encryption and decryption can be treated as follows
e. Raw data + Encryption Key → Encrypted data
f. Encrypted data + Encryption Key → De-crypted data
g. Here `+' operation with symmetric key results in either Encrypted data or Decrypted data depending on the input.

4.2 Algorithm for encryption

Input: Raw Data
Output: Encrypted data, array index

```
1: Generate array of MaskBits
2: Index to this array is generated based on the in
   put text
3: Compute SkipCount
4: Encrypt the character by X-ORing the character
   with key
5: Find new index by adding SkipCount to the
   index
6: Repeat Step 3 and 4 for each character input
7: Encrypted data will be written to a file
8: Transmit the file to receiver
```

4.3 Algorithm for decryption

Input: Encrypted data, array index
Output: Decrypted original data

```
1: Read encrypted data
2: Generate array of MaskBits
3: Index to the MaskBits is computed
4: Compute SkipCount
5: Decrypt the character by X-ORing encrypted
   character with MaskBits[Index]
6: Compute new index by adding SkipCount
7: Repeat Step 5 and 6 for each encrypted character
8: Write decrypted characters to a file.
```

4.4 Key Features

Proposed system is unique based on below factors

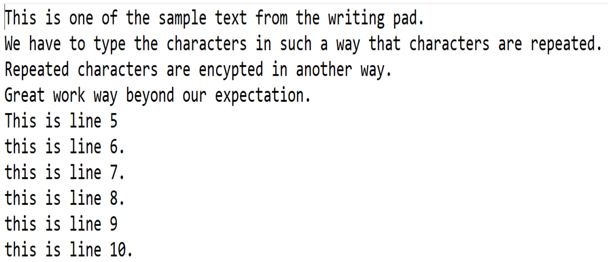
a. Securing D2D communication using lightweight cryptographic techniques
b. Mutual authentication of high-end devices (UE's) , followed by key exchange
c. Data collected from different sources are treated separately, placed in different streams, treated with same encryption and decryption algorithm
d. Adds security layer for all low-end devices
e. There are many protocols supporting security features for high-end devices in 4G/5G technology
f. Our objective is to provide security for the low-end resource constrained devices by aggregating data from those devices, do bit of pre-processing, encrypt data and transfer using specific technology such as Bluetooth or Wi-Fi
g. In case Bluetooth and Wi-Fi technology provide some security, our implementation,

will provide additional security on the top of it

4.5 Implementation Details

Lightweight encryption algorithm has been developed and tested. This algorithm has been implemented using Python 3 and tested on Intel(R) Core(TM) i7-9850H CPU @ 2.60GHz 2.59 GHz, installed with 32 GB RAM running Windows 10 Operating System.

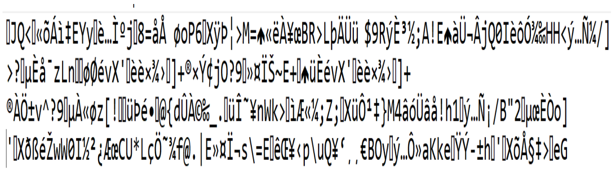
a. Symmetric key algorithm
b. Pre-shared keys
c. Only key index is transmitted along with the message
d. Computationally key index is derived.
e. Computationally efficient than other symmetric key algorithms
f. MaskBits are populated randomly, and this order can be changed
g. Each byte is having uniformly distributed number of bit 1's and bit 0's
h. This algorithm encrypts and decrypts one byte at a time, hence can be used for encrypting text, audio and image files.



```
This is one of the sample text from the writing pad.
We have to type the characters in such a way that characters are repeated.
Repeated characters are encypted in another way.
Great work way beyond our expectation.
This is line 5
this is line 6.
this is line 7.
this is line 8.
this is line 9
this is line 10.
```

Figure 8: Sample Input Data for encryption

Using proposed algorithm sample text has been encrypted. Figure 8 shows sample input data used for encryption.



```
□JQ<□«õÁì‡EYy□è…Ìºj□8=åÅ ϕoP6□XÿÞ¦>M=↑«ëÀ¥œBR>LþÄÜü $9RýÈ³½;A!E↑àÜ¬ÂjQ0IèôÓ¾‰HH<ý…Ñ¼/]
>?□µÈå¯zLn□□øØévX'□èèx¾›□]+®xÝ¢jO?9□»¤ÏŠ~E+□↑üÈévX'□èèx¾›□]+
®ÀÖ±v^?9□µÀ«øz[!□□üÞé•□@{dÛÀ©‰_.□üÎ˜¥nWk>□ìÆ«¼;Z;□XüÔ¹‡}M4âóÜâå!h1□ý…Ñ¡/B"2□µœÈÒo]
'□XðßéŽwW0I½²¿ÆœCU*LçÖ˜¾f@.|E»¤Ï¬s\=E□êŒ¥‹p\uQ¥ʻ,,€BOy□ý…Ô»aKke□ŸÝ-±h□'□XõÅ§‡>□eG
```

Figure 9: Encrypted Data output

Figure 9 shows encrypted output. Close observation of the encrypted text shows that it is difficult to guess the plain text by looking at the encrypted text. This is one of the most desirable characteristics for robust encryption scheme.

5. Performance Analysis

Initial results are encouraging which reveals that 23 Milliseconds required for encrypting 127 KB of text data and same amount of time required for decrypting message. However, this algorithm is taking 81 Milliseconds for encrypting 445 KB digital image data. We can further optimize this algorithm and apply this to various D2D communication scenarios as well.

6. Conclusion

D2D communication presents unique opportunities and security challenges as well. Upcoming 5G technology supports connectivity and co-existence of heterogeneous devices, in such scenario, proposed security algorithm can play major role in securing the communication. Encryption algorithm proposed in this paper is very much efficient for protecting communication between low end devices. The entire world is moving towards 5G Technology, however, still there is a need to protect communication between two low end or resource constrained device. Proposed algorithm can be used to protect low-end, resource constrained devices in turn serves as additional layer of protection for such devices.

References

1. A. Asadi, Q. Wang, V. Mancuso, A Survey on Device-to-Device Communication in Cellular Networks, IEEE Communications Surveys & Tutorials, Vol.16, 2014, pp.1801-1819.
https://doi.org/10.1109/COMST.2014.2319555

2. A. Zhang, J. Chen, R. Q. Hu, Y. Qian, SeDS: Secure Data Sharing Strategy for D2D Communication, IEEE Transactions on Vehicular Technology, Vol.65, No.4, 2016, pp. 2659-2672.
https://doi.org/10.1109/TVT.2015.2416002

3. A. Zhang, L. Wang, X. Ye, X. Lin, Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems, IEEE Transactions on Information Forensics and Security, Vol.12, No.3, 2017, pp. 662-675.
https://doi.org/10.1109/TIFS.2016.2631950

4. Akhil Kaushik, Satvika, Manoj Barnela, Anant Kumar, Keyless User Defined Optimal Security Encryption, International Journal of Computer and Electrical Engineering, Vol.4, 2012, pp.99-103.

5. C. Chen, K. Wang, T. Wu, J. Pan, H. Sun, A Scalable Transitive Human-Verifiable Authentication Protocol for Mobile Devices, IEEE Transactions on Information Forensics and Security, Vol.8, No.8, 2013, pp.1318-1330. https://doi.org/10.1109/TIFS.2013.2270106

6. Höyhtyä M, Apilo O, Lasanen M, Review of Latest Advances in 3GPP Standardization: D2D Communication in 5G Systems and Its Energy Consumption Models, Future Internet, 2018.
https://doi.org/10.3390/fi10010003

7. Yasir Javed, Adnan Shahid Khan, Major Security attacks in D2D Communication, Ubiquitous Computing and Communication Journal, Vol.1, 2019.

8. Wang, M, Yan, Z, A Survey on Security in D2D Communications, Mobile Networks and Applications, Vol.22, No.2, 2017, pp.195–208. https://doi.org/10.1007/s11036-016-0741-5

9. R. Sedidi, A. Kumar, Key exchange proto-cols for secure Device-to-Device communication in 5G, Proceedings of the International Conference on Wireless Days (WD), 23-25 March 2016, Toulouse, France, pp.1-6.
https://doi.org/10.1109/WD.2016.7461477

10. Sencun Zhu, S. Setia, S. Jajodia, Peng Ning, An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. IEEE 22nd International Symposium of Quality of Service (IWQoS)Proceedings, 12-12 May 2004, Berkeley, CA, USA, pp.259-271.
https://doi.org/10.1109/SECPRI.2004.1301328

11. Xi, Wei & Li, Xiang-Yang & Qian, Chen & Han, Jinsong & Tang, Shaojie & Zhao, Jizhong & Zhao, Kun. KEEP: Fast secret key extraction protocol for D2D communication, IEEE International Workshop on Quality of Service, IWQoS, 26-27 May 2014, Hong Kong, pp.350-359.
https://doi.org/10.1109/IWQoS.2014.6914340