Comparative Analysis and Integration of Other Technologies for Enhancing Device-to-Device (D2D) Security Using Hybrid Method

[1]Chaithanya D.J. [2]Dr. Anitha S

[1]Research Scholar
ACS College of Engineering, Bangalore
Visvesveraya Technological University,
Belagavi-590018
rcchaithudj@gmail.com

[2]Research Supervisor
Dept. of Electronics and Communication Engineering,
ACS College of Engineering, Bangalore
Visvesveraya Technological University,
Belagavi-590018
dranithasammilan@gmail.com

Abstract: With the advent of 5G networks, Device-to-Device (D2D) gained attention for improving network efficiency and user experience. However, ensuring the security of Device-to-Device (D2D) communication in 5th Generation networks remains a critical challenge. This work presents a comprehensive study on enhancing Device-to-Device (D2D) security in 5th Generation networks by integrating Python, White Shark, Open5GS, and UERANSIM as tools for system implementation and evaluation. A comparative analysis with 4G networks is conducted to highlight the advancements and improvements achieved in 5G. The proposed D2D secure communication framework leverages authentication and key management schemes, secure communication protocols, and privacy preservation techniques specifically designed for 5G networks. This work uses the Hybrid method which is a combination of both AES and Huffman coding, performance evaluation is conducted using Python programming language, White Shark software, Open5GS, and UERANSIM for simulating and analysing the performance of the proposed research work.

Keywords: D2D, Open5GS, UERANSIM, 5G

1. Introduction

In recent years, the demand for seamless and efficient wireless communication has witnessed unprecedented growth. Traditional cellular networks, such as 3G and 4G, have been successful in providing reliable connectivity and enabling various services. However, these networks primarily rely on base stations for communication between devices, resulting in increased latency and network congestion.

Device-to-device (D2D) communication emerged as a solution to overcome these limitations[1][2]. D2D communication refers to the direct exchange of data between nearby devices without the need for routing through a base station. This proximity-based communication paradigm offers several advantages, including reduced latency, improved network efficiency, and enhanced spectrum utilization. Device-to-device (D2D) communication has the potential to bring significant transformation to various domains, including emergency response, multimedia content sharing, and collaborative applications. For instance, in public safety scenarios, D2D communication allows direct communication between emergency responders, leading to quicker response times and improved coordination[3]. In content-sharing applications, users can exchange files or stream multimedia content without consuming additional network resources. However, implementing D2D communication presents new challenges, particularly related to security, interference management, and resource allocation. It is crucial to ensure the security and privacy of D2D communication to prevent unauthorized access, eavesdropping, and data breaches. Managing interference becomes essential to avoid disruptions to existing cellular users, and optimizing resource allocation is necessary to strike a balance between D2D and cellular communication. This research primarily focuses on enhancing the security aspect of D2D communication within the context of 5G networks. The fifth generation (5G) of cellular networks offers significant advancements in data rates, capacity, and connectivity, which can be leveraged to further enhance D2D communication and enable secure and efficient direct communication between devices.

This research aims to develop robust security mechanisms and protocols tailored for D2D communication in 5G networks. By addressing security challenges and ensuring the privacy and integrity of D2D communication, the goal is to promote the widespread adoption and seamless integration of D2D technology in future wireless networks.

1.1.1 Overview of existing D2D communication techniques in 4G and 5G

In 4G networks, D2D communication mainly served proximity-based services, such as peer-to-peer file sharing and gaming. The two primary D2D communication techniques employed in 4G were as follows:

- LTE Direct: This technique enabled direct communication between LTE devices using a dedicated discovery protocol. Within a range of 500 meters, the devices could discover each other and communicate directly without relying on a centralized base station[4][5].

- Wi-Fi Direct: This technique allowed devices to connect to each other using Wi-Fi technology without requiring an access point. Wi-Fi Direct enabled direct peer-to-peer communication between devices.

In 5G networks, D2D communication has found applications in new service types like vehicle-to-vehicle communication, public safety communication, and industrial IoT applications. The two primary D2D communication techniques employed in 5G are:

- Cellular D2D: This technique utilizes the 5G cellular network to facilitate D2D communication. The devices communicate directly with each other through the cellular connection, while the network still plays a role in managing communication and ensuring quality of service[6].

- Device-to-Device Discovery and Communication (DDC): This technique enables devices to discover and communicate with each other using a dedicated D2D discovery protocol. DDC allows for direct peer-to-peer communication between devices without the need for a centralized network.

1.1.2 Background and Motivation

Wireless communication has become an essential aspect of our daily lives, connecting people and devices globally. The increasing demand for data-intensive applications and the widespread use of mobile devices necessitates efficient and reliable wireless networks. While traditional cellular networks like 4G have made considerable progress in providing reliable connectivity, they still face challenges related to network capacity, latency, and energy efficiency[7][8].

To address these challenges and improve wireless network performance, Device-to-Device (D2D) communication has emerged as a promising solution. D2D communication enables nearby devices to communicate directly with each other, bypassing the need for intermediate base stations. Leveraging device proximity offers advantages such as reduced latency, enhanced spectral efficiency, and improved network capacity[9][11].

However, D2D communication also introduces new security challenges. Direct communication between devices raises concerns about privacy, authentication, and data integrity. Integrating D2D communication into 5G networks further complicates matters due to the diverse nature of devices, various applications, and dynamic network conditions[10]. Ensuring the security of D2D communication in 5G networks becomes crucial to foster its adoption and realizing its full potential.

The motivation behind this research is to address the security challenges associated with D2D communication in 5G networks. By enhancing the security aspects of D2D communication, the goal is to enable secure and reliable direct communication between devices while safeguarding user privacy and protection against potential threats. The research aims to develop robust security mechanisms, authentication protocols, encryption techniques, and privacy preservation methods specifically tailored for D2D communication in 5G networks[12][13].

Furthermore, this work plans to leverage various technologies such as Python, White Shark, Open5GS, and UERANSIM for system implementation and performance evaluation. These tools provide valuable capabilities for simulating and analyzing the proposed D2D secure communication framework in 5G networks, enabling a comprehensive assessment of its effectiveness and performance.

The outcomes of this research are expected to benefit researchers, network operators, and policymakers involved in designing and deploying secure D2D communication systems in 5G networks. By addressing security concerns, the aim is to promote wider adoption of D2D communication, unlocking its potential to enhance network efficiency, enable new applications, and improve the overall user experience.

2. Overview of 4G and 5G networks

Fourth-generation (4G) networks represent the previous generation of cellular networks, designed to offer high-speed wireless communication and advanced features compared to their predecessors. Technologies like Long-Term Evolution (LTE) and WiMAX empowered 4G networks to provide substantial improvements in data rates, capacity, and latency over 3G networks. The key features of 4G networks encompass:

- High data rates: 4G networks catered to peak data rates for mobile users, enabling smooth streaming of high-quality videos and swift file downloads[14].
- Low latency: 4G networks significantly reduced latency, allowing real-time interactive applications and services, such as online gaming, video conferencing, and instant data transfer[15][16]
- Increased capacity: Through improved spectral efficiency and advanced network technologies, 4G networks increased overall network capacity, supporting more simultaneous connections and a higher number of devices within a coverage area.
- Advanced multimedia services: 4G networks facilitated the delivery of high-quality multimedia content, including HD video streaming, video conferencing, and multimedia messaging services[18].
- Enhanced mobility: 4G networks introduced seamless handover and mobility management capabilities.

On the other hand, 5G networks represent the latest generation of cellular networks developed to meet the growing demands of mobile connectivity and unlock new applications and use cases. 5G networks promise significant advancements in data rates, capacity, latency, and connectivity compared to 4G networks. Key features of 5G networks include:

- Massive data rates: 5G networks aim to deliver multi-gigabit per second (Gbps) data rates, enabling ultra-fast download and upload speeds for applications like 4K/8K video streaming, virtual reality (VR), and augmented reality (AR).
- Ultra-low latency: 5G networks target substantially reduced latency in milliseconds, enabling real-time applications like autonomous vehicles, remote surgeries, and industrial automation.
- Enhanced energy efficiency: 5G networks aim to be more energy-efficient compared to previous generations, optimizing power consumption through techniques like dynamic spectrum allocation and improved sleep modes for idle devices[17][19].
- Edge computing: 5G networks leverage edge computing capabilities, bringing computational resources closer to the network edge, reducing latency, and enabling real-time processing for latency-sensitive applications.

Overall, 5G networks provide a foundation for transformative technologies and services, encompassing autonomous vehicles, smart cities, and advanced industrial applications. The advanced capabilities of 5G networks pave the way for innovative use cases and significantly improve the overall wireless communication experience.

3. Importance of security in D2D communication

The security of device-to-device (D2D) communication holds immense significance for the following reasons:

i.User Privacy: D2D communication involves direct communication between nearby devices without intermediaries, raising concerns about user privacy. Without robust security measures, unauthorized parties could gain access to sensitive information exchanged between devices, leading to potential misuse of personal data.

ii. Data Integrity: Ensuring the integrity of data exchanged in D2D communication is crucial to prevent tampering, unauthorized alteration, or modification of information. Without proper security, malicious entities might intercept and alter data packets, leading to data corruption or unauthorized access to critical information.

iii. Authentication and Authorization: D2D communication requires mechanisms for device authentication and authorization to verify the identity and legitimacy of participating devices. Establishing trust between devices is essential to prevent unauthorized devices from accessing the network or impersonating legitimate devices, thereby avoiding various security breaches and unauthorized network access.

iv. Secure Content Sharing: D2D communication enables users to share content directly between their devices. To ensure the secure sharing of sensitive content, robust security measures are necessary to prevent unauthorized access, unauthorized distribution, or content leakage.

v. Network Resilience: D2D communication can significantly enhance network resilience by enabling direct communication between devices during network outages or in areas with limited coverage. However, ensuring the security of such direct communication is crucial to prevent unauthorized access and mitigate potential security threats that could exploit these alternative communication channels.

vi. Mitigation of Interference and Jamming Attacks: D2D communication operates in the same frequency bands as cellular communication, making it susceptible to interference and jamming attacks. Implementing security mechanisms in D2D communication can help mitigate such attacks, ensuring uninterrupted and secure communication between devices[20][21].

vii. Trustworthiness of Applications and Services: D2D communication facilitates the development of various applications and services that rely on direct device interactions. Ensuring the security of these applications and services is essential to establish trust among users and encourage their adoption. Secure D2D communication enhances the trustworthiness of the overall system, enabling the development of innovative and secure applications.

In summary, the importance of security in D2D communication lies in safeguarding user privacy, protecting data integrity, establishing trust among devices, and ensuring the secure exchange of information. By addressing security concerns, D2D communication can be leveraged to its full potential, enabling a wide range of applications and services while maintaining the confidentiality, integrity, and availability of user data.

4. Security challenges and threats in D2D communication:

Device-to-Device (D2D) communication offers the potential to enhance network efficiency and enable new services, but it also presents various security challenges and threats. Some of the common security challenges and threats in D2D communication include[22]:

Authentication and Authorization: D2D communication requires devices to authenticate and authorize each other before initiating communication. However, D2D communication is vulnerable to spoofing attacks, where an attacker masquerades as a legitimate device to gain unauthorized network access.

Confidentiality and Privacy: D2D communication may expose sensitive information to unauthorized parties, compromising the confidentiality and privacy of the communication. For instance, attackers can eavesdrop on D2D communication and intercept sensitive data like passwords or financial information.

Malware and Viruses: D2D communication is susceptible to malware and virus attacks, which can infect devices and compromise network security. The rapid spread of malware and viruses in D2D networks makes containment challenging.

Denial of Service (DoS) Attacks: D2D communication can be vulnerable to DoS attacks, where an attacker floods the network with excessive traffic or disrupts communication between devices. Such attacks degrade network performance and render it unusable.

Interference and Jamming: D2D communication rely on wireless technologies like Wi-Fi or Bluetooth, which can be prone to interference and jamming attacks. Attackers can disrupt communication by jamming wireless signals or introducing interference.

To overcome these security challenges and threats, several security mechanisms and protocols have been developed, including secure key exchange, encryption, and intrusion detection systems. Nonetheless, securing D2D communication remains an ongoing challenge, with researchers continuously working on innovative security solutions to ensure the safety and security of D2D communication.

5. Review of existing security solutions and protocols for D2D communication in 4G and 5G

Device-to-Device (D2D) communication poses various security challenges and threats, necessitating the development of security solutions and protocols to ensure secure communication. In this response, an overview of existing security solutions and protocols for D2D communication in both 4G and 5G networks will be provided.

LTE Direct Security: In 4G networks, LTE Direct employs secure key exchange and encryption protocols to establish a secure D2D communication channel. Devices authenticate each other using digital certificates, and AES-256 encryption ensures encrypted communication. Intrusion detection and prevention systems are used to detect and prevent malicious activities.

Wi-Fi Direct Security: Wi-Fi Direct in 4G networks utilizes standard Wi-Fi security protocols like Wi-Fi Protected Access II (WPA2) for secure D2D communication. WPA2 employs AES encryption and a pre-shared key for authentication[23].

Cellular D2D Security: In 5G networks, cellular D2D communication adopts the same security protocols as the cellular network, including authentication, encryption, and authorization. Digital certificates are used for device authentication, and AES encryption secures communication.

5G D2D Security: 5G D2D communication incorporates a dedicated security mechanism called the D2D Security Protocol (D2DSP), providing end-to-end security. D2DSP includes mutual authentication, secure key exchange, and encryption to ensure confidentiality and integrity.

Group Communication Security: Group communication in D2D networks is vulnerable to attacks like eavesdropping and message modification. Secure group communication protocols such as Group Key Management Protocol (GKMP) and Group Secure Association Key Management Protocol (GSA-KMP) have been developed to ensure secure group communication.

Securing D2D communication remains challenging, and existing security solutions and protocols continuously evolve to address these challenges. The choice of specific security mechanisms for D2D communication depends on application requirements and the underlying network architecture.

6. System Architecture and Model

System Architecture and Model refer to the design and structure of a system or model used in a specific context or domain. In the context of enhancing D2D security in 5G networks, the system architecture and model involve components, modules, and interactions to achieve secure D2D communication.
A general outline of the system architecture and model for enhancing D2D security in 5G networks includes:

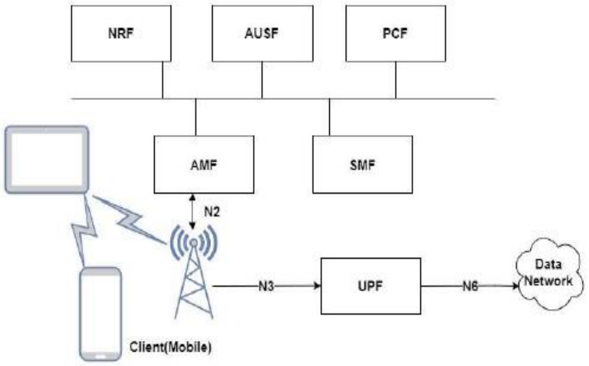


Figure 1. System Architecture and Model

User Equipment (UE): Represents the devices engaged in D2D communication, such as smartphones, tablets, or IoT devices. UEs act as both senders and receivers in the D2D communication process.

D2D Communication Interface: Provides a direct communication channel between UEs, enabling secure data exchange and facilitating proximity-based communication.

Authentication and Key Management Module: Handles UE authentication and manages the distribution and updating of cryptographic keys used for secure communication. It ensures that only authorized devices can participate in D2D communication.

Security Protocol Module: Implements security protocols and algorithms for securing D2D communication. This module includes encryption and decryption mechanisms, integrity checks, and secure channel establishment protocols to protect data confidentiality and integrity during transmission.

Privacy Preservation Module: Incorporates techniques for preserving user privacy during D2D communication. This module may use privacy-enhancing technologies like pseudonymization, anonymization, or differential privacy mechanisms to protect user identities and sensitive information.

Interference Management Module: Addresses interference issues that may arise due to D2D communication. It includes interference mitigation techniques, resource allocation strategies, and power control mechanisms to ensure D2D communication does not degrade the cellular network's performance.

Monitoring and Intrusion Detection Module: Monitors D2D communication for suspicious or malicious activities. It includes intrusion detection systems, anomaly detection algorithms, and traffic analysis techniques to identify and mitigate potential security threats.

Network Management and Control: Provides overall management and control of the D2D communication system. It includes functionalities like network configuration, policy enforcement, and access control mechanisms to ensure secure system operation.

It is essential to recognize that the specific architecture and model may vary depending on the research context, security requirements, and technologies employed. The outlined architecture serves as a fundamental framework, and additional components or modules can be integrated based on specific research or system design needs.

7. Authentication and key management schemes for D2D communication in 5G

AES (Advanced Encryption Standard) and Huffman coding are two commonly used techniques for securing and compressing data, respectively. AES is a symmetric encryption algorithm that is widely used for securing data in transit or at rest, while Huffman coding is a lossless data compression technique used to reduce the size of data.

When used together, AES and Huffman coding can enhance the security and efficiency of data transmission. The data is first compressed using Huffman coding to reduce its size and then encrypted using AES before transmission. At the receiving end, the encrypted data is first decrypted using AES and then decompressed using Huffman coding to obtain the original data.

The combination of AES and Huffman coding provides several benefits, including:

Enhanced Security: AES provides strong encryption of data, ensuring that the data is protected from unauthorized access. Huffman coding, on the other hand, reduces the size of the data, making it difficult for attackers to intercept and decipher the data.

Improved Efficiency: Huffman coding reduces the size of the data, which reduces the time and bandwidth required for data transmission. This makes data transmission faster and more efficient.Reduced Storage Requirements: Compressed data requires less storage space, which can be beneficial in situations where storage space is limited.

However, it is important to note that the effectiveness of these techniques depends on the specific use case and the implementation details. Careful consideration should be given to the trade-offs between security, efficiency, and storage requirements when using these techniques.

AES (Advanced Encryption Standard) is a widely used encryption algorithm for securing data in transit or at rest. Huffman coding, on the other hand, is a lossless data compression technique that is used to reduce the size of the data. Both AES and Huffman coding can be used together to enhance the security and efficiency of data transmission.

When using AES and Huffman coding together, the data is first compressed using Huffman coding to reduce its size. The compressed data is then encrypted using AES before transmission. At the receiving end, the data is first decrypted using AES and then decompressed using Huffman coding to obtain the original data[4][5].

The combination of AES and Huffman coding provides several benefits, including:

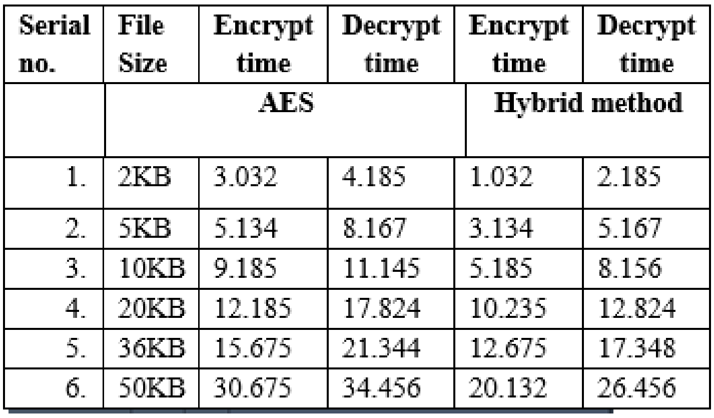
- Improved Security: AES provides strong encryption of data, ensuring that the data is protected from unauthorized access. Huffman coding, on the other hand, reduces the size of the data, making it difficult for attackers to intercept and decipher the data.
- Increased Efficiency: Huffman coding reduces the size of the data, which reduces the time and bandwidth required for data transmission. This makes data transmission faster and more efficient.
- Reduced Storage Requirements: Compressed data requires less storage space, which can be beneficial in situations where storage space is limited.

Overall, the use of AES and Huffman coding together can enhance the security and efficiency of data transmission. However, it is important to note that the effectiveness of these techniques depends on the specific use case and the implementation details. Careful consideration should be given to the trade-offs between security, efficiency, and storage requirements when using these techniques.

8.Comparative analysis in 5G networks while transferring data in the Hybrid method

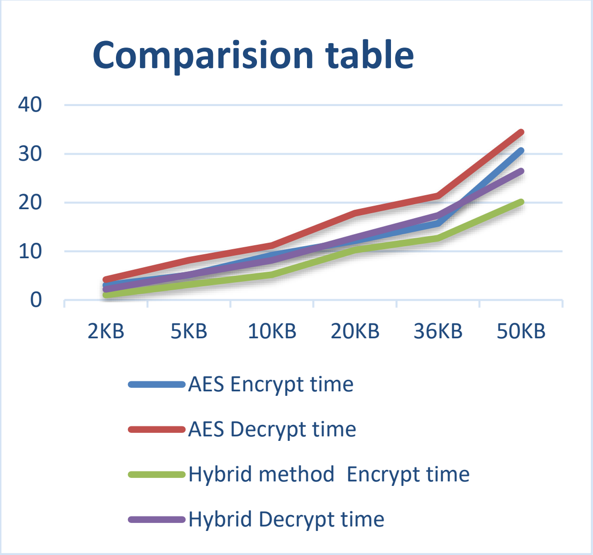
The hybrid method combines AES encryption with Huffman coding, adding an additional layer of security by compressing the encrypted data. However, the security level primarily depends on the strength of AES encryption. The hybrid method achieves data compression by applying Huffman coding to the encrypted data. This results in a compressed data stream that is smaller in size compared to the original data. While the hybrid method introduces additional steps for Huffman coding, the overall efficiency can be improved due to the reduced data size for transmission and storage. The hybrid method is advantageous when both data security and efficient data transmission are critical. It can be applied in secure communications over constrained networks or storage of encrypted data with reduced space requirements. The hybrid method combines both encryption and data compression but introduces additional complexity in the encryption and decryption processes.

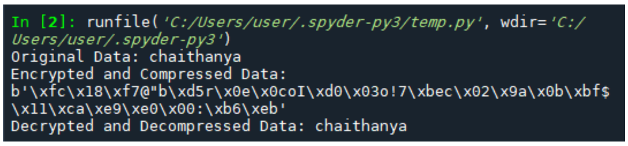
Table 1. Results of Hybrid method for encryption and decryption



Serial no.	File Size	Encrypt time	Decrypt time	Encrypt time	Decrypt time
	AES			Hybrid method	
1.	2KB	3.032	4.185	1.032	2.185
2.	5KB	5.134	8.167	3.134	5.167
3.	10KB	9.185	11.145	5.185	8.156
4.	20KB	12.185	17.824	10.235	12.824
5.	36KB	15.675	21.344	12.675	17.348
6.	50KB	30.675	34.456	20.132	26.456

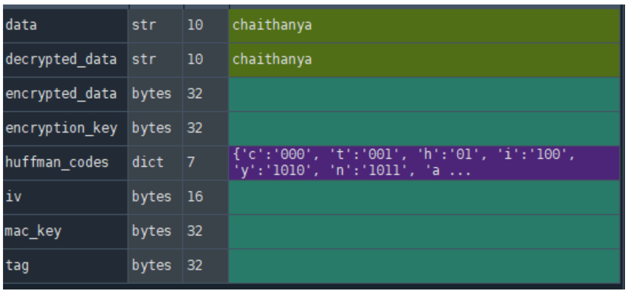
Table 1. Comparison table of AES and Hybrid Method





```
In [2]: runfile('C:/Users/user/.spyder-py3/temp.py', wdir='C:/
Users/user/.spyder-py3')
Original Data: chaithanya
Encrypted and Compressed Data:
b'\xfc\x18\xf7@"b\xd5r\x0e\x0coI\xd0\x03o!7\xbec\x02\x9a\x0b\xbf$
\x11\xca\xe9\xe0\x00:\xb6\xeb'
Decrypted and Decompressed Data: chaithanya
```

Figure 2. Screenshot of Decrypted and Decompressed Data



data	str	10	chaithanya
decrypted_data	str	10	chaithanya
encrypted_data	bytes	32	
encryption_key	bytes	32	
huffman_codes	dict	7	{'c':'000', 't':'001', 'h':'01', 'i':'100', 'y':'1010', 'n':'1011', 'a ...
iv	bytes	16	
mac_key	bytes	32	
tag	bytes	32	

Figure 3. Screenshot of Decrypted data along with Huffman Codes

8. Contributions of the proposed D2D secure communication system for 5G

The proposed D2D secure communication system for 5G networks offers several contributions to enhance the security of D2D communication. Here are the key contributions:

Enhanced Security Measures: The system incorporates advanced security measures, including authentication, encryption, privacy preservation, and intrusion detection. By integrating these measures into the 5G network architecture, the system enhances the overall security of D2D communication, protecting against unauthorized access, data breaches, and other security threats.

Integration of Technologies: The system integrates various technologies, such as Python, White Shark, Open5GS, and UERANSIM. This integration enables the system to leverage the capabilities of these technologies for enhanced security. For example, Python provides a flexible programming language for implementing security algorithms, while White Shark offers simulation capabilities for analyzing and testing the system's security measures.

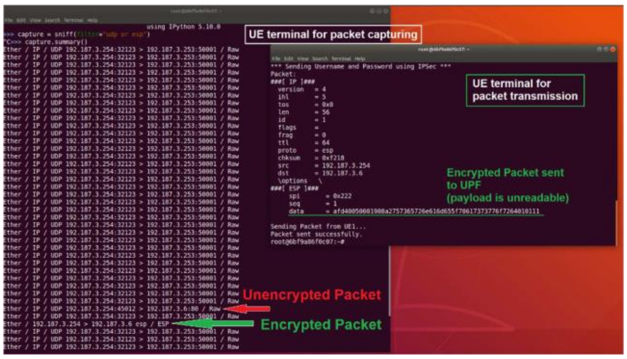
Compatibility with 5G Networks: The proposed system is designed to be compatible with existing 5G networks. By aligning with 5G standards and protocols, the system can seamlessly integrate into the 5G network architecture, ensuring interoperability with different network components and devices. This compatibility enables the system to be readily deployed and integrated into existing 5G infrastructure.

Scalability and Performance: The system is designed to handle the scalability requirements of 5G networks. With the integration of technologies like Open5GS and UERANSIM, the system can efficiently allocate resources, optimize performance, and manage the increasing network traffic associated with 5G deployments. This scalability ensures that the security measures can be effectively applied in large-scale and high-density network environments.

Flexibility and Customization: The modular design of the proposed system allows for flexibility and customization. It can be tailored to the specific security requirements of different applications and use cases in the 5G ecosystem. This flexibility enables the system to adapt to evolving security challenges and accommodate diverse security needs, promoting the adoption of the system in various industry sectors.

Future Potential: The proposed system lays the foundation for further research and development in the field of D2D security in 5G networks. By integrating technologies and addressing the security challenges specific to D2D communication, the system contributes to advancing the state-of-the-art in secure communication frameworks for 5G networks. It opens possibilities for future enhancements, optimizations, and the exploration of emerging security technologies in the context of 5G D2D communication.

Overall, the proposed D2D secure communication system makes significant contributions by enhancing the security of D2D communication in 5G networks. Through its advanced security measures, integration of technologies, compatibility with 5G networks, scalability, and customization capabilities, the system provides a robust and adaptable solution for ensuring secure communication between devices in the dynamic 5G ecosystem. Figure 4 shows the encrypted version of the packet on the right terminal. We can see that IPsec encrypted the payload of the UDP packet and the new payload (data) is encrypted and unreadable.



```
                              using IPython 5.10.0
>>> capture = sniff(filter="udp or esp")
^C>>> capture.summary()
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:45012 > 192.187.3.6:80 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / 192.187.3.254 > 192.187.3.6 esp / ESP
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
Ether / IP / UDP 192.187.3.254:32123 > 192.187.3.253:50001 / Raw
```

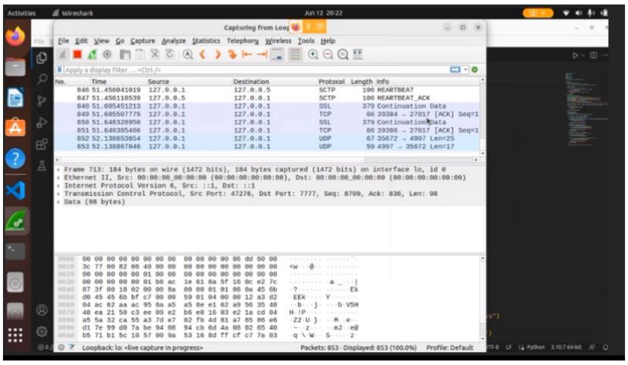
```
*** Sending Username and Password using IPSec ***
Packet:
###[ IP ]###
  version   = 4
  ihl       = 5
  tos       = 0x0
  len       = 56
  id        = 1
  flags     =
  frag      = 0
  ttl       = 64
  proto     = esp
  chksum    = 0xf218
  src       = 192.187.3.254
  dst       = 192.187.3.6
  \options   \
###[ ESP ]###
     spi       = 0x222
     seq       = 1
     data      = afd40050001900a2757365726e616d655f70617373776f7264010111

Sending Packet from UE1...
Packet sent successfully.
root@6bf9a86f0c07:~#
```

UE terminal for packet capturing
UE terminal for packet transmission
Encrypted Packet sent to UPF (payload is unreadable)
Unencrypted Packet
Encrypted Packet

Figure 4 Transmission of a packet from the UE - Encrypted packet

Wireshark is a network protocol analyzer that captures packets from a network connection, such as your computer to the internet. It is widely used and considered the most popular packet sniffer available. Being free and open-source, Wireshark is utilized for network troubleshooting, analysis, software, and communications protocol development, and education as shown in Figure 7.


Wireshark
Jun 12 20:22
Capturing from Loop
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source     Destination  Protocol Length Info
 846 51.456041019  127.0.0.1  127.0.0.5    SCTP      106 HEARTBEAT
 847 51.456110539  127.0.0.5  127.0.0.1    SCTP      106 HEARTBEAT_ACK
 848 51.605451213  127.0.0.1  127.0.0.1    SSL       379 Continuation Data
 849 51.605507775  127.0.0.1  127.0.0.1    TCP        66 39384 → 27017 [ACK] Seq=1
 850 51.648328950  127.0.0.1  127.0.0.1    SSL       379 Continuation Data
 851 51.648385466  127.0.0.1  127.0.0.1    TCP        66 39386 → 27017 [ACK] Seq=1
 852 52.138653654  127.0.0.1  127.0.0.1    UDP        67 35672 → 4997 Len=25
 853 52.138867046  127.0.0.1  127.0.0.1    UDP        59 4997 → 35672 Len=17

› Frame 713: 184 bytes on wire (1472 bits), 184 bytes captured (1472 bits) on interface lo, id 0
› Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
› Internet Protocol Version 6, Src: ::1, Dst: ::1
› Transmission Control Protocol, Src Port: 47276, Dst Port: 7777, Seq: 8709, Ack: 836, Len: 98
› Data (98 bytes)

0000  00 00 00 00 00 00 00 00  00 00 00 00 86 dd 60 00   ········ ········
0010  3c 77 00 82 06 40 00 00  00 00 00 00 00 00 00 00   <w···@·· ········
0020  00 00 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 01 b8 ac  1e 61 8a 5f 16 0c e2 7c   ········ ·a·_···|
0040  87 3f 80 18 02 00 00 8a  00 00 01 01 08 0a 45 6b   ·?······ ······Ek
0050  d0 45 45 6b bf c7 00 00  59 01 04 00 00 12 a3 d2   ·EEk···· Y·······
0060  04 ac 62 aa ac 95 6a a5  a5 8e e1 62 a9 56 35 48   ··b···j· ···b·V5H
0070  48 ea 21 50 c3 ee 09 e2  b6 e0 16 03 e2 1a cd 04   H·!P···· ········
0080  a5 5a 32 ca 55 a3 7d e7  02 fb 4d 81 a7 65 86 e6   ·Z2·U·}· ··M··e··
0090  d1 7e 99 d0 7a be 94 08  94 cb 6d 4a 08 02 65 40   ·~··z··· ··mJ··e@
00a0  b5 71 b1 5c 10 57 00 9a  53 16 8d ff cf c7 7a 03   ·q·\·W·· S·····z·

Loopback: lo: <live capture in progress>     Packets: 853 · Displayed: 853 (100.0%)     Profile: Default
```

Figure 7 Wireshark network protocol analyzer

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. ρ ISSN: 2088-8708 IJECE Vol. 6, No. 6, December 2016 : 2962 – 2970 2970

[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.

[22] Chaithanya D J and Dr.Anitha S "D2D Protection in 5G Communication with Free5GC by Utilizing Docker for Enhanced Security" **European Chemical Bulletin,** ISSN 2063-5346,2023.

[23] Anitha, S., Chaithanya, D.J. (2021). Low Complexity and Efficient Implementation of WiMAX Interleaver in Transmitter. In: Pandian, A.P., Palanisamy, R., Ntalianis, K. (eds) Proceedings of International Conference on Intelligent Computing, Information and Control Systems. Advances in Intelligent Systems and Computing, vol 1272. Springer, Singapore.