INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Enhancing Secured Network Slicer for Cloud Security Systems

Vanlalruata Hnamte[1]*, Jamal Hussain[1], Samuel Lalmuanawma[2], Chhakchhuak Lalrinawma[3], Lalchhanhima Hmar[4]

1 Department of Mathematics and Computer Science, Mizoram University, India
2 Department of Computer Science, Government Champhai College, India
3 Department of Computer Science, Government Zirtiri Residential Science College, India
4 Department of Computer Science, Government Serchhip College, India

OPEN ACCESS

Received: 23-01-2023

Accepted: 09-06-2023

Published: 13-09-2023

Citation: Hnamte V, Hussain J, Lalmuanawma S, Lalrinawma C, Hmar L (2023) Enhancing Secured Network Slicer for Cloud Security Systems. Indian Journal of Science and Technology 16(SP1): 179-191. https://doi.org/10.17485/IJST/v16sp1.msc25

* **Corresponding author**.

vanlalruata.hnamte@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: The mobile's Ad-hoc 5G networks are now used in almost every sector. The increasing usage of mobile Ad-hoc 5G networks may be used not only on personal computers but also on mobile phones, tablets, and laptops due to their low cost and simplicity. Developing a slicing approach to security for mobile Ad-hoc 5G/6G networks and their wired equivalents are proposed. If the attacker must first get physical access to the cable system or terminal devices on the mobile Ad-hoc 5G networks, then a standard receiver put within the network range on the mobile Ad-hoc 5G networks will be granted authorization. **Methods**: The 5G network slicing design allows the multiplexing of virtualized and separate logical networks on the same physical network infrastructure. Each network slice is a self-contained, end-to-end network designed to meet the unique needs of a certain application. Mobile Ad-hoc 5G data encryption is handled using the Temporal Key Integrity Protocol (TKIP), which employs the same encryption method as RC4 as WEP but, unlike WEP, utilizes static keys (i.e., keys change frequently). **Findings**: 5G network slicing enables mobile network operators to build a virtual border for a single customer or range of devices. Only approved devices are permitted to connect to the segmented network, reducing this attack vector significantly. Slicing may be used as part of a private network to provide an extra layer of security, or on a public network to add a security layer without incurring the costs associated with maintaining the network infrastructure. There is a notion of shared security responsibility when network slicing is employed on public mobile networks. Comparable to cloud computing, where network operators are responsible for safeguarding the infrastructure and the business handles the software security layer. Future 6G network security planning must take into account the new possibilities, risks, and trust paradigms presented by the development of cellular communication offered by 5G. Despite changes in communication implementation, the slicing approach to security for mobile Ad-hoc 5G/6G networks and their wired equivalents is comparable to the proposed model. This model focuses more on the needs for authentication of mobile Ad-hoc 5G clients and access points, as well as maintaining the confidentiality and integrity of the data shared, in order to secure information on mobile Ad-hoc 5G/6G networks. **Novelty**: The signals of Mobile Ad-hoc 5G devices have a highly complicated structure and a broad spectrum, so standard radio surveillance equipment cannot detect these signals and the nearby Mobile Ad-hoc 5G devices. The experiment has demonstrated that reliable detection of a Mobile Ad-hoc 5G signal by contemporary radio surveillance systems within a broad frequency band is only possible based on an energy characteristic in the presence of parallel analytics bands of several tens of megahertz width at a minimum of 400 velocities and its ranges MHz/s and in the adjacent field zone.

Keywords: Cloud Security; Mobile Adhoc; 5G networks; Personal Computers; Security; Terminal device; Slicing approach

1 Introduction

In today's digital age, cloud computing has become a crucial element of business operations, offering unparalleled flexibility, scalability, and cost-efficiency. The increasing use of mobile Ad-hoc 5G networks in almost every sector has opened new avenues for connectivity, communication, and data sharing. However, with the growing complexity of mobile Ad-hoc 5G networks, ensuring security has become a major challenge. In this study, we propose developing a slicing approach to security for mobile Ad-hoc 5G/6G networks and their wired equivalents. To address this, cloud security systems have evolved rapidly, incorporating new technologies and techniques to enhance network security.

One of the most effective tools for securing cloud infrastructure is a Network Slicer. A Network Slicer is a security technique that partitions a network into smaller, more manageable sections, allowing security administrators to isolate threats and limit the potential impact of a security breach. However, while Network Slicers have been widely adopted, they are not without their limitations.

To overcome these limitations, researchers have been working to enhance Network Slicer technology, creating more effective and efficient security solutions. This article will explore some of the latest advancements in Network Slicer technology, highlighting how these enhancements are improving cloud security systems.

First, we will examine the limitations of traditional Network Slicer technology, discussing how these limitations impact cloud security. We will then discuss the latest enhancements to Network Slicer technology, including advancements in artificial intelligence and machine learning, which are revolutionizing how network security is managed. Finally, we will explore the potential future of Network Slicer technology, discussing how these advancements may shape the future of cloud security systems.

While enhancing secured Network Slicer technology for cloud security systems has shown great potential in improving network security, there are still some limitations that need to be addressed.

One of the major limitations of Network Slicer technology is the lack of scalability. As the number of devices and applications in a cloud network increases, the network slicing process becomes more complex, making it difficult for security administrators to manage and monitor security threats effectively.

Another limitation is the lack of interoperability between different cloud environments. Each cloud provider has its own unique security architecture and approach, making it challenging for security administrators to integrate Network Slicer technology across multiple cloud environments. As a result, this limits the flexibility and effectiveness of Network Slicer technology in securing cloud infrastructure.

Overall, the aim of this article is to provide an overview of the current state of Network Slicer technology, highlighting its importance in securing cloud infrastructure and how it can be improved to meet the ever-growing demands of cloud security.

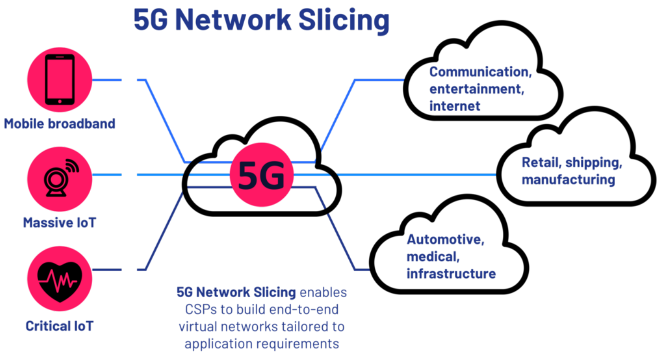
5G Network Slicing
Mobile broadband
Massive IoT
Critical IoT
5G
Communication, entertainment, internet
Retail, shipping, manufacturing
Automotive, medical, infrastructure
5G Network Slicing enables CSPs to build end-to-end virtual networks tailored to application requirements

Fig 1. 5G Network and issues

As a consequence, the number of Wi-Fi networks with their own access points and clients, which may number in the hundreds, can be found in almost every large city today, next to practically any object. Subedi *et al.*[1] implemented the virtualization of the physical 5G infrastructure by leveraging advancements in technology, specifically software-defined networking and network function virtualization. Further, Lv *et al.*[2] discuss potential information security vulnerabilities associated with the usage of Wi-Fi networks. Wireless technologies operate without the physical and logical boundaries of their wired equivalents, putting the network infrastructure and users at risk[3]. 5G networks confront a multitude of dangers. Some are inherited from previous generations and norms of the past. Other threats are unique to the software-defined networking technology that 5G introduces.

2 Related Studies

The integration of cloud computing and 5G technology has resulted in the development of a new paradigm known as 5G-enabled cloud computing. However, the security of this paradigm is a major concern due to its susceptibility to various cyber threats. To address this issue, researchers have proposed several solutions, one of which is the 5G secured network slicer.

5G links essential infrastructures such as e-health, transportation, and electrical grid systems to user settings like smart homes and portable devices through the network. If sufficient attention is not given to the underlying security problems, the integration of ML with 5G might result in possible security dangers and difficulties.

The 5G secured network slicer is a novel approach that provides secure communication between different slices in a cloud-based 5G network. This approach offers a scalable and secure solution that enables the isolation of different network slices to ensure that they do not interact with each other. As a result, it becomes possible to protect sensitive data and applications from unauthorized access, thus enhancing the overall security of the cloud-based 5G network.

The study[4] indirect attacks pose a hazard not just to information processed on computer networks, but also to spoken information. Consider immediate dangers. Mobile Ad-hoc 5G technology employs a data transfer radio interface to optimise a wireless communication channel. As a communication medium, it is susceptible to illegal intervention intended to intercept, distort, or block data. The work[5] states that during the development of Mobile Ad-hoc 5G technology, certain information security concerns were considered; however, as shown by actual use, these considerations were insufficient. Numerous ”holes” in Mobile Ad-hoc 5G security have spawned a new trend in computer hacking known as ward driving. The paper[6] has referred individuals that hack into other people's Mobile Ad-hoc 5G networks for ”game” purposes do not lessen the likelihood of threat.

Shah *et al.*[7] focused on the advancements made in the field of E2E network slicing, which involves the use of various technologies and solutions to achieve this goal. The paper also delves into the standardization efforts made in this area. Additionally, it identifies the current research challenges and offers recommendations and possible solutions to address these issues.

Several studies have investigated the effectiveness of the 5G secured network slicer in enhancing cloud security systems. For example, Zhang *et al.*[8] proposed a slicing-based approach that provides secure communication between different slices in a cloud-based 5G network. The approach uses a secure channel to establish communication between different slices, and it isolates the network slices to prevent unauthorized access.

In another study, Kourtis *et al.*[9] proposed a secure network slicing framework for 5G-enabled cloud computing. The framework enables the isolation of different network slices, thus preventing unauthorized access. The authors conducted experiments to evaluate the effectiveness of the framework, and the results showed that it provided better security than traditional cloud-based 5G networks.

Serckumecka *et al.*[10] proposed a method for safe long-term archival of cloud events, which employs multi-cloud storage to ensure data security, scalability, and cost-effectiveness. The system groups events in blocks and uses indexing techniques to facilitate their recovery. The researchers evaluated the system using a real dataset and found that it is more cost-efficient compared to other alternatives available in the market. But the proposed method is not compared with modern slicing algorithm.

Zhang *et al.*[11] provided a summary of network slicing and devoted one part on network slicing security. In addition, the report indicated future research objectives, such as RAN virtualization and slicing, holistic slice orchestration, and secure sliced networks. Guolin Sun *et al.*[12] have presented a hierarchical structure and DQN-based duelling autonomous slicing refinement for heterogeneous traffics in virtualized RAN. Using a duelling DQN method, autonomous slicing refinement modifies the resources allocated to individual slices to achieve a balance between QoS satisfaction and resource utilisation. Dueling DQN employs a two-stream Q-function that can learn which states are crucial to the agent without knowing the consequence of each action on each state.

5G utilises mobile clouds, SDN, and NFV to address significant connectivity, flexibility, and cost issues[13]. The incorporation of IoT seems to increase security problems, particularly regarding privacy. Therefore, it is necessary to seek for unique security solutions that use advances in technologies such as artificial intelligence and context awareness to allow proactive network forensics and reaction using the programmability offered by SDN and runtime. Hussain *et al.*[14] recommended secure 5G-based VANET apps/services and indicated that an increase in investors' interest in the commercialization of VANET and consumers' use of VANET services in their everyday lives would significantly enhance the service of 5G-based VANET applications. The majority of VANET services need precise location data and user identification. Consumers are most concerned about user and location privacy, however. Security solutions for VANET applications implemented over 5G networking must be both fast and adaptable. From an efficiency standpoint, cryptographic methods are often both storage- and processing-intensive, which will negatively impact VANET applications[14].

Butt *et al.*[15] conducted a review of various machine learning (ML) algorithms that have been employed to address cloud security challenges, including supervised, unsupervised, semi-supervised, and reinforcement learning. The researchers compared the performance of each technique based on their characteristics, benefits, and drawbacks. Additionally, they identified potential research areas to enhance the security of cloud computing models in the future. The limitation of their study is that there are no new propose method.

Barakabitze *et al.*[16] conducted a thorough review and analysis of 5G network slicing using SDN and NFV, presenting updated solutions to the topic. The paper begins by introducing the service quality and business requirements of 5G networks, followed by a description of the softwarization and slicing paradigms with relevant concepts, history, and use cases. The authors then provide a tutorial of the technological enablers of 5G network slicing, including SDN, NFV, MEC, cloud/Fog computing, network hypervisors, virtual machines, and containers. The paper also surveys various industrial initiatives and projects that are working towards the adoption of SDN and NFV in 5G network slicing, comparing different architectural approaches in terms of practical implementations, technology adoptions, and deployment strategies. The authors discuss the standardization efforts in 5G networks related to network slicing and softwarization, as well as the management and orchestration of network slices in a single domain and across multiple domains while supporting multiple tenants.

Xiangle Cheng *et al.*[17] claimed that network slicing, as a major 5G enabling technology, has the potential to enable the provided services and infrastructure management with more flexibility, agility, and intelligence. However, as modern networks become more dynamic, diverse, and large-dimensional, real-time monitoring and explicit modelling of the networking environment become more expensive or perhaps impossible. It is crucial for a slicing system to monitor environmental changes, identify uncertainties, and schedule reaction measures appropriately.

Wichary *et al.*[18] conducted an analysis of the current standards and trends aimed at addressing the vulnerabilities mentioned above. The study also proposed various security controls and classified them based on their efficiency and applicability, particularly their ease of development. While security controls are commonly used to secure networks, they only enforce security policies in their respective areas. The study lacks comparison of the proposed method with other algorithms.

Khan *et al.*[19] proposed a scheme that involves adjusting the optimal bandwidth slicing and dynamically adapting to instantaneous network load conditions to ensure a targeted performance. The problem is solved by utilizing a Genetic Algorithm

(GA), and the results are compared with the previously proposed 5G VANET architecture. The simulations conducted reveal that the proposed slicing framework optimizes resources and delivers on the key performance metrics for mission-critical communication. First, the use of encryption lowers the pace of information transmission across the channel by a factor of many, and network managers often stop encryption to enhance traffic. Second, the widespread usage of WEP encryption technology in Mobile Ad-hoc 5G networks has been ridiculed for a long time owing to flaws in the RC4 key distribution technique, which is combined with WEP. Hamdi *et al.*[20] said that there are several tools that enable guessing of ”weak” WEP keys. The term FMS was derived from the first letters of the creators' surnames. Each pocket with a weak key returns one byte of the secret key with a 5 percent chance, therefore the total number of packets an attacker needs gather to start an attack is largely dependent on his level of luck.

The work[21] states that one needs around six million encrypted packets to break on average. Taspoten Labs' hackers also known as H1kari has upgraded the FMS mechanism, decreasing the number of necessary packets from six million to 500,000 in their experiment. Mazurczyk *et al.*[22] mentioned that 5G systems are now the focus of academics, business, and governments throughout the globe, since they generate many new needs for various network capabilities.

One potential research gap in the area of 5G Secured Network Slicer for Cloud Security Systems could be the development of a comprehensive evaluation framework to assess the effectiveness and performance of various slicing approaches in terms of security and resource allocation. While several studies have proposed different slicing approaches, there is a need for a standardized methodology to compare and evaluate these approaches based on their security and resource allocation capabilities.

Additionally, there is a need for more studies that investigate the economic and regulatory implications of implementing 5G secured network slicing for cloud security systems. This includes assessing the cost-effectiveness of different slicing approaches, and identifying the potential legal and regulatory barriers that may arise when deploying these systems.

3 Methodology

Figure 2 illustrates the self-sustainable slicing model (SSSM) that was suggested. In contrast, the issue of information blockage on the Mobile Ad-hoc 5G channel is almost neglected in the development of technology. Obviously, blocking a channel is not dangerous because Mobile Ad-hoc 5G networks are always auxiliary, but blocking is often employed as a precaution against a one-man attack, which occurs when a third device appears between the customer and the access point and redirects traffic between you and the customer. In this instance, not only is the interception of the information a danger but so is its change.

There are at least a few known DOS (service denial) attacks on Mobile Ad-hoc 5G networks, but we will not focus on them here; instead, we will discuss the existence of serious complications. We will evaluate indirect vulnerabilities to the information security of a facility that is directly associated with Mobile Ad-hoc 5G technology. Wi-Fi channels are very desirable as a transport infrastructure for damaging devices for a variety of reasons.

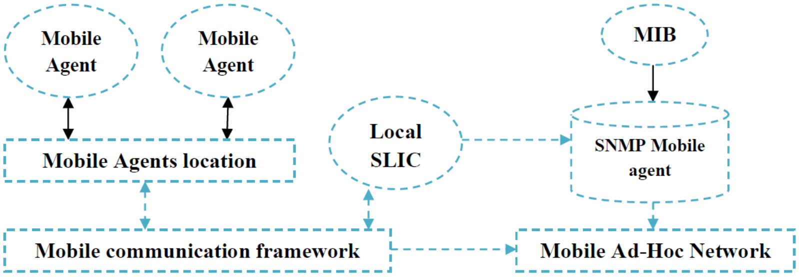

Fig 2. Diagram block for proposed model

3.1 Slicing Approach

The 5G network slicing design allows the multiplexing of virtualized and separate logical networks on the same physical network infrastructure. Each network slice is a self-contained, end-to-end network designed to meet the unique needs of a certain application. Mobile Ad-hoc 5G data encryption is handled using the Temporal Key Integrity Protocol (TKIP), which employs the same encryption method as RC4 as WEP but, unlike WEP, utilizes static keys (i.e., keys change frequently). It employs a lengthy boot vector and cryptographic security to validate the packets' integrity (the latter being the source and target address and the function of the data field). Figure 3 depicts the slicing procedure methodology.

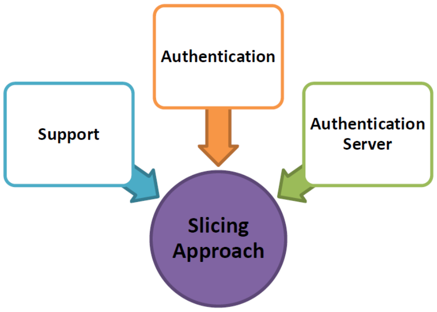

Fig 3. Approach for slicing protocol

Steps involve in slicing technique:

- SLICE-SIM is utilized in SLICE-AKA-GSM mobile networks at the first step.
- A pre-retina system from slicing systems is the second step.
- SLICE -MD5 - Simple approach like SLICING (not continuous).
- Network authentication with a username and password.
- TLS - Digital Certification Authorization is the fifth step.
- SLICE-SecureID is a mechanism for one-time passwords (OTP).

The SLICING protocol is meant to function with an authentication server,which is often a SLICING server. The wireless access points in this instancerun in enterprise mode. The accrediting programme has three parts:

- Support - Software operating on the client PC that tries a network connection.
- Authentication - authentication at the access point (wireless access point or wired switch that supports 802.1x).
- Authentication Server (usually a RADIUS server).

Mobile Ad-hoc 5G technology is certainly handy and adaptable for streamlining wireless information access. However, this presents a variety of grave challenges to the information security of the institution. At the same time, information security faces both direct and indirect risks. If direct hazards may be addressed by abandoning Mobile Ad-hoc 5G devices in the corporate network architecture and by not utilizing Mobile Ad-hoc 5G networks readily, then indirect threats exist regardless of the facility's usage of Mobile Ad-hoc 5G technology. Moreover, indirect threats are more serious than direct ones since they reveal not only the information on the computer networks but also the verbal information in the facility. The network devices may facilitate malicious wireless data transfers. Self-Sustaining Slicing Model is shown in Table 1.

Table 1. Algorithm: Self Sustainable Slicing Model (SSSM)

Steps	Description
Step 1	Start
Step 2	Send an authorization request
Step 3	Getting an access point (AP) responds to the customer
Step 4	Sends a SLICE-response
Step 5	The authentication server sends a challenge packet
Step 6	Mutually identifying the server
Step 7	Receives the required information
Step 8	Provide access after opening port
Step 9	Starts communication
Step 10	End

The SSSM authentication procedure comprises the following steps:

- The client is able to transmit an authorization request (SLICE-start message) to the access point.
- The access point (authorization) sends a SLICE request / identification message in response to the customer's request. If any of the authorizer's ports are active, the authorizer may submit the SLICE request on its own.

- The customer responds with a SLICE-response packet with the needed data, which redirects the access point (authentication) to the radius server (authentication server).
- The authentication server sends a challenge packet (request for customer credibility information) to the authorization server (access point). It is sent by the authorizer to the client.
- Following this, the process of mutually identifying the server and client occurs. The number of rounds varies based on the SLICE system, however, for wireless networks, only mutual client-server authentication (SLICE-TLS, SLICE-TTLS, SLICE-PSLICE) and communication pre-encryption are suitable for the “strong” authentication channel.
- The authentication server subsequently gets the relevant information from the client and either accepts (accepts) or rejects (rejects) the message to the authorizer. If the server responds positively (accept), the authorizer (access point) will open the port for the applicant.
- The port is opened, authentication delivers a successful completion message to the client, and the consumer receives network access.
- After the client is disconnected, the port at the access point returns to the “closed” status.

Bluetooth devices are much inferior to Mobile Ad-hoc 5G in terms of communication range and channel bandwidth, but they have one big advantage: low power consumption, which is crucial for an unauthorized transmitter. Another technology that is beginning to compete with Mobile Ad-hoc 5G in offering wireless internet is mobile Ad-hoc. However, Ad-hoc devices are now considerably less prevalent, and their existence is more of an unseen aspect than a means of concealing an illicit communication route. Mobile Ad-hoc 5G is now not only the most prevalent wireless access technology but also the most convenient in terms of unlawful data reception and transmission.

SNS is a novel approach that enhances the security of cloud computing systems in 5G Mobile Ad-hoc Networks (MANETs) by dynamically creating and managing secure virtual slices for different user groups. The main novelty of SNS is its ability to provide tailored security for different user groups, each with their own unique security requirements. This is achieved by dividing the cloud infrastructure into multiple virtual slices, each with its own set of security policies and protocols.

In addition, SNS uses a distributed security model that allows for the efficient and effective management of security policies and protocols across multiple virtual slices. This enables SNS to provide a high level of security while minimizing the impact on system performance. Furthermore, SNS is designed to be highly scalable and can be easily integrated into existing cloud computing systems.

Overall, the combination of SNS and 5G MANETs provides a highly secure and robust cloud computing environment that can meet the evolving security needs of modern organizations.

4 Results and Discussion

5G network slicing enables mobile network operators to build a virtual border for a single customer or range of devices. Only approved devices are permitted to connect to the segmented network, reducing this attack vector significantly. Slicing may be used as part of a private network to provide an extra layer of security, or on a public network to add a security layer without incurring the costs associated with maintaining network infrastructure.

Our proposed self-sustainable slicing model (**SSSM**) is compared with the existing local topology control algorithm (LTCA), energy-aware topology model (EATM), Location-aided routing algorithm (LARA) and topology-control algorithm (TCA) as shown in Table 2. The SSSM achieved best in all the experiments, thus applicable for further use.

Table 2. Performance Comparison

Comparison	Model	Accuracy (%)
Spectrum Management Comparison	LTCA	75.0
	EATM	90.0
	LARA	79.0
	TCA	84.5
	SSSM	96.0
Transmission Devices Comparison	LTCA	74.5
	EATM	87.5
	LARA	82.0
	TCA	87.0
	SSSM	95.0
Threat Analysis Comparison	LTCA	76.5
	EATM	85.0

Continued on next page

Table 2 continued

	LARA	77.0
	TCA	83.0
	SSSM	98.5
Wireless Security Comparison	LTCA	65.5
	EATM	85.0
	LARA	80.0
	TCA	80.0
	SSSM	98.0
DoS Attack Comparison	LTCA	73.0
	EATM	81.0
	LARA	72.5
	TCA	74.5
	SSSM	99.5
Anonymous Attacks Comparison	LTCA	41.0
	EATM	80.0
	LARA	60.0
	TCA	72.5
	SSSM	91.0
Data Transfer Comparison	LTCA	38.0
	EATM	79.0
	LARA	59.5
	TCA	62.0
	SSSM	90.5

There is a notion of shared security responsibility when network slicing is employed on public mobile networks. Comparable to cloud computing, where network operators are responsible for safeguarding the infrastructure and the business handles the software security layer.

There is a notion of shared security responsibility when network slicing is employed on public mobile networks. Comparable to cloud computing, where network operators are responsible for safeguarding the infrastructure and the business handles the software security layer.

4.1 Spectrum management

The signals of Mobile Ad-hoc 5G devices have a highly complicated structure and a broad spectrum, so standard radio surveillance equipment cannot detect these signals and the nearby Mobile Ad-hoc 5G devices. The practice has demonstrated that reliable detection of a Mobile Ad-hoc 5G signal by contemporary radio surveillance systems within a broad frequency band is only possible based on an energy characteristic in the presence of parallel analytics bands of several tens of megahertz width at a minimum of 400 velocities and its ranges MHz/s and in the adjacent field zone. Additionally, your network adapter must enable 802.1p tagging for the QoS Packet Scheduler to function effectively. Figure 4 shows a comparison of Spectrum management.

Remote AB signals are below the receiver's noise level. In general, it is difficult to discover Mobile Ad-hoc 5G transmitters by continuous scanning with short band receivers.

4.2 Transmitting Devices

Private Mobile Ad-hoc 5G networks or public Mobile Ad-hoc 5G networks are used at or near each location. Surrounded by such networks, it is very difficult to discern between one's own legal clients and adjacent networks' capacity to obtain sensitive information from clients, which allows to successfully conceal illicit communication between valid Mobile Ad-hoc 5G channels.Figure 5 shows a comparison of Transmission devices.

The 5G Mobile Ad-hoc transmitter is known as an OFDM signal. This indicates that the device transmits one signal at a time, a large frequency range (about 20 MHz), and several carrying information - sub-carriers of the information channels, which are typical receiving device when they are near together, the signal appears as a single "dome." In such a "dome," the subcarriers are segregated and only a specialized receiver can identify the transmitting devices.

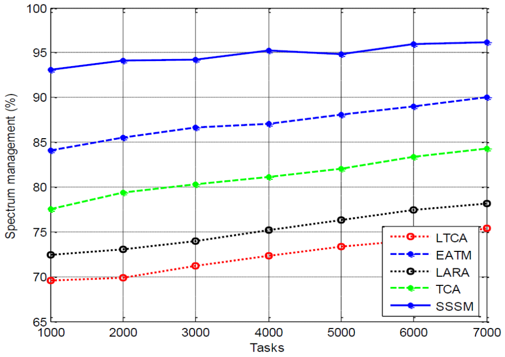

Fig 4. Spectrum Management Comparison

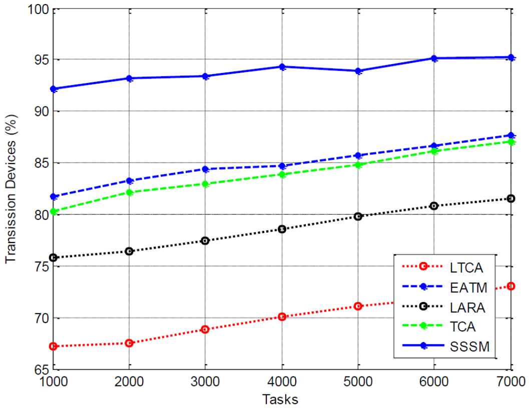

Fig 5. Transmission Devices Comparison

4.3 Threat analysis

The concept of wireless data transport allows for the potential of unwanted access point connections. When establishing a business network, executives must offer not just high-level security for the office's communications, but also the ability to join from a parked automobile on the street. Figure 6 illustrates a comparison of Threat analysis.

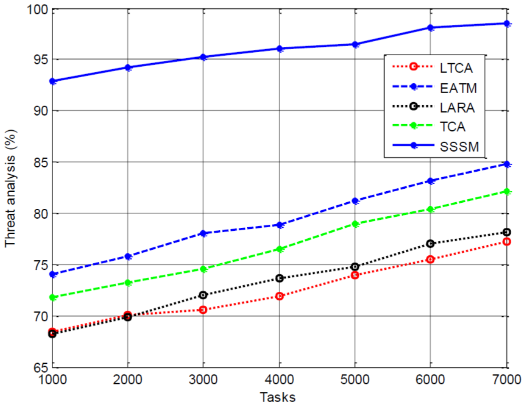

Fig 6. Threat Analysis Comparison

4.4 Wireless Security

Theft of hardware, such as the router, antenna, and adapter, is an equally significant threat to wireless networks. If the wireless network's security policy relies on MAC addresses, an attacker's stolen network card or router will provide access to the network. Figure 7 demonstrates a comparison of wireless security.

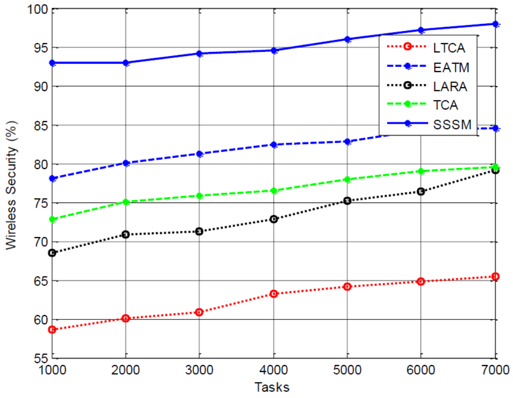

Fig 7. Wireless Security Comparison

4.5 Denial of service

A denial of service (DoS) attack may be carried out in several ways. If a hacker is successful in establishing a connection to a wireless network, his malicious conduct might have severe implications, such as altering the ARP tables of network devices by sending answers to the Address Resolution Protocol (ARP). Figure 8 illustrates comparisons between Denial of Service.

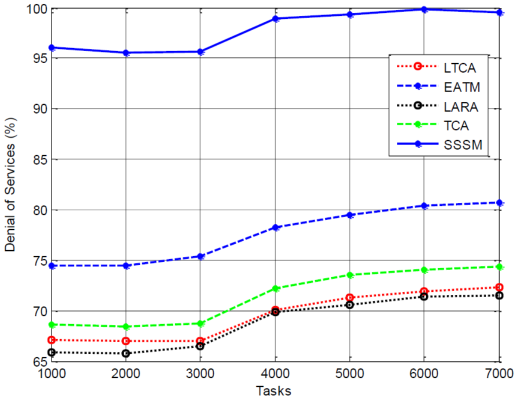

Fig 8. DoS Comparison

Operating an unauthorized Dynamic Host Configuration Protocol (DHCP) server on the network or giving inactive addresses and network masks is a security risk. If a hacker discovers information about wireless network systems, he may reconnect users to his access point, disconnecting them from the network services accessible through the "legal" access point.

4.6 Anonymous attacks

It can both intercept and encrypt radio messages. The technology needed to tap into a network is no more advanced than the equipment used to access that network daily. To intercept the signal, an adversary must be in close proximity to the transmitter. These sorts of disruptions are almost hard to capture and tough to avoid. Figure 9 depicts a comparison between Anonymous Attacks.

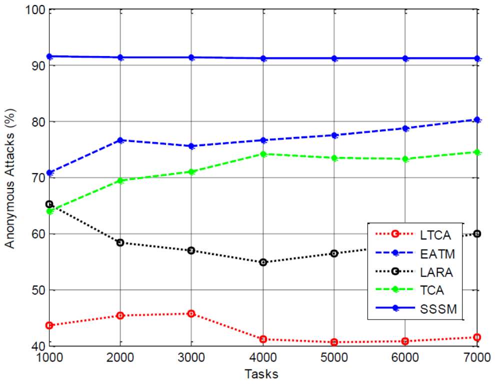

Fig 9. Anonymous Attacks Comparison

During the interception procedure, the use of antennae and amplifiers allows the attacker to be at a great distance from the target. Eavesdropping permits the gathering of information about a network, which is then assumed to be under attack. The major objective of the attacker is to determine who uses the network, what data it contains, the capabilities of the network tools when it is seldom and actively used, and what portion of it is being used.

4.7 Data transfer

The mobile Ad-hoc 5G - Enables the movement of resources, voice, data, and video in real-time over network channels. This aspect creates several options for devices that intercept the information. Now, not just audio data from PCs or a local network is at risk, but also video data. Figure 10 illustrates a comparison of Data transmission.

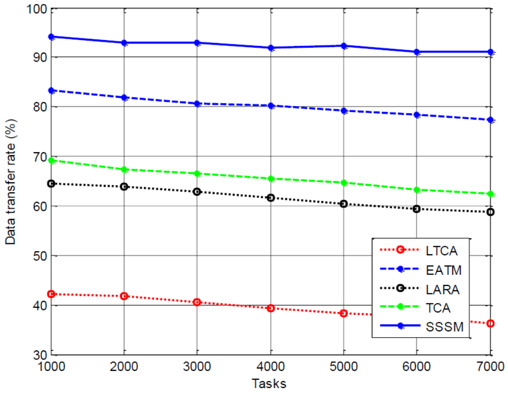

Fig 10. Data Transfer Comparison

5 Conclusion

The number of 5G devices under development is increasing exponentially. The 5G technology’s greatly enhanced speed, decreased latency, and device density support (devices/region) provide new options for unique use cases. The growth in the number of connected devices will rapidly establish 5G as an essential infrastructure for business continuity and a highly desirable target for hostile actors attempting to exploit linked devices for illegal purposes.

The implementation of 5G and the IoT are part of a worldwide transformation that is integrating cellular technology into every area of our lives, from electricity meters to fleet monitoring. As 5G becomes part of the crucial infrastructure that governs our everyday lives, it is essential to include security in the design, deployment, and maintenance of every 5G network architecture.

The Analysis of wireless network risks, the most aggravating threat to strangers, frequent non-communication, reluctance to turn around and listen. It obtains the key using a slicing pseudo-random number generator. Due to the fact that the last component is not encrypted, a third party may regenerate the WEP key. The suggested Slicing method for securing data on wireless networks demonstrates the applicability of the mobile Ad-hoc 5G programme. The mobile Ad-hoc 5G programme is an enhanced wireless certification scheme. The mobile Ad-hoc 5Gene offers advanced encryption standard (AES) encryption and improves data security and wireless access management. Set the network SSID and, if possible, activate mobile Ad-hoc 5G encryption and pick the key input method in the box that displays. It is possible to assign generation to the operating system or manually input the keys. If the first option is chosen, a dialogue will appear requesting the required key (or keys).

In future, we will be implementing a hybrid Deep Learning technique to secure the 5G / 6G Network since they are highly dependent on the SDN level for traffic control.

6 Declaration

Presented in 4th Mizoram Science Congress (MSC 2022) during 20th & 21st October 2022, organized by Mizoram Science, Technology and Innovation Council (MISTIC), Directorate of Science and Technology (DST) Mizoram, Govt. of Mizoram in collaboration with science NGOs in Mizoram such as Mizo Academy of Sciences (MAS), Mizoram Science Society (MSS), Science Teachers' Association, Mizoram (STAM), Geological Society of Mizoram (GSM), Mizoram Mathematics Society (MMS), Biodiversity and Nature ConservationNetwork (BIOCONE) and Mizoram Information & Technology Society (MITS). The Organizers claim the peer review responsibility.

References

1) Subedi P, Alsadoon A, Prasad PWC, Rehman S, Giweli N, Imran M, et al. Network slicing: a next generation 5G perspective. *EURASIP Journal on Wireless Communications and Networking*. 2021;2021(102):1–26. Available from: https://doi.org/10.1186/s13638-021-01983-7.
2) Lv J, Man D, Yang W, Gong L, Du X, Yu M. Robust Device-Free Intrusion Detection Using Physical Layer Information of WiFi Signals. *Applied Sciences*. 2019;9(1):1–17. Available from: https://doi.org/10.3390/app9010175.
3) Lugovic S, Mrsic L, Korona LZ. Public WiFi Security Network Protocol Practices in Tourist Destination. In: International Symposium on Pervasive Systems, Algorithms and Networks: Pervasive Systems, Algorithms and Networks. Springer International Publishing. 2019;p. 321–332. Available from: https://doi.org/10.1007/978-3-030-30143-9_27.
4) Bhardwaj A, El-Ocla H. Multipath Routing Protocol Using Genetic Algorithm in Mobile Ad Hoc Networks. *IEEE Access*. 2020;8:177534–177548. Available from: https://doi.org/10.1109/ACCESS.2020.3027043.
5) Ande R, Adebisi B, Hammoudeh M, Saleem J. Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*. 2020;54:101728–101728. Available from: https://doi.org/10.1016/j.scs.2019.101728.
6) Haque ME, Baroudi U. Dynamic energy efficient routing protocol in wireless sensor networks. *Wireless Networks*. 2020;26:3715–3733. Available from: https://doi.org/10.1007/s11276-020-02290-7.
7) Shah SDA, Gregory MA, Li S. Cloud-Native Network Slicing Using Software Defined Networking Based Multi-Access Edge Computing: A Survey. *IEEE Access*. 2021;9:10903–10924. Available from: https://doi.org/10.1109/ACCESS.2021.3050155.
8) Zhang Y, Wu A, Chen Z, Zheng D, Cao J, Jiang X. Flexible and anonymous network slicing selection for C-RAN enabled 5G service authentication. *Computer Communications*. 2021;166:165–173. Available from: https://doi.org/10.1016/j.comcom.2020.12.014.
9) Kourtis MAA, Anagnostopoulos T, Kuklilski S, Wierzbicki M, Oikonomakis A, Xilouris G, et al. 5G Network Slicing Enabling Edge Services. In: 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 10-12 November 2020, Leganes, Spain. IEEE. 2020. Available from: https://doi.org/10.1109/NFV-SDN50289.2020.9289880.
10) Serckumecka A, Medeiros I, Ferreira B, Bessani A. SLICER: Safe Long-Term Cloud Event Archival. In: 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), 01-03 December 2019, Kyoto, Japan. IEEE. 2019. Available from: https://doi.org/10.1109/PRDC47002.2019.00021.
11) Zhang S. An Overview of Network Slicing for 5G. *IEEE Wireless Communications*. 2019;26(3):111–117.
12) Sun G, Xiong K, Boateng GO, Liu G, Jiang W. Resource slicing and customization in RAN with dueling deep Q-Network. *Journal of Network and Computer Applications*. 2020;157:102573–102573. Available from: https://doi.org/10.1016/j.jnca.2020.102573.
13) Esmaeily A, Kralevska K, Gligoroski D. A Cloud-based SDN/NFV Testbed for End-to-End Network Slicing in 4G/5G. In: 2020 6th IEEE Conference on Network Softwarization (NetSoft), 29 June 2020 - 03 July 2020, Ghent, Belgium. IEEE. 2020;p. 29–35. Available from: https://doi.org/10.1109/NetSoft48620.2020.9165419.
14) Hussain R, Hussain F, Zeadally S. Integration of VANET and 5G Security: A review of design and implementation issues. *Future Generation Computer Systems*. 2019;101:843–864. Available from: https://doi.org/10.1016/j.future.2019.07.006.
15) Butt UA, Mehmood M, Shah SBH, Amin R, Shaukat MW, Raza SM, et al. A Review of Machine Learning Algorithms for Cloud Computing Security. *Electronics*. 2020;9(9):1–25. Available from: https://doi.org/10.3390/electronics9091379.
16) Barakabitze AA, Ahmad A, Mijumbi R, Hines A. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*. 2020;167:1–40. Available from: https://doi.org/10.1016/j.comnet.2019.106984.
17) Cheng X, Wu Y, Min G, Zomaya AY, Fang X. Safeguard Network Slicing in 5G: A Learning Augmented Optimization Approach. *IEEE Journal on Selected Areas in Communications*. 2020;38(7):1600–1613. Available from: https://doi.org/10.1109/JSAC.2020.2999696.
18) Wichary T, Batalla JM, Mavromoustakis CX, Zurek J, Mastorakis G. Network Slicing Security Controls and Assurance for Verticals. *Electronics*. 2022;11(2):1–29. Available from: https://doi.org/10.3390/electronics11020222.

19) Khan AA, Abolhasan M, Ni W, Lipman J, Jamalipour A. An End-to-End (E2E) Network Slicing Framework for 5G Vehicular Ad-Hoc Networks. *IEEE Transactions on Vehicular Technology*. 2021;70(7):7103–7112. Available from: https://doi.org/10.1109/TVT.2021.3084735.

20) Hamdi MM, Audah L, Rashid SA, Mohammed AH, Alani S, Mustafa AS. A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs). In: 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 26-28 June 2020, Ankara, Turkey. IEEE. 2020;p. 1–7. Available from: https://doi.org/10.1109/HORA49412.2020.9152928.

21) ño IGM, Lacuesta R, Rajarajan M, Lloret J. Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain. *Ad Hoc Networks*. 2019;86:72–82. Available from: https://doi.org/10.1016/j.adhoc.2018.11.010.

22) Mazurczyk W, Bisson P, Jover RP, Nakao K, Cabaj K. Challenges and Novel Solutions for 5G Network Security, Privacy and Trust. *IEEE Wireless Communications*. 2020;27(4):6–7. Available from: https://doi.org/10.1109/MWC.2020.9170261.