Improving User Equipment Privacy using Non-Redundant Traffic Authentication Scheme in 5G Networks

Sakthibalan P (balan11091@gmail.com)
Annamalai University
Devarajan K
Annamalai University

Research Article

Keywords: 5G Communication, Data Security, Key Generation, Traffic Classification, Sequential Authentication

Posted Date: May 4th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-438746/v1

Improving User Equipment Privacy using Non-Redundant Traffic Authentication Scheme in 5G Networks

Sakthibalan P [a,*], Dr. Devarajan K [b]

[a] Assistant Professor, Annamalai University, Annamalai Nagar -608002, Tamil Nadu [b] Assistant Professor, Annamalai University, Annamalai Nagar -608002, Tamil Nadu Email: : balan11091@gmail.com; devarajan_lecturer@yahoo.com

* Corresponding Author - balan11091@gmail.com

Abstract

End-to-end authentication is a critical necessity in 5G networks due to increasing device demands and autonomously transmitted user data. A difficult problem in obtaining shared information is the lack of data-related characteristics and the communicating network. Furthermore, due to the network's lack of traceability and handoff, managing protection for the created data is impractical. The non-redundant traffic authentication scheme (NRTAS) is proposed with the aim of authenticating data sources and contact traffic through active user equipment. This scheme provides more efficient non-replicated authentication by classifying traffic based on its errors. Using a differential private key, the classified traffic is authenticated in a linear or discrete way. The suggested scheme's mechanism is tailored to all of the available contact slots, increasing the likelihood of success. Non-redundant authentication eliminates information sharing overhead while simultaneously achieving the shortest access time and response delay.

Keywords—5G Communication, Data Security, Key Generation, Traffic Classification, Sequential Authentication

1. Introduction

Fifth generation (5G) wireless communication technology provides various insights by assimilating different standards and protocols with interoperable features for heterogeneous users. This advanced communication technology is expected to improve the overall development of multiple applications and integrated smart city environment by providing pervasive access to the resources and ease of scalability [1]. It is capable of interconnecting diverse applications operated using smart user equipment's (UEs), communicating machines, intelligent "objects", things (as in Internet of Things), etc. The features of 5G communication are reliable data

processing, improved resource allocation strategies, flexible service provisioning, etc [2, 3]. Mobile and cellular communication in this environment permits interoperable and adaptable technology insights by providing heterogeneous and scalable platform of ease of access. 5G communication technology integrates the existing paradigms such as multi-input, multi-output (MIMO), human computer interaction (HCI) systems, device-to-device (D2D), vehicular communication network (VCN), software defined networks (SDNs), distributed cloud network (CN). The diverse paradigms are jointly used for resource allocation, query processing, resource slicing, storage, computation offloading, seamless service, offloading, as requested by the UE and the deployed application [4, 5].

The fundamental building block of the communication network is the wireless channel or medium. This wireless channel encloses a variety of challenges in deployment due to its openness and ease of access. The prime issue is the security that is mandatory in this autonomous and heterogeneous platform [6]. The security measure adopted by the user and the service provider over different applications is not similar and therefore, escalating such measures in coherence to the service provider increases the complexity in processing. Different from this issues, the type of security administered for the communication environment is notable as it requires both device and data security [7]. Data authentication is the conventional measure adopted in the communication systems, to improve the reliability and confidentiality of the end-to-end data sharing. The receiving terminal demands data freshness and integrity irrespective of the different adversaries that are experienced in the transmission and information exchange process. With the help of different security infrastructures such as intrusion detection systems (IDS), firewall, authentication server, peer-to-peer encryptions, the security requirements of the users are satisfied. Though, the security requirements are satisfied in a convenient manner, the demand for authentication increases due to the volume and interval of data and resource handled by the communicating and sharing terminals [8, 9].

The rate of data shared/ exchanged in a communication interval is unpredictable due to the varying user and request densities. In a 5G environment, the radio resources are provided at ease with fewer constraints and therefore, the utilization ratio is greatly improved. Besides, the service provider ensures optimal handoff, service pause ability, offloading, shared storage, slotted communication, collision-less data exchange, to augment the resource utilization and availability in a verge to improve the service reliability of 5G systems [2, 3]. Contrarily, the rate

of data/ resource exchanged and shared needs to be provided with defined security measures to ensure application reliability and concealed communication. Providing security for the generated traffic is less feasible due to the limitations in communication architecture and computation capability of the communicating terminals [4, 5]. Therefore, traffic classification becomes a necessary process for ensuring service compliance in an end-to-end manner. Based on the different applications, the class of traffic and the resource utilization varies. Identifying the appropriate traffic without errors helps to provide reliable authentication and ensuring data integrity [10, 11]. The contributions of the article are listed as follows:

i. Design and validation of non-redundant traffic authentication scheme for strengthening the privacy of the users, by improving the communication success rate.
ii. Presenting a traffic classification method based on resource utilization and allocation probability ensuring reliable authentication is provided.
iii. Providing end-to-end authentication by classifying linear and discrete communication in the established session without additional overhead and response delay.
iv. Performing a comparative analysis of the proposed NRTAS with the existing techniques and assessing its performance using different metrics.

The organization of the article is as follows: Section 2 discusses various contributions that are proposed in the past. In Section 3, the proposed NRTAS is discussed with the traffic classification and end-to-end authentication methods. The performance assessment of the proposed scheme is detailed in Section 4 with a comparative study, followed by the conclusion in Section 5.

2. Related Works

Celik et al. [12] proposed a 5G device-to-device communication to increases the throughput and coverage and decreases the power consumption of the cellular environment. The author addresses the issues such as eavesdropping, jamming, primary user emulation attack and injecting attack because the multi path routing emerges some of the security issues and simulation reveals more effective eavesdropping.

5G Narrow Band Internet of Things (NB-IoT) System in massive device is introduced by Cao et al. [13] to resolve the mutual authentication by the traditional access. The NB-IoT addresses the access authentication and data transmission of a group of NB-IoT devices based on the lattice-based homomorphism encryption technology. It reduces the network burden and private security and anti-quantum attack.

Block chain and content centric in 5G network was observed by Fan et al. [14]. In the upcoming 5G era the information should be protected in the network. The author proposed the scheme on block chain to solve the privacy issues in content-centric mobile networks for 5G. The mutual trust is implemented in between the content provider and the user.

Garrocho et al. [15] proposed Device-to-Device (D2D) pervasive communication system reduces the mobile traffic load, reduce energy consumption and effectively use the available electrical radio spectrum. The author presented a middleware based on Wi-Fi infrastructure mode that establishes connections and performs data exchange without human interaction.

A Dynamic Chameleon Authentication Tree (DCAT) is introduced by Xu et al. [16] for verifiable data streaming in 5G networks. The DCAT is divided into four phases: setup, append, query, verification. At the time of data querying phase the average authentication path length is been reduced that leads to the space requirement and better form of verification.

Service Oriented authentication for 5G enabled IoT is proposed by Ni et al. [17]. An efficient and secure service oriented authentication (ES3A) framework supporting network slicing and fog computing for 5G-enabled IoT services is proposed. It is developed to setup the connection with the 5G core network and anonymously access IoT service. The privacy slice selection mechanism is used to make a secure access of data.

An efficient quantum-based security protocol is observed by El-Latif et al. [18]. A new efficient cryptographic protocols and mechanisms are needed in order to design and achieve information sharing and data protection protocols in 5G networks. QWHF-1 and QWHF-2 is the two efficient hash function mechanism for 5G network is been developed.

3GPP 5G Network for massive NB-IoT is proposed by Cao et al. [19] for popularization and application of mobile Internet standards. NB-IoT employs the traditional authentication process of User Equipment (UE). The method ensures robust security protection including user anonymity and non-repudiation.

Software-defined services-based Network Security is introduced by Guan et al. [20] for 5G security. Software Defined Security (SDS) is a security paradigm that is more flexible and centralized security protection. The author proposed a scheme that adopts Group Routing Betweenenss Centrality (GRBC) as a metric and introduces a successive algorithm to compute the GRBC.

Ying and Nayak [21] proposed a lightweight and remote user-untraceable authentication protocol (LRUAP) for multi-server-based 5G networks. It is introduce to reduce the computational complexity, self-certified public key cryptography is based on the elliptical curve to authenticate the validate user and server.

Zhang et al. [22] observed a Privacy-Preserving Communication and Power Injection for Vehicle to grid and 5G smart grid slices. The aim is to tackle the security and privacy issues in Autonomous Vehicle Network (AVN) s. Hash-then-homomorphism is used to aggregate the blinded bids of different time slots and the individual bids are hidden and secure Vehicle –to-vehicle (V2V) communication is been ensured.

Xie and Hwang [23] proposed a two factor security in smart city by security enhanced roaming authentication. While providing convenience, mobile networks face a series of challenges in security and privacy protection due to the ability of the terminal. To fix this issue the two factor security is been introduced.

Massive MIMO systems for 5G communications is introduced by Yang et al. [24] for awareness theory of 5g-oriented MIMO system security. It is based on the MIMO system of 5G secure network and it is under the situation of awareness technology, security situation awareness system of 5g-oriented large-scale MIMO system is modeled.

Celdrán et al. [25] proposed a autonomous provision of self-protection in 5G network. Self-protection is a critical capability of Self-Organizing Networks (SON) focused on protecting the network resources in a flexible and autonomic way. Software Defined Networking and Network Functions Virtualization technologies are used to optimize the usage of network resources for monitoring services.

The methods presented in the above survey are restricted in performance due to varying UE and traffic conditions. Administering unanimous security throughout the communication process, and retaining the response success rate is less feasible. The reasons are centrality [20], virtualization [as in 25], privacy selection [as in 17], etc. This article focuses on the privacy

method without compromise in authentication retaining the response success rate under controlled time for varying UE density.

3. Non-Redundant Traffic Authentication Scheme (NRTAS)

The design goal of NRTAS is to improve the communication security of the users by verifying the instantaneous traffic flow. This scheme facilitates concealed data exchange and communication between the heterogeneous users by mitigating the impacts of adversary authentication and it also prevents suspicious traffic incusing in the concealed link. The false authentication based complex and redundant security measures are mitigated by this scheme. In the following section, the communication architecture along with the interface model is presented.

Communication Architecture

The design of 5G communication architecture is differentiated into three layers namely user equipment (UE), access and resource. An illustration of the layers is presented in Fig. 1.

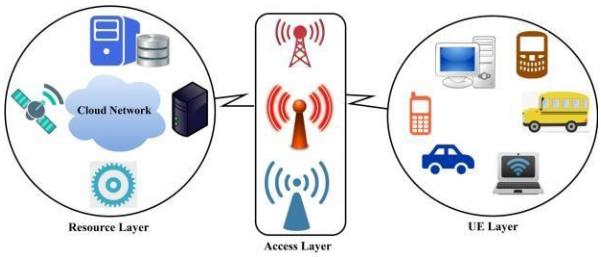


Fig. 1. 5G communication Illustration

In the UE layer, heterogeneous devices are present that requires the communication and information exchange through the other layers. Users of different classes including residential, commercial, industrial, transportation system, etc. form the fundamental elements of this layer. The UE's initiate communication request and resource access through specific applications. Access layer components such as gateways, access points, hotspots, etc. provide Communication bridge between UE and resource layers. Handoff, mobility support, pervasive accesses are the functions delivered from this layer. Resource layer houses different communication and service providers, heterogeneous network, and virtualization functions. With the aid of these functions, universal resource access, retrieval and storage is granted for the UE. Service response, user access control and security features are determined in this layer. The type and model of the security and its attributes vary with the service providers.

In this communication architecture, traffic generated by this user is classified by the resource layer. The classified traffic is disseminated through the access layer to prevent congestion and communication slot overloading. Instead, traffic authentication is an end-to-end process modeled between resource and UE layers. The authentication projected by the service provider is pursued by the access layer and is delivered to the UEs.

The composition of UE's in a 5G environment makes up a heterogeneous assimilation of interconnected devices. The communication standards and protocols employed in this environment differ with the UE capacity and applications.

However, Let I denote the set of interfaces $\{ I_1, I_2, \dots, I_n\}$, where n is the number of UE. The access layer device allocates S slots $\{ _1, S_2, \dots, S_n\}$ in the communication process. The allocated interfaces are divided into $\frac{I}{S}$ slots of even response of the resource layer. The proposed scheme consists of two different working phases namely traffic classification and end-to-end authentication. The following session discusses the traffic classification and authentication process in detail.

Traffic Classification

The type of traffic generated by the UE and the resource granted varies with the user requirement and application type. For example, the service request of a user relaying on transportation system is different from that of user demanding multimedia service. The type of traffic is classified is sensed from the interface allocated and the attributes associated with it. The attributes refers to the allocated bandwidth transmit power signal strength, etc. as preferred by the service provider. Let t_r be the traffic request time that prolongs for a maximum time oft_m. Therefore, the interval of $\frac{I}{S}$ is $[t_r, t_r + t_m]$. Let (t) denote the set of attributes associated with the traffic as observed in the above time interval. The attributes are discovered, classified and address using v vectors such that

$$\{ (t_{r-1}), v \leq 0 \quad \} \quad (1)$$
$$subject\ to \arg\min [(t_r), (t_r + t_m)] \forall (a, v) \in A\ and\ v \geq 0$$

The representation in equation (1) demands the error $[.]$ between the attribute matrix $A_v(t)$ and the response matrix is $R(t_r + t_m)$. The errors are estimated as the different between actual and compromised (false) response observed in the time $(t_r + t_m)$. The attributes set $\{a_1(t), a_2(t), \dots a_n(t)\} \in (t)$ that relies on the flow rate (f_r) observed in $\frac{I}{S}$ interval. The f_r is

computed between $[t_r, t_a]$ interval, after which $(t_r + t_m)$ is the time for response. The consecutive flow assignment probability (ρ_{f_r}) is then estimated using equation (2) as

$$\rho_{f_r} = \frac{f_r[A_v]}{\{E\,[(t_r)] \cup A_v(t_r - 1)]} \quad \} \qquad (2)$$
$$such\ that, t_r < t_a \leq [t_r + t_m]$$

In equation (2), the next set of traffic that is to be disseminated is estimated. There are two cases in classifying $f_r$and A_v namely $t_a < t_r + t_m$ and $t_a = t_r + t_m$.

Case 1: If the access time is less than the response time (i.e.) $+ t_m > t_a$.

Validation 1: In this case, the response is initiated with a time difference after receiving the request. Resource allocation is performed at a different time instance such that $(t_a - t_r) \neq 0$. Therefore, the response is shared allocating the available resource in a sequential manner. Thus, the chances of [.] is less in this case. On the other side, this is not a final validation as the resource allocation and response varies abruptly due to multiple accesses.

The classification here is A_v and [.] and the order is represented as

$$traffic = (t_{r-1}) + \alpha_1(t_{r-2}) + \cdots + \alpha_n A_v(t_{rn}), \forall v \geq 0$$
$$Erro = \{(t_{rn}) \cap \rho\}_r \quad \} \qquad (3)$$

In this case, the authentication is required in a sequential manner without considering the error case. Therefore, the decision of administering security for $^{I} \underset{S}{\in} [t_r, t_r + t_m]$ is made by the service provider. This decision is pursued for all I in different S in a unanimous manner until error is encountered.

Case 2: if the access time is same as the response time $(i.e.)t_a = [t_r + t_m]$

Validation 2: In this case analysis, if there is no time difference between the access and response time, then the entire sequence of $\rho_{f_r}$is considered as an error. In simple terms, the errors have left in failed or dropped responses. The UE has to re-initiate the service discovery and access. The error in this sequence is computed using equation 3(a)

$$Error = (t_{r1}) + (t_{r2}) + \cdots + A_v(t_{rn}), for\ any\ v < 0 \& \rho_{f_r} = 0 \qquad (3a)$$

This sequence of traffic is not accounted by confining the slots allocated fort_r. Post the interface replacement and slot variation, the $f_r$is classified again using the above instances. The traffic generated in this instance [as denoted in equation (3)] is provided with authentication. This authentication process for linear and discrete traffic is discussed in the following section.

End-to-End Authentication

End-to-End traffic authentication relies on the classified f_r as discussed above. This ensures the linear or discrete traffic is alone provided with authentication. Administering end-to-end concealed authentication varies with the identified traffic for its linearity and discreteness. Both the process of authentication employs tree based measures for expelling replications.

Linear Authentication

In a linear authentication, the sequence of traffic as in equation (3) is considered with an assumption that no-retransmission of the request is generated in $\frac{I}{S}$. This means, the re-transmission of the service requests are generated in different t_r. With this consideration, the traffic sequence for 1 to n UE's sharing a common I with independent S at different t_r and $\frac{I}{S}$ intervals, the authentication is modeled. Let the $[t_r + t_m]$ be different for each $\frac{I}{S}$ for which a secret key (s_k) is generated to conceal the communication. It is to be noted that s_k is valid for traffic without [.] and for request transmissions (re-transmission follows different t_r. Therefore, the validity of s_k is modeled between $[t_r, t_r + t_m]$. The encryption process and the secret key are jointly used for authenticating the message exchange sequence. The sequence (q) of s_k demand is constructed as

$$\left.\begin{matrix} = s_1 + \cdots + \ + im_1 + m_2 + \cdots + m_n|p1|, if\ 1 \le i \le m \\ S_1 + 2^{i-m-1}S_2 + \cdots + m^{I-M-1}|P|, If\ M < i < s \end{matrix}\right\} \quad (4)$$

The sequence is modeled for a message M of length m and the available slots S for the $n \cup E_s$.

In a linear tree representation, the s_k generated for m and S must be different to prevent unnecessary key computation. The sequence is then constructed as

$$\begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_s \end{pmatrix} = \begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1m} \\ s_{21} & s_{22} & \cdots & s_{2n} \\ \vdots & \vdots & & \vdots \\ S_{t_r^1} & S_{t_r^2} & & S_{t_r^m} \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} \quad (4a)$$

In equation 4(a), if $t_r = m$, then the s_k sequence is generated for either of the occurrence. Therefore, if the above condition occurs, the s_k required is $q - S_{t^m}\forall\ t_r = m$. The linear tree constructed and modified for the cases in equation (4) and (4a) is illustrated in Fig. 2(a) and 3(b).

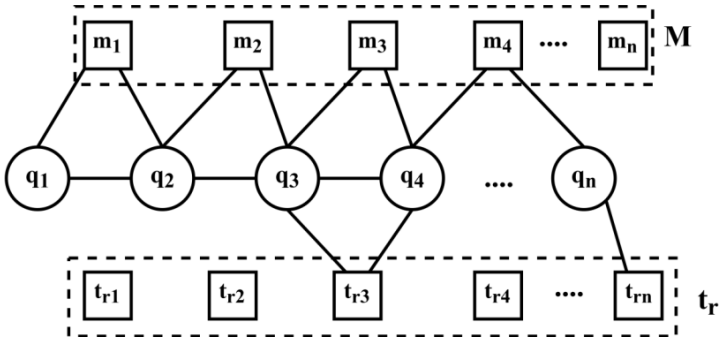


Fig. 2(a). Normal Sequence of q_i

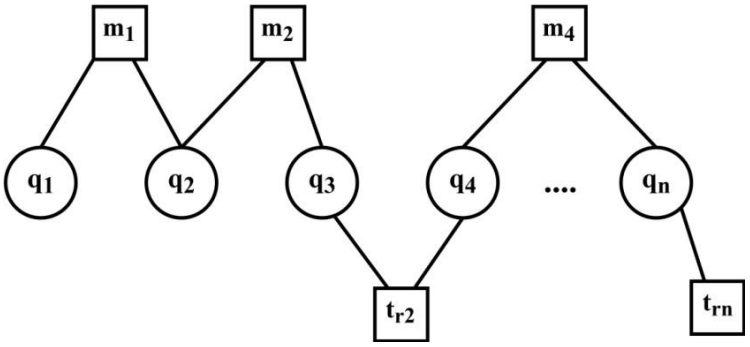


Fig. 2(b). Modified Sequence of q_i

The linear tree as represented in 2(b) consists of s_k modeled for either m ort_r. Therefore, dual and replicated secret key for securing the communication session is prevented. In a probable analysis of sequential f_r, the elements S_{11}, S_{22}, . . S_{mm} or $S_{t_r t_r}$] are expelled by replacing the session with one key instance. The process of encryption follows signature (K) for the M in either S ort_r. The hash of a message is a combination of $[(M), \beta, k]$ where (M) is the cipher of the message M that is secured usingk_1. The entire hash is assimilated usings_k. The process of generating s_k and (M) is presented as follows. The variable β is a random integer from the sequence q. The signature is estimated using equation (5)

$$k = [\frac{\beta}{h(r,q_i) - h(R,P_{UE})}] \quad and \quad \beta = \frac{\sum m - \sum t^r}{i}, i \in q \quad \} \tag{5}$$

Where, P_{UE} is the public key of the UE. In this authentication process, let P_s, Q_{UE} and Q_S denote the public key of the service provider, and private key of the UE and service provider respectively. The s_k is generated with this combination as

$$s_k = \begin{cases} P_S.Q_{UE}.|p| \oplus \frac{q}{|m|}\frac{i.\beta}{}, if\ q_i \in m \\ P_S.Q_{UE} > |p| \oplus \frac{q^{i.\beta}}{|t_r|}, if\ q_i \in t_r \end{cases} \quad (6)$$

The cipher of the message (M) is computed as $(Q_{UE} > M)$. Finally the authentication is provided with the integrated package of $[(M), \beta, k]$ and s_k that is denoted as $h([C(M), \beta, k].\ s_k)$. This process of securing the M is valid only $\rho_{f_r} \in$ traffic sequence as in equation (3). Now, the s_k generation sequence for the matrix as in equation 4(a) is represented as

$$\begin{matrix} q_s = S_{1t_r}m_1 + S_{2t_r}m_2 + \cdots + S_{nt_r}m_n \\ q_{t_r} = S_{nt_{r1}}m_1 + S_{nt_{r2}}m_2 + \cdots + S_{nt_{rn}}m_n \end{matrix}, \forall n \neq t_r\ and\ n \in S\} \quad (7)$$

The above sequence for a linear validation is used for a communication session stabled in $\frac{I}{S} \in [t_r, t_r + t_m]$ interval. The sequence q_i is halted in generating β if error is encountered or $\rho_{f_r} = 0$.

Discrete Authentication

Unlike linear authentication, discrete authentication follows either t_r or m based s_k generation until the next sequence change is observed. The authentication $'q'$ is switched over if there is a replication as with $t_r = m$ instance. In particular, the change in s_k is observed if $\rho_{f_r} = 0$, the cause of (i.e.) either $or\ t_r$ is temporarily suspended until $\rho_{f_r} \neq 0$ condition is achieved. The s_k generation and k determination is different based on the discrete representation of q_i based on S and m independently. The discrete (q_i) is represented as

$$d(q_i) = \begin{cases} (S_1 - [.]_0) + (s_2 - \Delta[.]_1) + \cdots . + (S_n - \Delta^{n-1}E[.]_n) \\ (S_{\ 1} - E[.]_0) + (2^{i-\Delta-1}S_2 - \Delta E[.]) + \cdots . + (2^{i-\Delta^{n-1}} - \mathbb{S}_{\ n} - \Delta^{n-1}[.]_n\ \ ) \end{cases} \quad (8)$$

In equation (8), the discrete sequence is represented for the q_i with respect to S and m respectively. Instead, in equation (8), either of sequence is alone true as the existence of both is denied. Therefore, if the sequence is known and the adversary mitigate the session, then (q_i) with modified or new s_k and generation process reduces the impact of $(t_r + t_m)$. Leaving out the errors, the change in q_i is considered to secure the communication session, without halting the exchange interval. Therefore, the additional delay due to new interval assigning and request re-transmission is confined in this process. In order to address the discrete representation of equation (8), the normalization of this process is mandatory. In this process, the boundary of the switch over between m and t_r is defined as

$$q_s" = \{ \begin{matrix} q_i\,(m), q_i\,(E[.\,]) \\ q_i(E[.\,]), q_i\,(t_{rn})] \end{matrix} \quad 8(a)$$

This boundary of q_E can be either a vice-verse relaying on the [.]. The change in Δ denotes the need for $q_s"$in $[t, t_r + t_m]$, where$t_r < t \leq (t_r + t_m)$. The finite validation of the required $q_s"$ is augmented by approximating the boundary estimated as

$$\begin{aligned} q_s" &= d(q_{\,i}) + f(q_{t_r}) \pm \Delta \\ q_s"(m) &= \int \frac{d}{d_m}(q_i) + \int \frac{d}{d_m}(q_{t_r}) \\ q_s"\,(t_r) &= \int \frac{d}{d_{t_r}}(q_i) + \int \frac{d}{d_m}(q_{t_r}) \pm \Delta \} \end{aligned} \quad 8(b)$$

If the above differentiation is found to lie between the appropriate boundaries defined in equation 8(a), then the authentication process initiated. The problem here is the finite validation of splitting the boundary as defined in 8(a). The finite point $(\mathbb{P})$ is computed as

$$\mathbb{P} = \{ \begin{matrix} \frac{q_i(E[.])-q_i(m)}{q_i(t_{rn})-q_i(m)}, q_s \in q_s"\,(m) \\ \frac{q_i(t_{rn})-q_i(E[.])}{q_i(t_{rn})-q_i(m)}, q_{s_r} \in q_s"\,(t_{rn}) \end{matrix} \quad 8(c)$$

The authentication sequence is now classified on the basis of $\mathbb{P}$ from which the process is instigated. In Figure 3(a), 3(b), the modified sequence for $q_s \in q_s"(m)$ is represented.

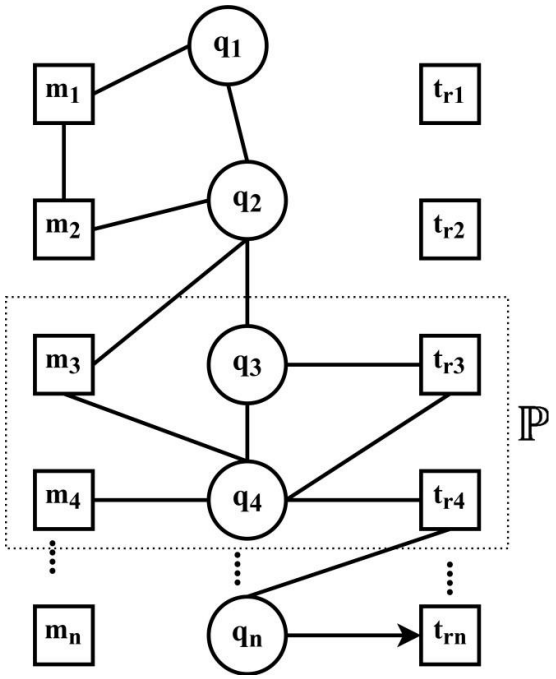


Fig. 3(a). $q_s \in q"$

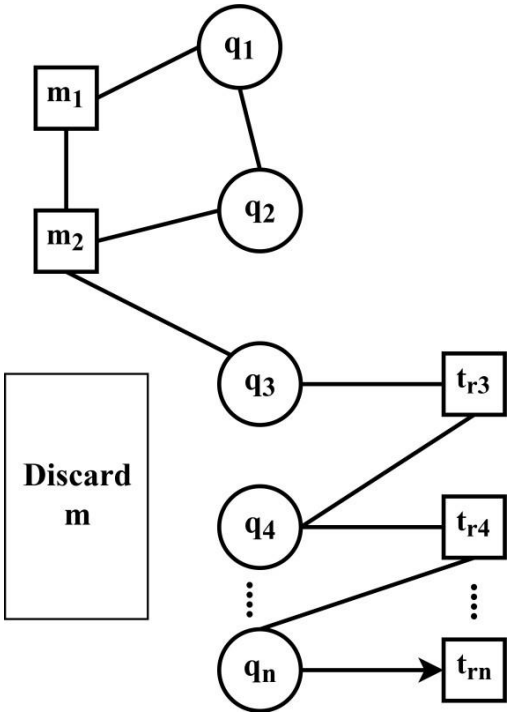


Fig. 3(b). Modified $Q_s based\ on\ \mathbb{P}$

The process of s_k and K varies with $E[.]$ observed in the sequence. The difference sequence of s_k and K are defined using equation 9(a) and 9(b) respectively.

$$s_k = \begin{cases} p_s.\, Q_{UE}.\, |p| \oplus \frac{q_s"(m)}{|m|}, if\ q_s \in q_s"(m) \\ p_s.\, Q_{UE}.\, |p| \oplus \frac{q_s"(t_r).E[.]}{|t_r|}, if\ e[.] \le q_s \in q_s"(t_r) \end{cases} \quad 9(a)$$

$$k = \begin{cases} \left[\frac{E[.]}{h(R,q_i) - h(\mathbb{P},P_{UE})}\right], if\ q_s \in q_s"(m) \\ \left[\frac{E[.]}{h(\mathbb{P},P_{UE}) - h(\mathbb{P},q_i)}\right], if\ q_s \in q_s"(t_r) \end{cases} \quad 9(b)$$

The value of s_k and K varies with the differentiation norm is equation 3(b) satisfying the boundary condition in 8(a). Another condition to be satisfied for non-replicated authentication is $[(m) < P \le (E[.])\ ]$and$[q_i(E[.]) < P \le q_i(t_{rn})]$

4. Performance Assessment

In this section, the performance assessment of NRTAS is presented with the appropriate validation environment and its associated metrics. In this validation process, a network with 300m*300m region with 150UEs is considered. The communication is modeled using wireless interface of 2Mbps bandwidth and the maximum accessible resource is 500Mb for each device.

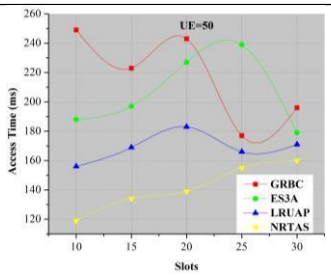
The performance environment is modeled as shown in Fig. 1, for which the experimental environment is used as in Table 1. The application modeled is voice, data and web access used as a constant bit rate calibration for multiple devices. Based on the request flow per unit time, the traffic flow varies.

Table 1 Experimental Setup and Values

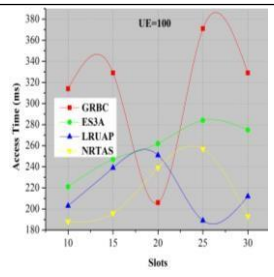
Experimental Setup	Value
Network Region	300m*300m
UEs	150
Requests	10-90/s
Slots	10-30
UE Bandwidth	2Mbps
Max. Resource Allocation Size	500Mb
I	80-240

The experimental results are verified using the metrics access time, response delay, traffic load, success ratio, and overhead. For an effective comparative analysis the existing methods GRBC [20], ES3A [17], and LRUAP [21] are considered in this article. For the metrics access time, traffic load, and success ratio, the density of the UE is varied as 50, 100 and 150 to analyze the performance of the proposed NRTAS.

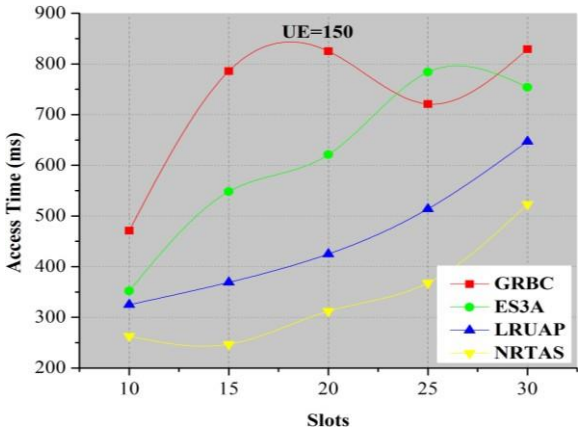
Access Time Assessment



(a) UE=50



(b) UE=100



(c) UE=150

Fig. 4. Access Time Comparisons

The proposed NRTAS achieves less access time to the generated requests from the varying $UE's$. This is achieved due to two prime reasons, the range of [.] is pre-estimated and traffic is classified using A_v. By estimating [.], the chances of $f_r$is computed that helps to retain $t_a \leq [t_r + t_m]$. In particular, the A_v based classification aims at reducing t_a by identifying traffic (as in equation (3)] from the available A_v and ρ_{f_r} feasibility. The change in $[(t_r)]$ is identified by segregating error in equation (3a) and equation (3) to classify traffic. Based on this classification, the range of the traffic (with respect to M to t_r) is defined using equation 8(a). Therefore, the mean access time observed for the classified traffic is comparatively less due to slots allocated and the verified (Refer Fig. 4)

Response Delay Comparison

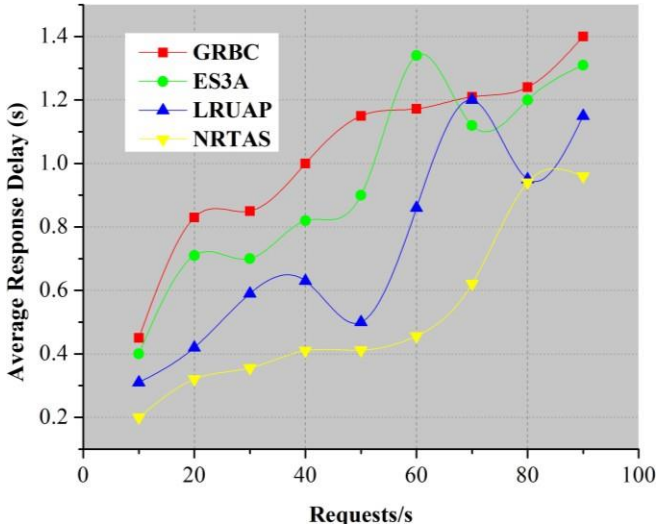


Fig. 5. Avg. Response Delay Analysis

The response delay observed is either $[t_r + t_m]$ or $[t_r + t_a + t_m]$ in the proposed NRTAS. If the traffic is classified, then the response delay is $[t_r + t_m]$, else it is prolonged by a time t_a. The authentication depends on M and t_r to model s_k and K depending on linear and discrete sequence of q_i. The replication of s_k and K where $t_r = m$ is expelled using the matrix analysis as in equation 4(a). Besides, A_v, are analyzed for all that generated traffic (refer equation (3)] to ensure $t_a < [t_r + t_m]$. These constructive features help to reduce the response delay in the proposed NRTAS. This comparison is presented in Fig. 5.

Traffic Load Analysis

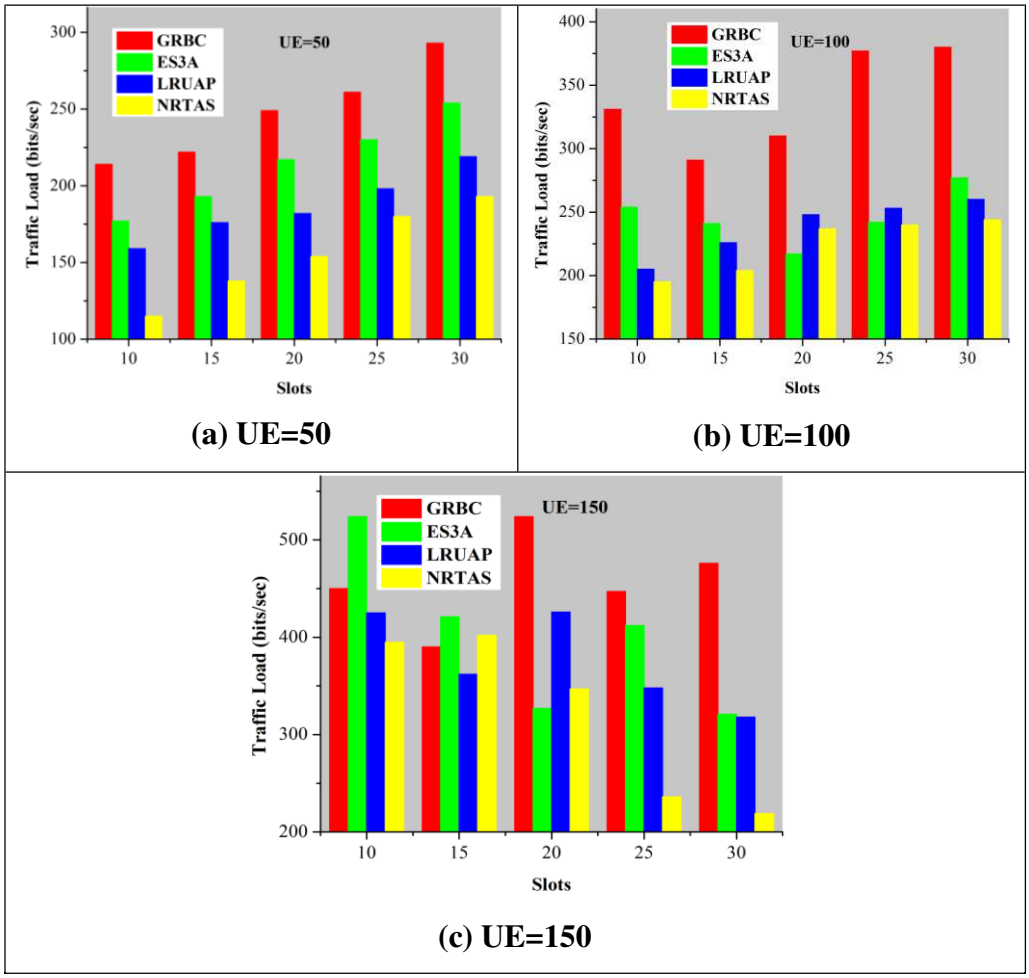


Fig. 6. Traffic Load Analysis

In Fig. 6 the traffic load experienced for the varying UE and slots is presented. The classified traffic in the proposed NRTAS helps to sustain the communication session between the

UEs. For all > 0 and $R(t_r + t_m)$ is true, the traffic load experience in the proposed scheme is less. The error is identified for $t_a = [t_r + t_m]$ and $t_a < [t_r + t_m]$ independently to suppress erroneous traffic across different UEs. This traffic is streamlined by providing appropriate authentication using $s_k$and K. The condition as in equation (1) is achieved by this traffic classification, reducing the rate of traffic.

Success Ratio Comparisons

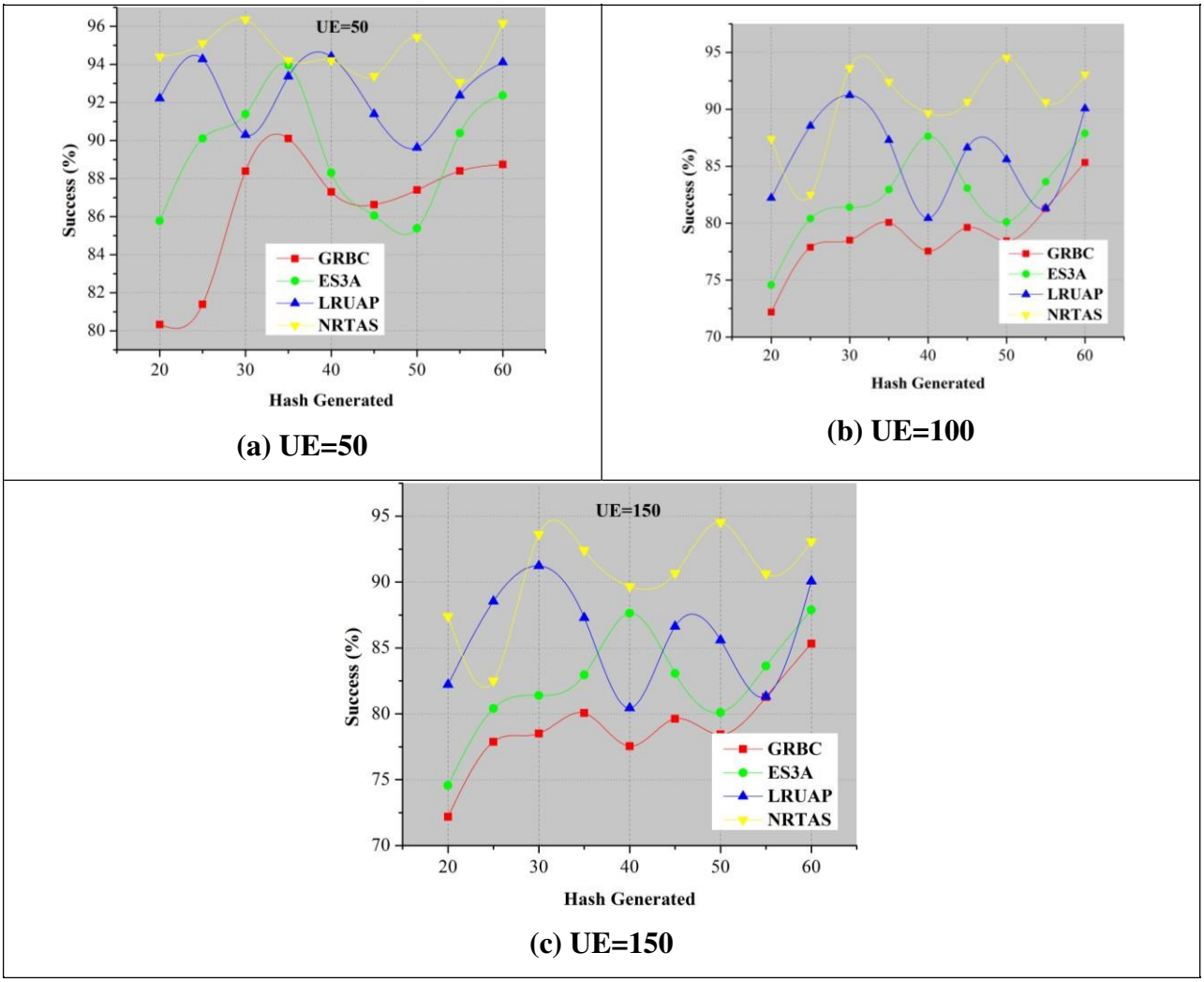


Fig. 7. Success Ratio Analysis

NRTAS achieves better reliability data and message sharing by providing specific authentication for the classified traffic. The authentication is modeled on the basis of M and for a differential K and s_k depending on the sequence of q_i. In a linear authentication, the hash

is generated by mitigating $t_r = m$ instances, preventing redundancy. On the other hand in a discrete authentication, q_s and q_{t_r} are categorized for a new sequence of q_s" to ensure differential s_k and K generation, for the change in M and t_r to reduce unnecessary authentication failure, therefore, irrespective of the change in UE and hashes, authentication is seamless for the $\frac{I}{S}$ intervals for all $[t_r + t_m]$. Due to these factors, the end-to-end security is administered in a optimal manner, improving the success ratio of data sharing (Refer to Fig. 7).

Overhead Assessment

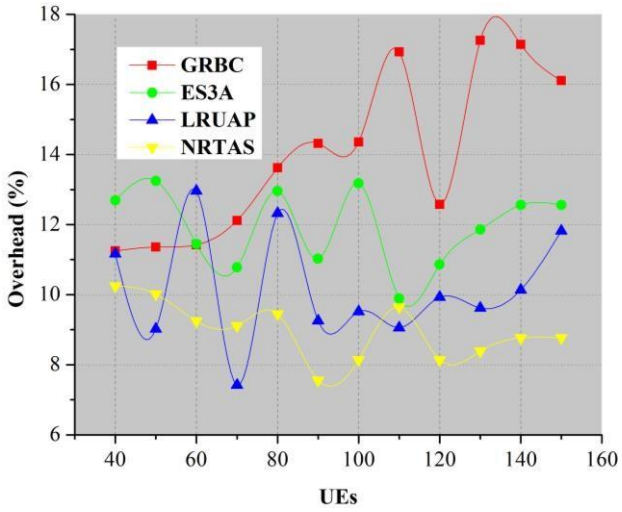


Fig. 8. Overhead Analysis

The overhead in the proposed NRTAS is less by reducing unnecessary authentication for all the generated traffic. The generated traffic is classified for [.] to provide either a linear/discrete authentication. On the other hand, the change in M to t_r or vice-verse is determined on the basis of $\mathbb{P}$, that helps to reduce the additional control message exchange. As mentioned earlier, the success ratio is high; the control message for differential authentication is less reducing the overhead in NRTAS. In Table 2 and 3, the comparative analysis results for the above metrics are presented.

Table 2 Comparison of Access Time, Traffic Load, and Success Ratio for Varying UE

Metrics	UE	GRBC	ES3A	LRUAP	NRTAS
Access	50	196.28	179.49	171.33	160.07
Time	100	329.01	275.44	212.84	193.63
(ms)	150	829.37	754.46	647.19	823.22
Traffic	50	293	254	219	193
Load	100	380	277	260	244

(bits/sec)	150	476	321	318	219
Success	50	88.74	92.37	94.11	96.17
Ratio	100	85.33	87.88	90.07	93.07
(%)	150	75.25	82.32	87.58	90.41

Table 3 Comparison of Avg. Response Delay and Overhead

Metrics	GRBC	ES3A	LRUAP	NRTAS
Avg. Response Delay (s)	1.4	1.31	1.15	0.96
Overhead (%)	16.11	12.56	11.82	8.77

5. Conclusion

This article discusses non-redundant traffic authentication scheme for securing 5G communication and information sharing in a heterogeneous platform. This scheme is modeled into two phases for traffic classification and authentication. The traffic is classified for its error in dissemination and resource sharing so as to provide authentication. The error less classified traffic is analyzed using linear and discrete models for providing replication-free authentication. The authentication is secured using a message and request time based range for improving the reliability of the secret key generation. Using differential secret key and hash, the communication session for the allocated slot is secured. By adapting this authentication model in an agreed manner, end-to-end session authentication for the classified traffic is provided with less overhead and better success ratio.

Funding Statement:

The authors received no specific funding for this study.

Conflicts of Interest:

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. Fortuna, A. Bekan, T. Javornik, G. Cerar, and M. Mohorcic, “Software interfaces for control, optimization and update of 5G machine type communication networks,” *Computer Networks*, vol. 129, pp. 373–383, 2017.

[2] G. Ancans, V. Bobrovs, A. Ancans, and D. Kalibatiene, “Spectrum Considerations for 5G Mobile Communication Systems,” *Procedia Computer Science*, vol. 104, pp. 509–516, 2017.

[3] M. M. Mowla, I. Ahmad, D. Habibi and Q. V. Phung, "A Green Communication Model for 5G Systems," in *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 3, pp. 264-280, Sept. 2017.

[4] L. Yin, Q. Ni and Z. Deng, "A GNSS/5G Integrated Positioning Methodology in D2D Communication Networks," in *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 2, pp. 351-362, Feb. 2018.

[5] G. Dimitrakopoulos, “Sustainable mobility leveraging on 5G mobile communication infrastructures in the context of smart city operations,” *Evolving Systems*, vol. 8, no. 2, pp. 157–166, 2016.

[6] Z. Kotulski, T. W. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, T. Osko, and J.-P.Wary, “Towards constructive approach to end-to-end slice isolation in 5G networks,” *EURASIP Journal on Information Security*, vol. 2018, no. 1, 2018.

[7] Y. D. Beyene, R. Jäntti and K. Ruttik, "Random Access Scheme for Sporadic Users in 5G," in *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1823-1833, March 2017.

[8] Y. Fu, Z. Yan, H. Li, X. L. Xin, and J. Cao, “A secure SDN based multi-RANs architecture for future 5G networks,” *Computers & Security*, vol. 70, pp. 648–662, 2017.

[9] P. Lindgren and K. Wuropulos, “Secure Persuasive Business Models and Business Model Innovation in a World of 5G,” *Wireless Personal Communications*, vol. 96, no. 3, pp. 3569– 3583, May 2017.

[10] P. Magdalinos, S. Barmpounakis, P. Spapis, A. Kaloxylos, G. Kyprianidis, A. Kousaridas, N. Alonistioti, and C. Zhou, “A context extraction and profiling engine for 5G network resource mapping,” *Computer Communications*, vol. 109, pp. 184–201, 2017.

[11] D. Sabella, P. Serrano, G. Stea, A. Virdis, I. Tinnirello, F. Giuliano, D. Garlisi, P. Vlacheas, P. Demestichas, V. Foteinos, N. Bartzoudis, and M. Payaró, “Designing the 5G network infrastructure: a flexible and reconfigurable architecture based on context and content information,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, 2018.

[12] A. Celik, J. Tetzner, K. Sinha, and J. Matta, "5G device-to-device communication security and multipath routing solutions," *Applied Network Science*, vol. 4, no. 1, Aug. 2019.

[13] J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, "Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9794–9805, 2019.

[14] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Communications*, vol. 12, no. 5, pp. 527–532, 2018.

[15] C. T. B. Garrocho, M. J. D. Silva, and R. A. R. Oliveira, "D2D pervasive communication system with out-of-band control autonomous to 5G networks," *Wireless Networks*, 2018.

[16] J. Xu, F. Li, K. Chen, F. Zhou, J. Choi, and J. Shin, "Dynamic Chameleon Authentication Tree for Verifiable Data Streaming in 5G Networks," *IEEE Access*, vol. 5, pp. 26448–26459, 2017.

[17] J. Ni, X. Lin, and X. S. Shen, "Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G-Enabled IoT," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.

[18] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, and W. Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5G networks," *Future Generation Computer Systems*, vol. 100, pp. 893–906, 2019.

[19] J. Cao, P. Yu, M. Ma, and W. Gao, "Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1561–1575, 2019.

[20] J. Guan, Z. Wei, and I.You, "GRBC-based Network Security Functions placement scheme in SDS for 5G security," *Journal of Network and Computer Applications*, vol. 114, pp. 48–56, 2018.

[21] B. Ying and A. Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography," *Journal of Network and Computer Applications*, vol. 131, pp. 66–74, 2019.

[22] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *Journal of Network and Computer Applications*, vol. 122, pp. 50–60, 2018.

[23] Q. Xie and L. Hwang, "Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city," *Neurocomputing*, vol. 347, pp. 131–138, 2019.

[24] S. Yang, D. Yin, X. Song, X. Dong, G. Manogaran, G. Mastorakis, C. X. Mavromoustakis, and J. M. Batalla, "Security situation assessment for massive MIMO systems for 5G communications," *Future Generation Computer Systems*, vol. 98, pp. 25–34, 2019.

[25] A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, and G. M. Pérez, "Towards the autonomous provision of self-protection capabilities in 5G networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 12, pp. 4707–4720, 2018.

Figures

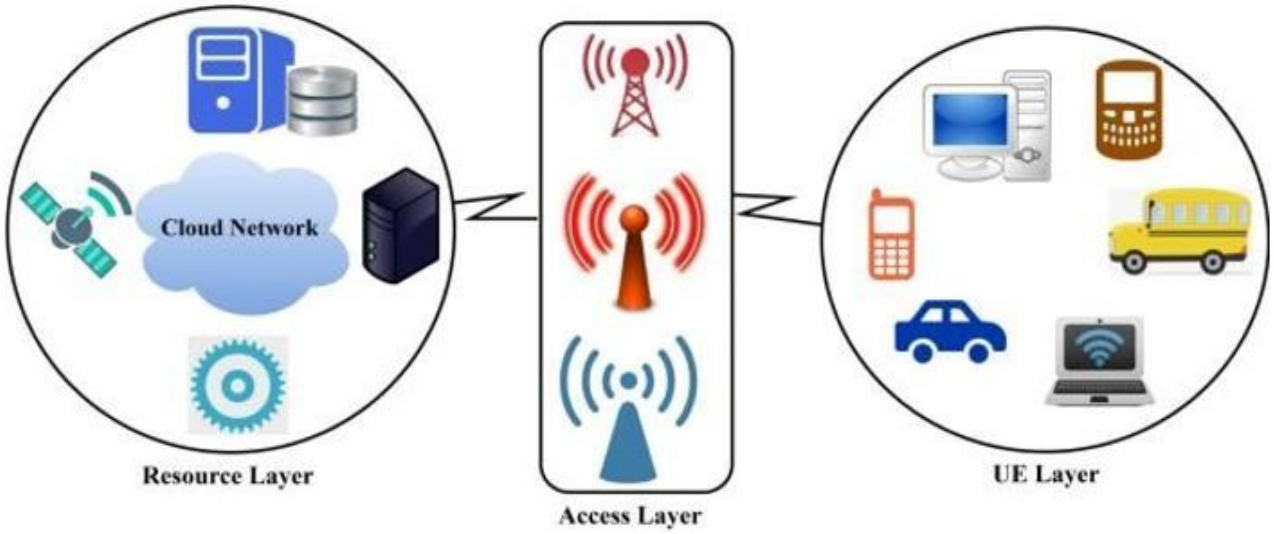


Figure 1

5G communication Illustration

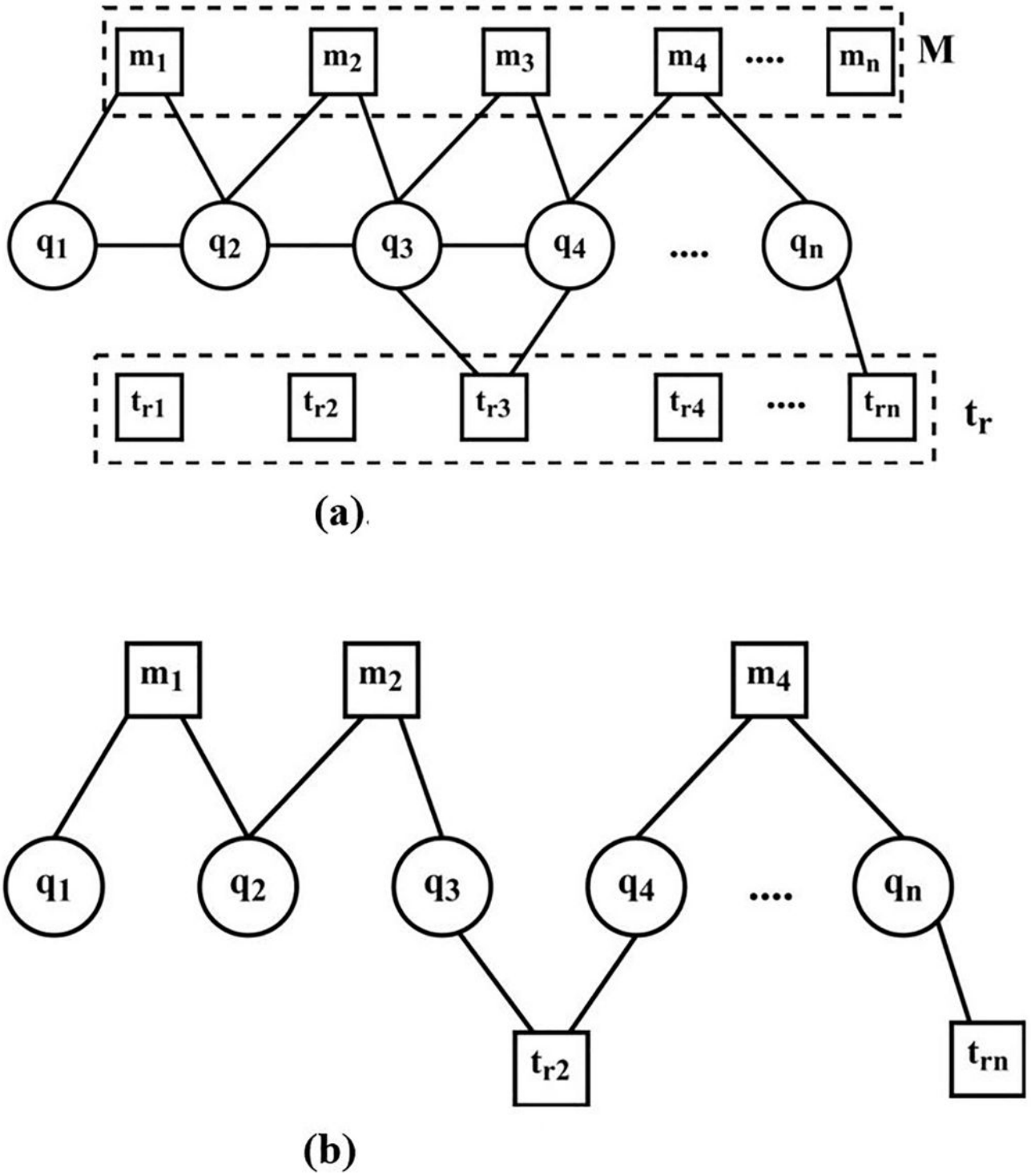


Figure 2

(a). Normal Sequence of ▯▯. (b). Modified Sequence of ▯▯.

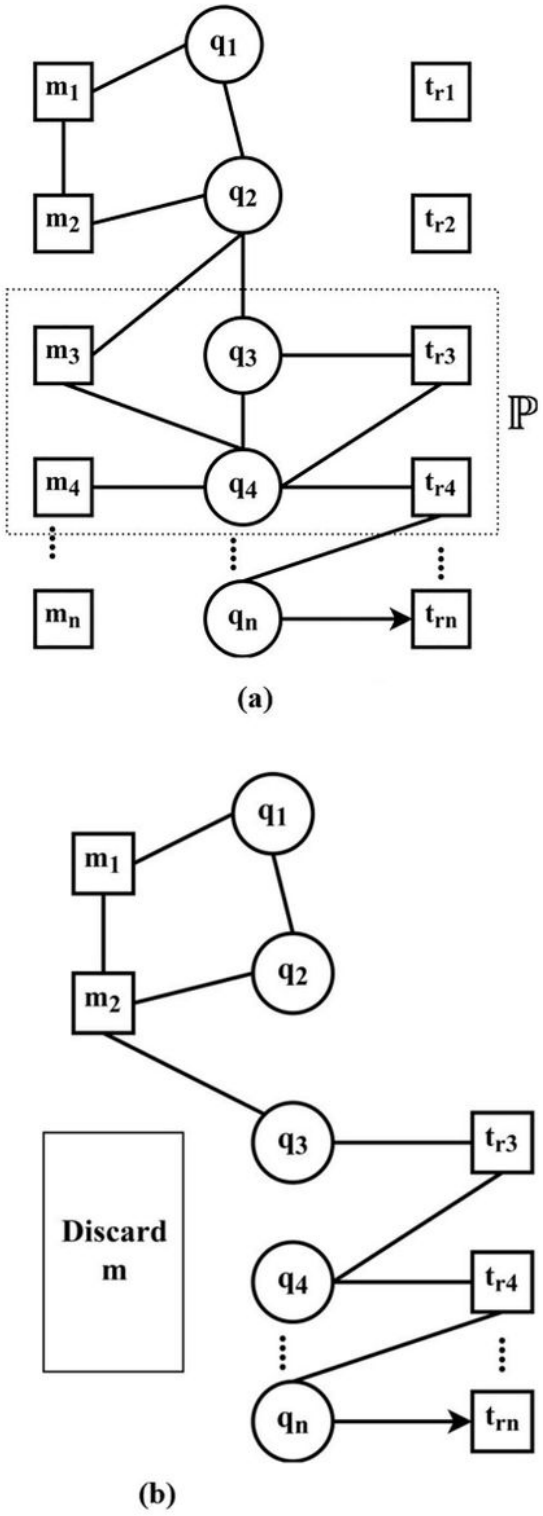


Figure 3

(a). □□ □ □". (b). Modified □□□□□□□ □□ □

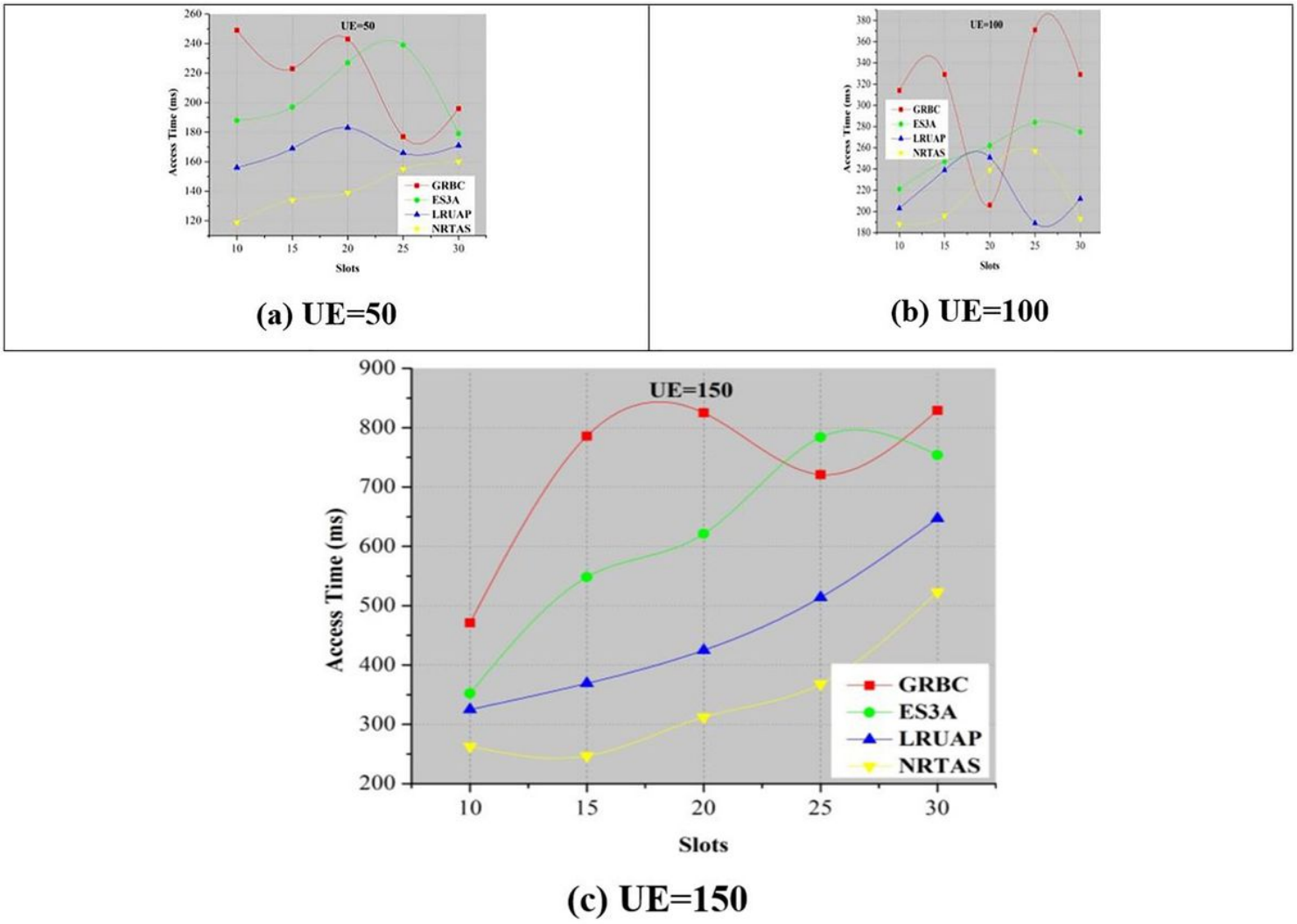


Figure 4

Access Time Comparisons

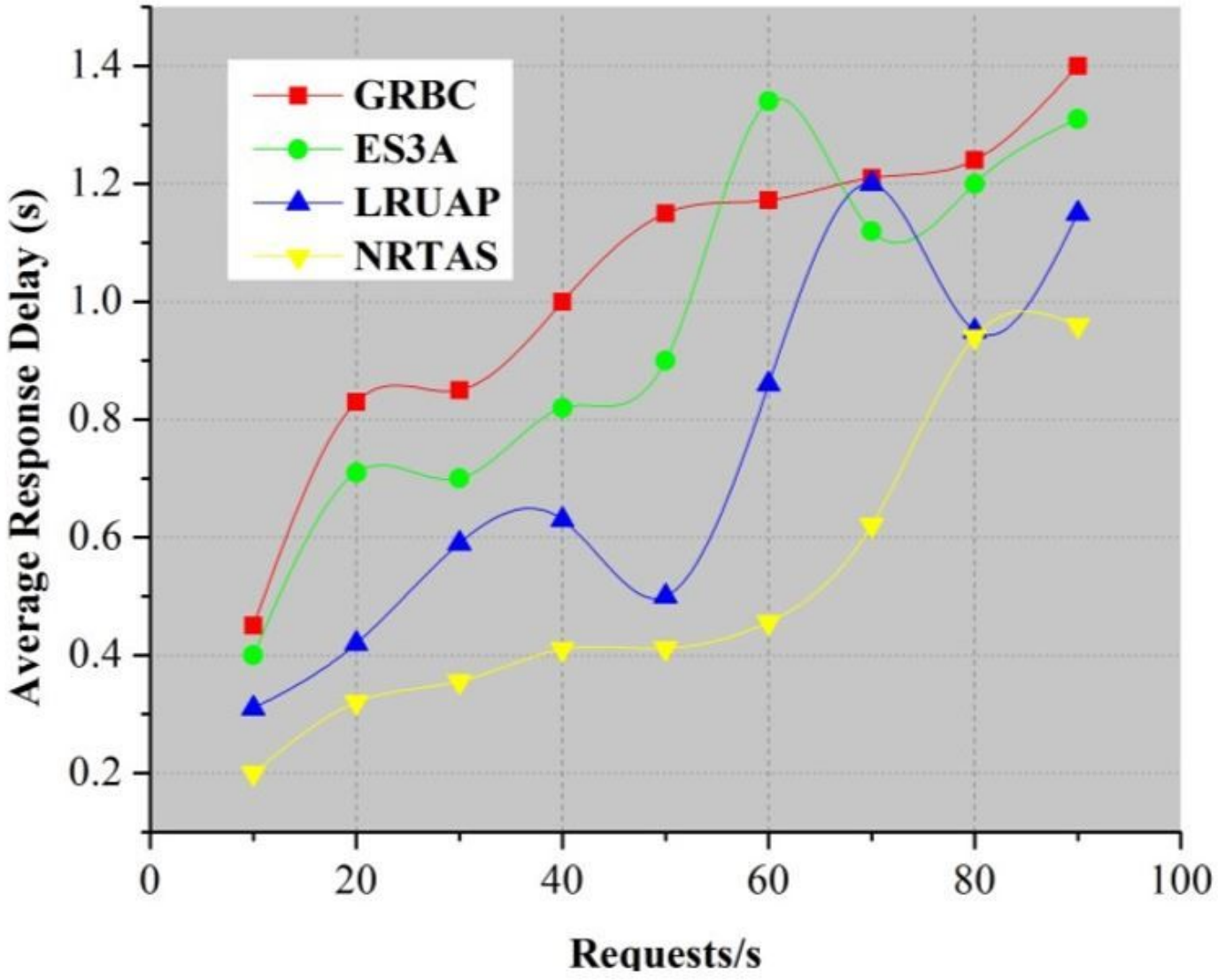


Figure 5

Avg. Response Delay Analysis

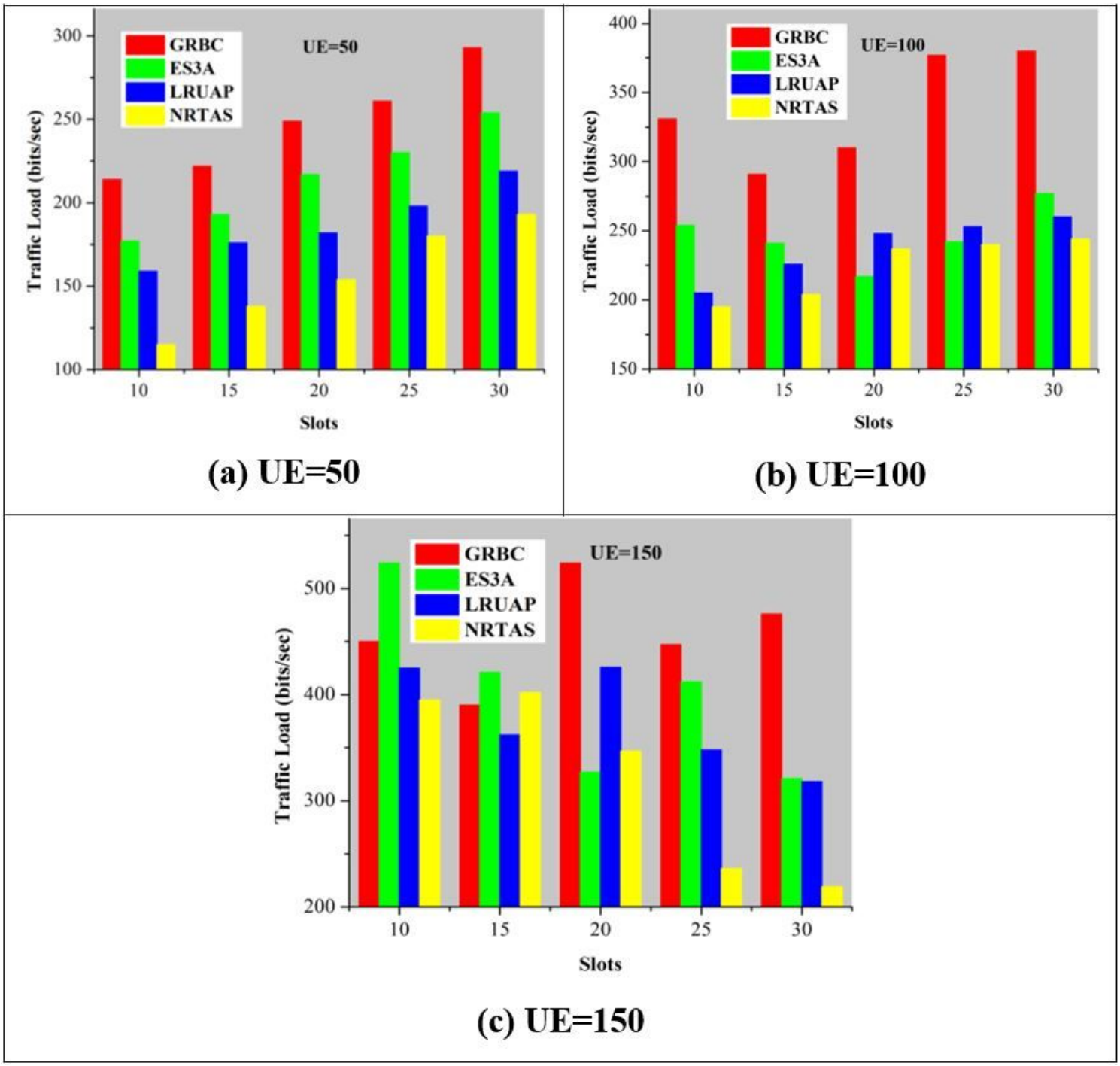


Figure 6

Traffic Load Analysis

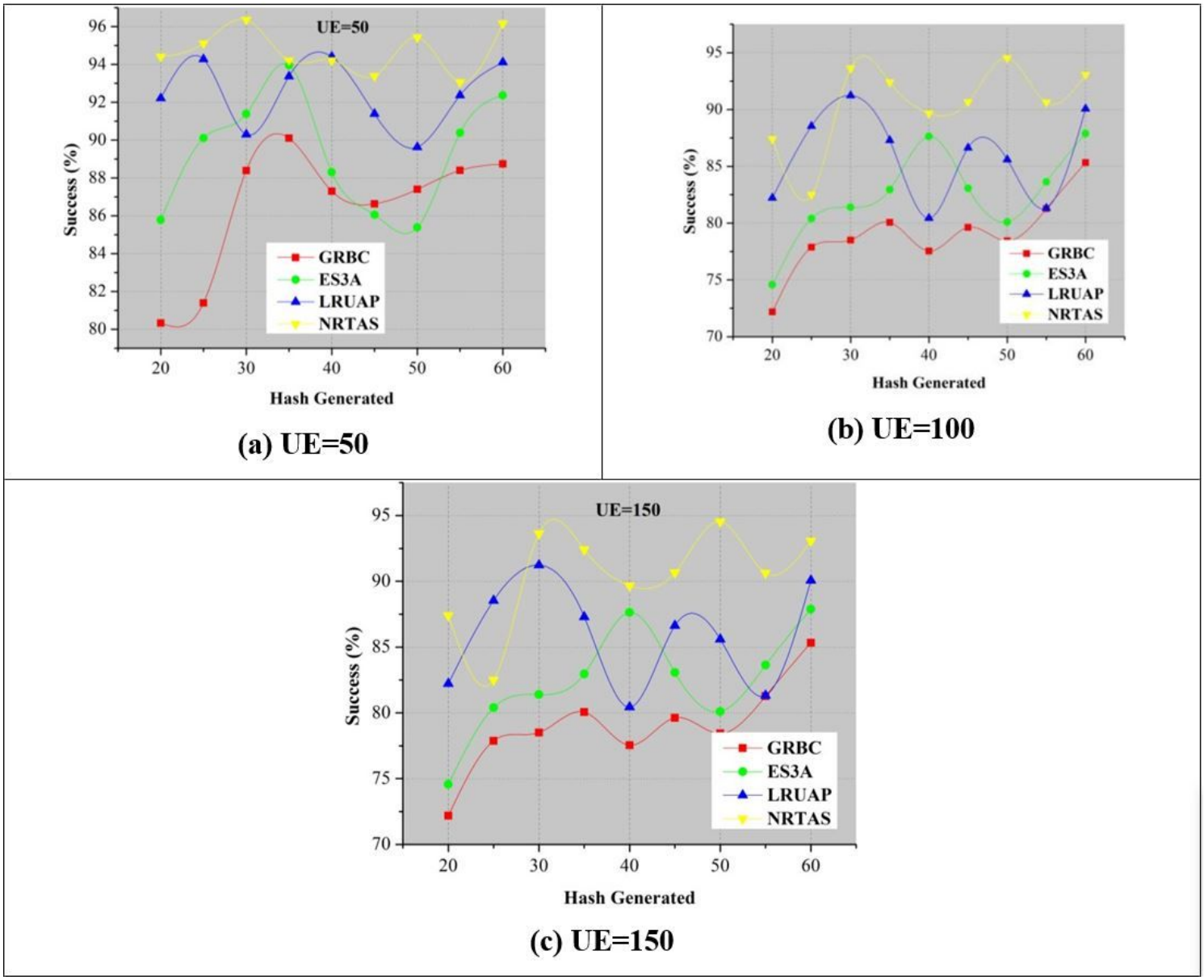


Figure 7

Success Ratio Analysis

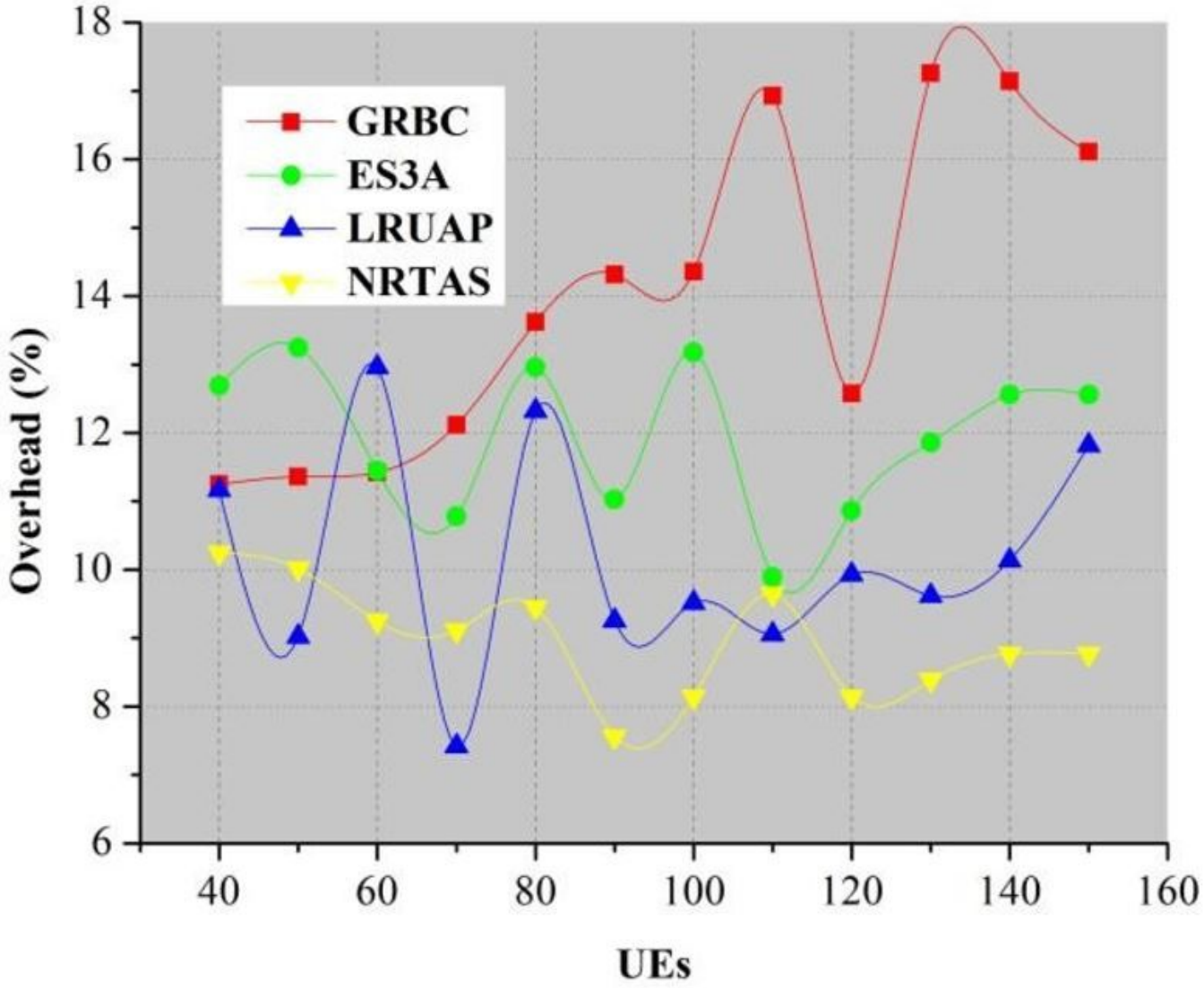


Figure 8

Overhead Analysis