Hindawi
Security and Communication Networks
Volume 2021, Article ID 5589352, 11 pages
https://doi.org/10.1155/2021/5589352

Research Article

Intelligent Media Forensics and Traffic Handling Scheme in 5G Edge Networks

Sa Math,[1] **Prohim Tam**,[1] **and Seokhoon Kim**[1,2]

[1]*Department of Software Convergence, Soonchunhyang University, Asan-si, Chungcheongnam-do 31538, Republic of Korea*
[2]*Department of Computer Software Engineering, Soonchunhyang University, Asan-si, Chungcheongnam-do 31538, Republic of Korea*

Correspondence should be addressed to Seokhoon Kim; seokhoon@sch.ac.kr

Received 21 January 2021; Revised 19 March 2021; Accepted 9 April 2021; Published 21 April 2021

Academic Editor: Jinwei Wang

The 5th generation (5G) communications evolved with heterogeneous user terminals and applications. A convergence of Mobile Edge Computing (MEC) and Software-Defined Networks (SDN) delivers gigantic challenges and opportunities for enhancing computing resources and user Quality of Service (QoS) in fronthaul and backhaul networks. Due to the precipitous expansion of user media in the 5G epoch, efficient media forensics methods are mandatory for specifying and offering effective safety handling based on individual application requirements. According to the exponential increment of Heterogeneous Internet of Things (HetIoT) devices, gigantic traffic will generate through bottleneck 5G fronthaul gateways. 5G fronthaul network environments consist of inadequate resources to surmount the enormous user traffic and communications, QoS will be reduced when the existence of traffic congestion occurs. To confront the aforementioned issues, this paper proposed intelligent media forensics and traffic handling scheme for controlling the Uplink (UL) transmission according to the Downlink (DL) statuses. Support Vector Machine (SVM) algorithm was applied to conduct the media forensics and MEC server integrated into fronthaul gateways, in which gateways resources are divided into UL and DL. Caching technology will be a part of 5G environments, and DL will be utilized for traffic caching. So, it is compulsory to adjust the communication traffic according to UL/DL resource utilization and control the forwarding traffic which relies on resource availability. The experiment was conducted by using computer software, and the proposed scheme illustrated a noteworthy outperformance over the conventional method in terms of diverse significant QoS factors including reliability, latency, and communication throughput.

1. Introduction

The heterogeneous user media will be increasing in the 5th generation (5G) era or next-generation networks (NGN). The caching techniques will be comprehensively applied for enabling local offloading which is enabled by Mobile Edge Computing (MEC). Edge cloud brings advance and significant technologies to the edge network environments, numerous research challenges, and opportunities. Particularly, security methods for edge networks are obligatory to guarantee secure communications of gigantic user applications and media [1]. Heterogeneous user media will be accumulated and cached in edge cloud servers which contain insufficient media inspection to guarantee the trustfulness of dedicated media defense. Next-generation user media will be massive and complicated; therefore, to perform high accuracy media forensics, Machine Learning (ML) will be beneficial for inspecting the distinct innards of the media behaviors [2, 3]. Additionally, real-time communications become Over the Top (OTT) user media in 5G/6G systems. In particular, during the Covid-19 periods, the diverse communications have been accomplishing by the Internet utilization including e-learning, video conference, voice conversation, and other time-sensitive communications [4]. Time-sensitive networks carry huge Packet Data Unit (PDU) sizes, so the big data transmission will have to be handled in the end-to-end (E2E) communications. 5G Radio Access Network (5GRAN) environments are installed by Millimeter-Wave (mm-Wave) technology, and massive Radio Remote Head (RRH) supports Multiple-Input Multiple-

Output (MIMO) technologies [5]. Therefore, 5GRAN will not suffer from resource constraints for handling big data traffic. However, the transmission from fronthaul toward core networks is the bottleneck areas that are installed by optical networks and contained inadequate serving capacity. Fronthaul network environments become significant research domains from a variety of academic and industrials. The network congestion occurs when incoming traffic exceeds the fronthaul capacity [6]. The packet drop ratio will increase when the communication resource is incapable of handling traffic congestion at an appropriate time. Time-sensitive traffic deliveries are based on User Datagram Protocol (UDP), a nonreliable transport protocol, which transmits the user traffic without handshake or acknowledgment (ACK). Therefore, intelligent schemes for handling big data traffic are required to guarantee E2E communications reliability in time-sensitive applications [7].

This paper addresses the intelligent media forensics and real-time traffic handling scheme for improving time-sensitive traffic and user Quality of Service (QoS) in 5G fronthaul networks. The rest of the paper is organized as follows: in Section 2, the related key technologies are illustrated. The proposed intelligent media forensics and traffic handling schemes are presented in Section 3. Section 4 thoroughly presented the results and discussion. Finally, the conclusion is presented in Section 5.

2. 5G Fronthaul Network Environments

ML technologies are under the umbrella of Artificial Intelligence (AI) and bring manifold opportunities for intelligent network systems [8–10]. Moreover, 5G/6G edge architectures evolve with heterogeneous computing platforms including Software-Defined Networks (SDN), MEC, Network Function Virtualization (NFV), AI, and Network Slicing (NS). [11–15]. A convergence of these key technologies overcomes tremendous media drawbacks which generate big data communication in edge networks. ML takes a crucial responsibility in the classification of different applications, while E2E NS is required to differentiate the behaviors of user devices, RRH, network resources, and media contents [16–19]. Different media requires different security and QoS obligations to ensure trustful E2E communication and satisfy the QoS requirement; therefore, the slicing of different media contents (e.g., media forensics) is mandatory [20]. 5G/6G edge environments consist of insufficient computing resources; therefore, the lightweight media inspection methods have to be considered. There exist abundant lightweight ML algorithms including Support Vector Machine (SVM), K-Mean, K-nearest Neighbour (KNN), Decision Tree (DT), and Random Forest (RF) which are appropriate for lightweight MEC devices that have constrained computing capacity. Subsequently, lightweight ML operates in simple computing machines and requires less computing time [21–23]. Moreover, SDN performs an influential position in next-generation 5G/6G fronthaul networks and intends for distributed Management and Orchestration (MNO) between the computing resources and user traffic [24]. SDN enables softwarization to fronthaul networks and supports Application Programming Interface (API), and OpenFlow protocol provides virtual communication interfaces between infrastructure and control layers [25]. 5G edge networks involve microwave links and optical networks (ON) which are suffering from communication QoS. Moreover, the delivery stability is always reported from microwave link applications while ON works well with a variety of environments. Nevertheless, ON environments will bring insufficient link capacity for massive user traffic. To cope with these challenging issues, future mobile networks are targeted to apply Passive Optical Network (PON) which was widely recognized by a variety of research organizations as a promising solution for tackling massive user traffic in bottleneck mobile networks. PON delivers the minimization of traffic congestion and Ultra-Low Latency (ULL) perspectives; additionally, PON connects base stations (BS) toward core gateways. Nevertheless, with the installation between X2 interface without PON, congestion can occur, and the integrated PON with fronthaul networks, UL, and DL resources will increase. Even though PON performs higher capacity for the data delivery, there is still inadequate competence to overcome massive traffic at the peak time from the heterogeneous IoT users. Additionally, the dynamic resource allocation for effective scheduling between PON and ON has to be taken into consideration, since the discrepancy QoS identifications from heterogeneous user traffic are essential constraints [26]. To guarantee time-sensitive communications, traffic classifications have to be performed, while the common communications are comprised of 4 classes including conversation, streaming, interactive, and background [27]. Conversation and streaming traffic are required to ensure ULL for E2E communication and wide bandwidth for rapid delivery. Most of the time-sensitive traffic in the legacy communication systems is less required for critical E2E communication reliability; however, in 5G/6G networks, it consists of numerous real-time applications required to deliver with ULL and Ultra-High Reliability (UHR) including real-time IoT traffic, narrow-band IoT traffic, e-health IoT, Industrial Internet of Things (IIoT), and so forth. The capability of identifying communication criteria and dynamic handling of time-critical applications will be significant for ensuring both QoS and safety communications. Therefore, the conversation and streaming classes are suitable to derive the computing resource from interactive and background, respectively.

Figure 1 shows the convergence of key technologies in next-generation mobile systems and the integration of 5G mobile edge networks with MEC to leverage the network devices for ameliorating computing power. Each network device runs multiple functions to perform different services. The parallel offloading will reduce the computing time of the control plane (CP), and 5G fronthaul environments will be decoupled based on the SDN perspective. The data plane (DP) will be separated from the CP, and both fronthaul DP and CP will be suffering from inadequate resources for massive users. The heterogeneous MEC servers will be located in Radio Access Network (RAN) for leverage RAN computing power and caching purposes. Cloud RAN will be

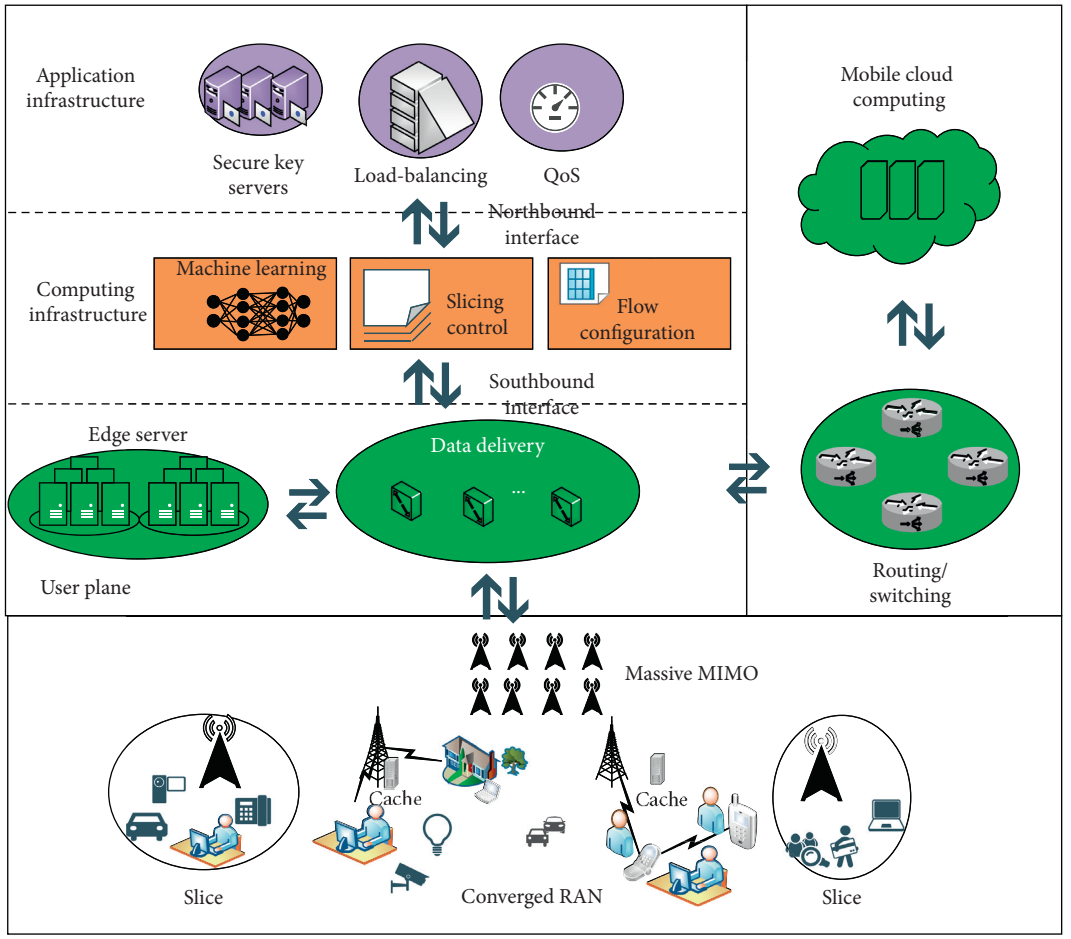

Figure 1: The common convergence of ML with MEC in the future 5G network systems.

enabled by the convergence of heterogeneous MEC platforms, and MEC caching will increase the utilization of the Downlink (DL) resources due to the huge amount of data that will be cached from the remote cloud to a variety of MEC servers in edge areas [28]. The network conditions between the fronthaul gateway and end-user will be not suffering from the bandwidth and computing power for both DL and Uplink (UL). Since fronthaul networks are installed by fiber to the home (FTTH), there are multiple access networking with multiple gateways in the edge areas. While the interfaces between Service Gateway (S-GW) and Packet Data Gateway (P-GW) are the Point-to-Pont (P2P) networks, the sharing resources between UL and DL suffer from insufficient computing power.

3. Proposed Scheme

To overcome the 5G heterogeneous communications and enable both trustfulness and QoS for 5G communication media, this paper proposed a media forensics method based on lightweight ML, namely, SVM, for differentiating the media contents. As shown in Figure 2, the proposed system architecture is comprised of three planes based on SDN perspectives. The user devices request applications from the MEC server via the 5G radio network through multiple RRH gateways. Likewise, the caching technologies have been comprehensively used; therefore, the DP communications will be delivered in the edge network areas. To guarantee E2E QoS and efficient safety traffic handling of the 5G multimedia, the slicing of different contents has to be critically fulfilled. Moreover, the unstructured and diversified media contents are accumulating in the heterogeneous edge cloud environments.

It consists of inadequate safety handling traffic between MEC interfaces and insufficiency of exchanging key certificates for the unclassified media. To cope with these issues, lightweight ML is used to inspect the user media and performs the classification of diverse information categories. The appropriate ML methods that meet the computing capacity of edge environments are required to compute with less memory, lower computing power, and short-term delay computing. The CP is targeted to integrate with the MEC server for boosting the computing power for three main entities including SVM, slicing control, and flow configurations. The SVM provided the data forensics based on the distinct dataset contents. The different slices indicated the different media behaviors and required different levels of security. The paper assumed that the MEC server contains user media with four different classes of various features in terms of the number of harmful attributes, unsecured

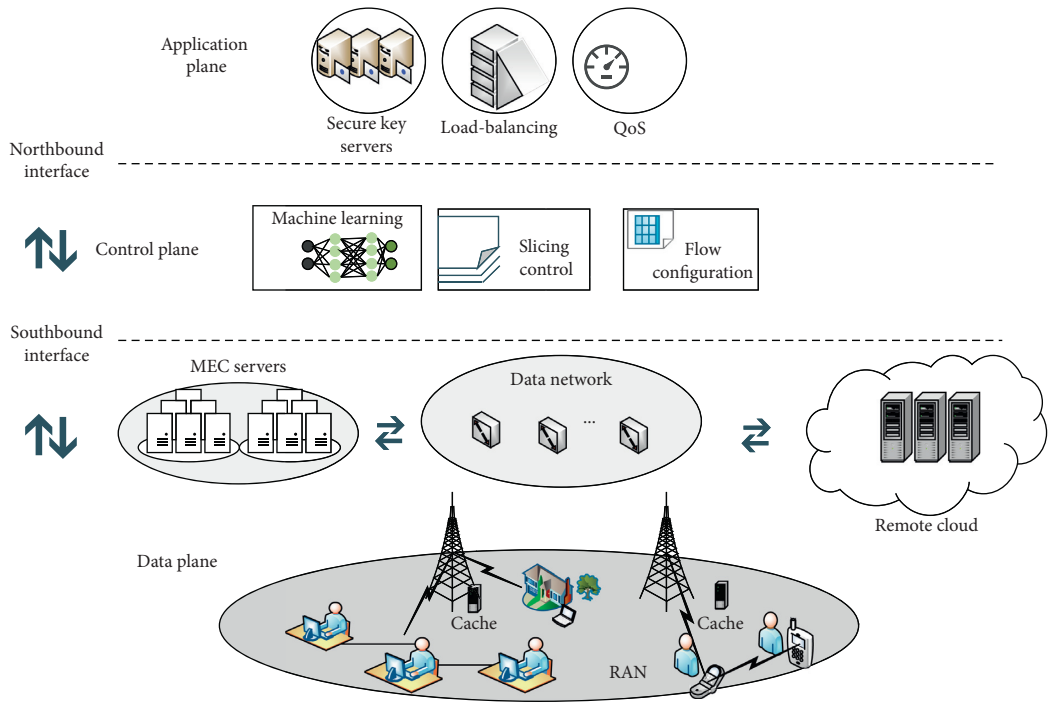

Figure 2: The proposed system architecture is based on a convergence of MEC, SDN, and ML.

sources, unspecific information, and disklike counts. These dataset features indicate the real-world 5G media behaviors and are sufficient to perform protection levels recognition. The application plane (AP) of the SDN controller was proposed to compute distinct slicing modules for reflecting with the CP entities. Each slice of media content can be labeled with a specific security level. So, the scheme performed individual safety control to specific media content.

To perform the media forensics, a convergence of One-Vs-Rest classifier and Radial Basis Function (RFB) kernel is used to define the class prediction probability of any input content traffic flows, $X' = \{x_1, x_2, x_3, \ldots, x_n\}$. For a calculated median value of class targets, $Y' = \{y_1, y_2, y_3, \ldots, y_m\}$, where each class y_m is represented as m-level of restrictions. To predict the probability in which each content flow x_n belongs to class m, the distant outcome between x_n and y_m is calculated, as described in Figure 3. $h_\theta^{(m)}(X')$ represents the One-vs-Rest classifier output estimation of content flows, partly based on RFB kernel calculation. The estimated maximum value of content flows toward m-level classes, $\max_m h_\theta^{(m)}(X')$, is the output decision.

Figure 4 illustrates the procedure flows of constructing Support Vector Classification (SVC) toward the final prediction on unseen real-time media content traffic flows.

Starting from raw data collection, the algorithm takes data processing into consideration and implementation. The training data has to be cleansed, normalized, and extracted useful features before inputting to SVM. To train the model, the training dataset is driven to supervise the algorithm. And each target class is required to define correctly. For model precision testing purposes, the overall input data split into constant randomized subsets (70% for training and 30% for testing). Next, the One-vs-Rest classifier is applied to fit each class against all the remaining classes. Then, RFB specifies the kernel types to be applied in the algorithm. After the model is constructed, the training data subset inputs to fit with the SVM for calculating the precision score estimation on testing data subset. If the score is satisfied, the implementation of real-time media content traffic flows is entered. However, if the score is unsatisfied, the SVC procedures are required to be synchronously remodified to improve the performance. Eventually, the media content flows are expected to be well-classified for assuring the level of accessibility conditions, securing the public distribution of harmful content classes, and authorizing the restricted content configuration.

To proceed with multiclassification, the input dataset has to be well-processed, cleansed, and well-defined target classes. Table 1 brainstorms the class names and characteristics based on the level of media restrictions which is possibly triggered by the SVM classifier process. Class 0 represents the group of contents that contain intense adult categories including violence, sexual scenes, mature subjects, inappropriate language, and drugs. In case of any content traffic flows belonging to Class 0, the accessibility conditions are obliged to be strictly defined and securely configured.

For Class 1 and Class 2, the content feature has respectively lower public impacts than Class 0 in terms of fewer dislikes, reports, or harmful comment detection. Exceptionally, Class 3 is defined as the inoffensive or harmless contents which possibly opens for free access in public.

Due to simultaneous user requests toward the MEC servers, there is inadequate resource capacity between user device to RRH interfaces, RRH to RRH/X2 interfaces, and the RRH to SGW. Subsequently, MEC servers will be

Require: Let $X' = \{x_1, x_2, x_3, ..., x_n\}$ denote number n of each content flow value and $Y' = \{y_1, y_2, y_3, ..., y_m\}$ value of *m-level* target classes

(1) Initialize classifier $h_\theta^{(m)}(X')$;

Apply RFB kernel of $(X', Y') = e^{(-(||X'-Y'||^2/2\sigma^2))}$ wiht free parameter σ;

(2) Use One-vs-Rest to predict probability of x_n belonging to class m

$$h_\theta^{(m)}(x_n) = P(y_m = m \mid x_n; \theta)$$

(3) Output decision: $\max_m h_\theta^{(m)}(X')$;

Figure 3: The algorithm flows of SVM.

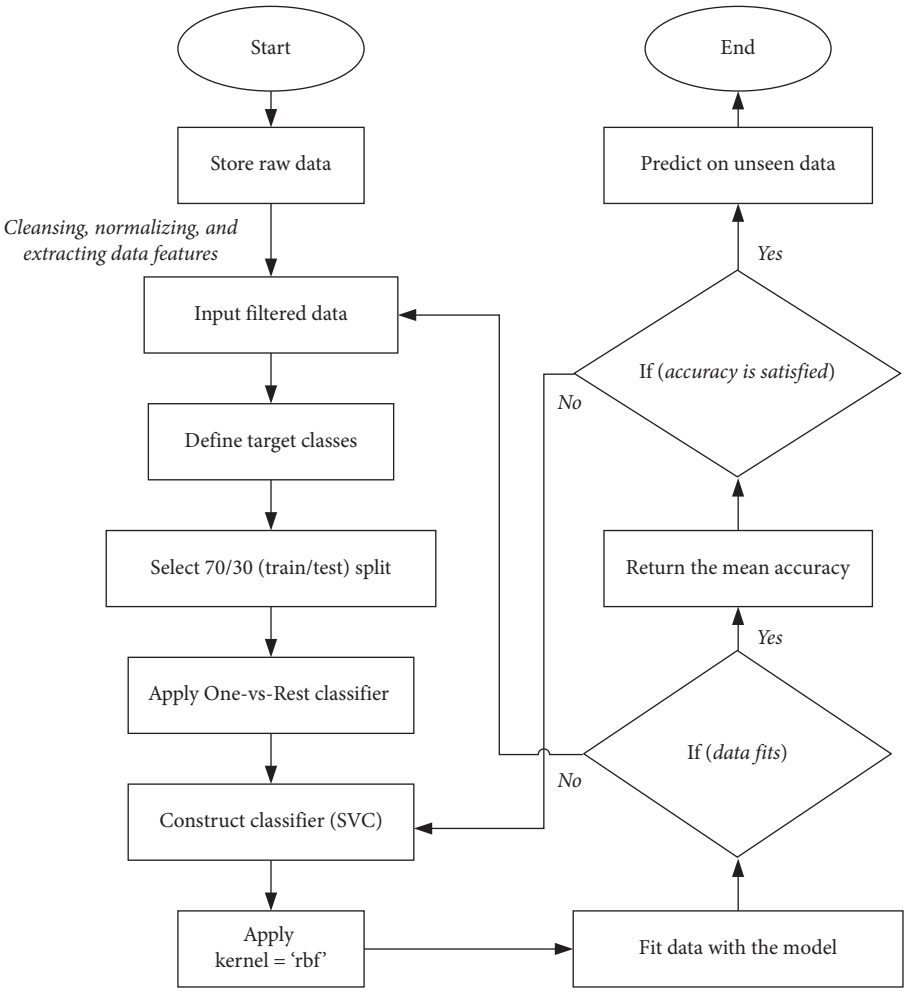

Figure 4: The data forensics diagrams are based on SVM ML.

connected to the SGW for content delivery and download the up-to-date information from the MCC while the caching traffic from MCC is mostly the interactive and background communication types completely manageable by the software-based network. The controller is required to monitor both SGW statuses and link bandwidth. The SGW handles both DL and UL end-users and caching traffic from the remote cloud. At the peak time in 5G network environments, the controller will check the content requests in the MEC server, and if the contents are not presented, the

Table 1: Media contents of target classes.

Class	Characteristics
Class 0	High prohibition and strict accessibility conditions
Class 1	Fair prohibition and restriction
Class 2	Less restriction and discouragement for sharing
Class 3	Open accessibility for public distribution

controller will update the forwarding flow of a specific request to the MCC server. Additionally, the MEC will be required to cache and update the missing contents from the external clouds. During the peak time, both DL and UL will carry tremendous user information; thus, the congestion will occur when the computing power reaches the limit threshold. To handle the congestion issues, the splitting and monitoring of DL and UL are obliged to be fulfilled. In real-world 5G communications, there will be a convergence of heterogeneous applications including time-sensitive and time-insensitive traffic. Thus, the capability of identifying distinct communication types will be essential for efficient QoS management. The proposed scheme handles the congestion based on the restriction on the caching traffic in DL. Whenever the UL situations are necessitated to be handled, the controller will be required to evaluate the resource restriction of DL based on the obvious traffic types. The DL resources will be utilized for carrying caching traffic and time-insensitive applications; thus, the restriction of DL will boost UL resources and will be efficient for handling real-time communications.

4. System Analysis

4.1. E2E System Latency. The E2E latency of packet transmission in the proposed system can be written as T which is the addition of multiple delay occurrences as follows:

$$T = T_{\text{Radio}} + T_{\text{Fronthaul}} + T_{\text{EPC}} + T_{\text{MNO}}, \tag{1}$$

where

(i) T_{Radio} is the broadcasting radio delay that occurs between the user devices and RRH interfaces. The massive MIMO technologies required the optimal methods for efficient scheduling in MIMO techniques since the latency can be increasing according to the insufficient handling of RRH.

(ii) $T_{\text{Fronthaul}}$ is the packet transmission delay which occurred at the interval of gNB SGW/PGW. The common SGW/PGW transmission mediums are installed by optical network environments. The communication latency can occur at a variety of interfaces including S1, X2, and both CP and DP.

(iii) T_{EPC} is the computing period that occurs at the control and data planes of the SGW/PGW gateways. The Evolved Packet Core (EPC) system is located in the control plane and it consists of several occurrence delays in various EPC entities, such as the SDN controller, Home Subscriber Server (HSS), Mobile Management Entity (MME), and Policy and Charging Rule Function (PCRF). EPC entities tackle the communication registration and resource management of the mobile systems.

(iv) T_{MNO} is the delay of MNO that occurs at the SDN controller. SDN manages each slice of the media forensic and caching synchronization of the DL and UL statuses. The delay can be occurring with the computation processes of ML algorithms and communication flows update based on the ML output.

The conditions of the UL depend on the serving of each gateway and the network device from the heterogeneous network can be defined as the M/M/1 queue model as follows:

$$\varrho = \frac{\lambda}{\mu}, \tag{2}$$

where ϱ expresses the serving ratio or threshold of the serving entities, λ denotes the incoming rate of user traffic, and μ corresponds to the serving rate of the gateway or any base stations. The statuses of DL and UL can be measured by determining the ϱ values. Ordinarily, if the incoming request λ exceeds the serving capacity μ, the system is compulsory to be manipulated.

4.2. Simulation Environment. The simulation system comprised of two different scenarios including the data forensics for 5G media based on the SVM ML algorithm and QoS handling for distinct traffic slices, as shown in Figure 5. The dataset was generated by using Python programming to reflect four classes of media as shown in Table 1. SVM was applied to scrutinize the dataset which encompasses diverse media manners. After scrutinization by SVM, four classes of media forensics with distinct manners are performed. The discrete network simulation version 3 (NS3) was utilized to conduct real-time experimentation. The simulation time (SimTime) was set to 450 seconds, and 6,611,130 traffic was generated for normal and bad conditions. And the Random Early Detection (RED) queue was integrated into the SGW/PGW gateway for buffering and QoS evaluation purposes.

5. Results and Discussion

The exhaustive dialogue of experimented outcomes is presented in this section. The evaluated results are comprised of two categories including media forensics analysis and QoS exposures of real-time user communication for each forensics classification. Figure 6 illustrates the slice of four media content groups. Each group indicated the different media innards as depicted in Table 1. SVM performed 99% accuracy of predictions and classifications of 12,500 elements into four distinctions from the media dataset. According to output, there exist 3,747 (29.976%), 4,030 (32.24%), 2,945 (23.56%), and 1,778 (14.224%) contents belonging to Class 0 (high prohibition and strict accessibility conditions), Class 1 (fair prohibition and restriction), Class 2 (less restriction and discouragement for sharing), and Class

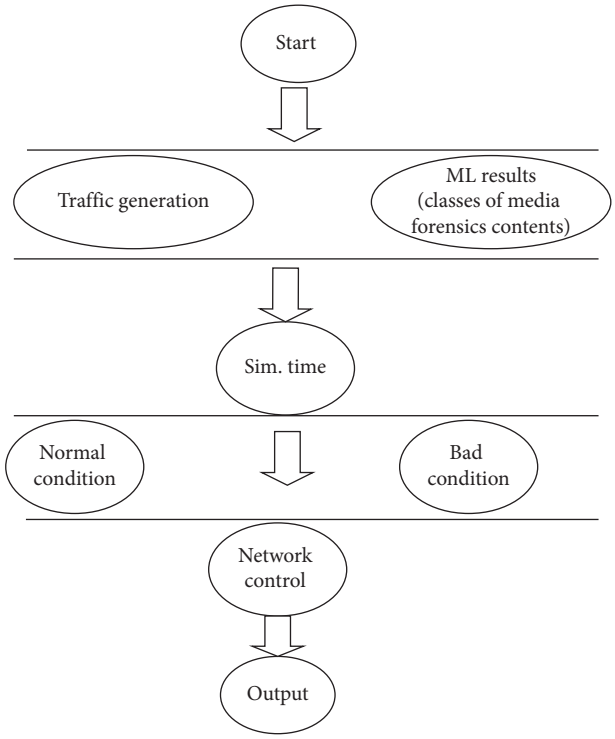

Figure 5: The simulation diagrams for the proposed system.

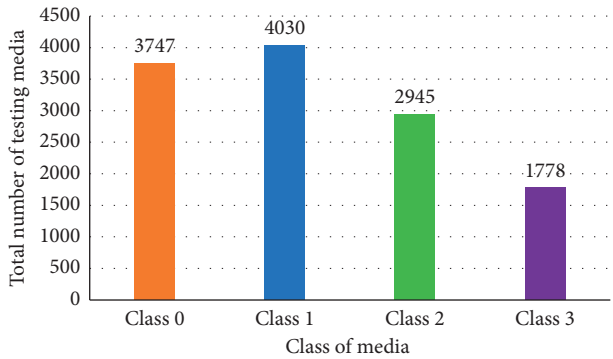

Figure 6: The scrutiny classes of 12,500 media datasets performed by SVM.

3 (open accessibility for public distribution), respectively. Each class indicated the different levels of harmful contents and conceivably alluded to the distinct levels of security compulsory.

Due to the slicing of distinct media contents, the distinct slices are conceivable to allocate and manipulate in the divergent containers. The detachability of distinct media contents dispenses a diverse opportunity for virtual computing environments since each detached group is competent to compute in an independent virtual machine or container that brings convenience and efficient MNO. Correspondingly, network slicing between the user and the MEC applications will be established, and multiple MEC servers will be utilized by individual operations while each MEC server has a unique interface connection to SGW/PGW. The paralleled offloading of multiple MEC servers will be established and the flexible handling of each communication interface will be obligatory.

Afterward, the E2E user traffic will be transpired by individual communication media. Thus, the simultaneous communications of multiple interfaces for both UL and DL mandatorily handle based on different traffic QoS Class Identifier (QCI). The proposed scheme ameliorates the real-time communications reliability and further QoS parameters by equilibrating the UL and DL based on the behaviors of the transmitting traffic. In 5G edge network environments, MEC will be real-time synchronous for identifying the up-to-date contents for caching. Likewise, the caching processes are elicited from the centralized discipline of the SDN controller; and the caching processes are completely manageable. Figure 7 illustrates that the proposed scheme remarkably outperforms the conventional scheme in terms of E2E communications reliability. Alluding to the graphs, the proposed scheme reached 99.98% while the conventional scheme had 99.95% of the E2E communication reliability. The increment of E2E reliability in real-time traffic transmission provides essential contributions to diverse time-sensitive applications. For next-generation network environments, real-time applications are rapidly increasing, especially, real-time IoT networks that have insufficient capacity for Transmission Control Protocol (TCP). Therefore, the majority of IoT applications are running over unreliable transmission methods called User Datagram Protocol (UDP). Ultra-High Reliability (UHR) is obligatory for diverse IoT applications, such as Industrial Internet of Things (IIoT), Internet of Medical (IoM), and safety system, and these applications required both ULL and UHR for E2E communications. To fulfill the mentioned requirements, the proposed scheme is felicitous to ameliorate the QoS of time-sensitive networks. In correspondence to the communication reliability, the total packet drop counts during the transmission are 1,201 while the conventional scheme has 3,010 packets drop counts.

Analogous to the E2E communication reliability, Figure 8 demonstrates the comparison of packet drop ratio between the proposed and conventional schemes. The graphs showed that the proposed scheme has the lowest packet drop ratio in distinction to the conventional scheme. The minimum packet drop ratio of proposed and conventional schemes are 0.018% and 0.045%, respectively. Regarding the drop ratio, the proposed scheme completely outperforms the conventional scheme, felicitous to ameliorate communication trustworthiness for adequate UHR. The augmentation of the user QoS conceivably contributed by restricting the time-insensitive traffic in the DL. Consequently, the UL computing capacity is conceivably enhanced by limiting the DL resources. The E2E communication reliability is one of the crucial QoS keys in real-time communication that guarantees the transmitted packet reaching the receiver without losing information. Furthermore, the stability of communication systems is a critical issue to be obliged and considered for strengthening the QoS. Figure 9 demonstrates the communication jitter comparisons between proposed and conventional schemes. Regarding the given graphs, the proposed scheme has lower

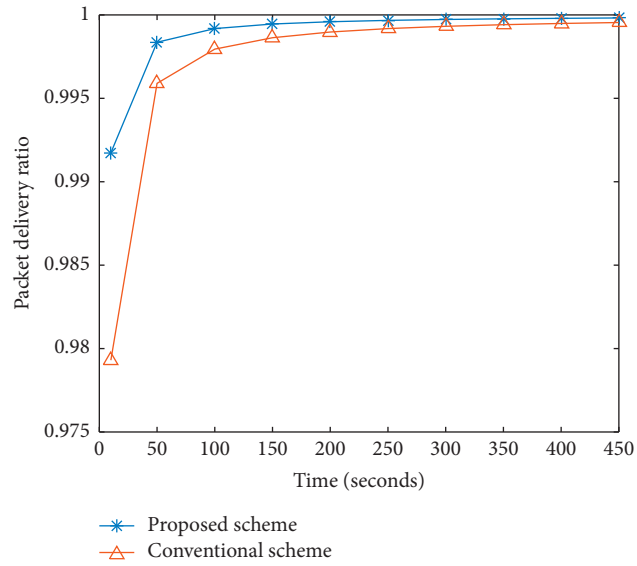

Figure 7: The comparison of E2E communication reliability between proposed and conventional schemes.

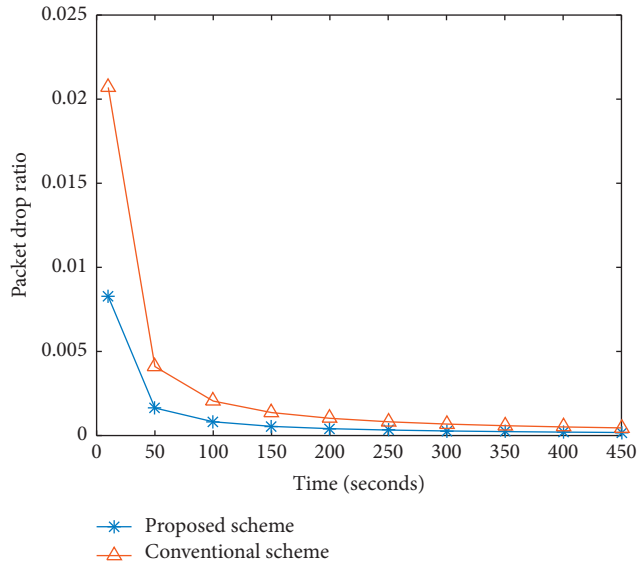

Figure 8: The packet drops ratio comparison between the proposed and conventional schemes.

jitter values while the conventional approach has the highest communication jitter. The lowest jitter value indicates that communication has higher steadiness. The proposed scheme provides the ultra-low jitter that enables efficient real-time communications. The average jitter values of the proposed and conventional schemes are 0.306 and 0.323 milliseconds, respectively. In the heterogeneous and massive communication networks, big data transmission will be occurring during peak time communications. In the bottleneck or insufficient areas, the transmission will not offer a steady handling system to users, so the fluctuation of serving times simultaneously increases the communication jitters. Consequently, the QoS/QoE will be reduced depending on the arising jitter fluctuations. To cope with these issues, the proposed scheme is applicable for improving QoS in massive edge network environments.

Figure 10 illustrates the average E2E communication delays of the proposed and conventional schemes. The graphs show that the proposed scheme outperformed the conventional scheme regarding E2E delays. The next-generation edge networks will have to handle tremendous user applications and traffic. Consequently, the bottleneck areas can occur whenever the request exceeds the serving capacity of network devices. Hence, the request forces to wait for valid resources from serving entities, and the waiting of user traffic will increase the E2E communication delay that lessens the QoS/QoE of the system. Real-time applications are critical time constraint which required less Round-Trip

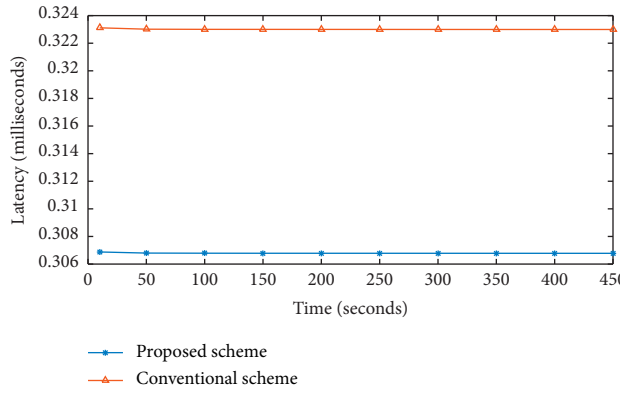

Figure 9: The communication jitters comparison between the proposed and conventional schemes.

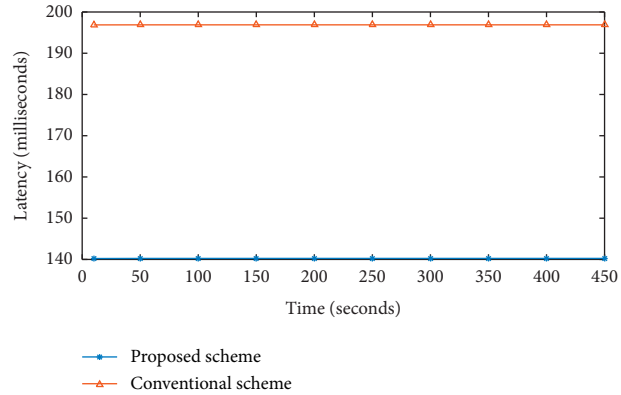

Figure 10: The communication delays comparison between the proposed and conventional schemes.

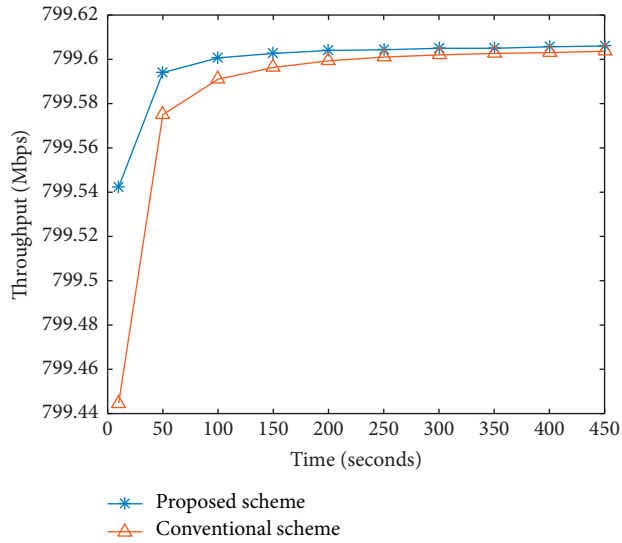

Figure 11: The communication throughput comparison between proposed and conventional schemes.

Time (RTT) for E2E communications. The graphs show the average delay of the system in poor conditions. The proposed scheme has an average communication delay of up to 140.24 milliseconds while the average delay of the conventional approach is 196.88 milliseconds.

Due to the E2E communication delays being reduced by the proposed scheme, the capacity of forwarding traffic simultaneously increased. Figure 11 demonstrates the comparison between the proposed and conventional schemes in which the proposed scheme has higher communication

throughputs than the conventional scheme, and the average throughputs of proposed and conventional schemes are 799.596 Mbps and 799.581 Mbps, respectively. Communication throughput relies on transmission delays, and since the proposed scheme has lower RRT than the conventional scheme, the proposed scheme provides more effective handling for massive traffic in the bottleneck network environments. Based on the graphs of the proposed scheme, numerous traffic can be forwarding rapidly; hence, the amount of traffic in the queue can be rapidly reduced simultaneously.

6. Conclusions

To guarantee safe media accessibility and capability of executive QoS for a particular user data exchange, the prerequisite of differentiating the media manners is necessitated to fulfill. This paper presented the efficient data slicing based on lightweight ML for 5G/6G media forensics perspectives. Furthermore, the efficient QoS handling of each forensics class has been presented. The scheme ameliorated the communication QoS by solving the congestion issues in the bottleneck of edge network environments. The resource utilization adjustment of the SGW/PGW between DL and UL is critical for ensuring E2E communication reliability. In particular, in the big data transmission environments, intelligent methods can accomplish that individual user requirements are essential. The proposed scheme provided the reference method for media forensics by scrutinizing the user data into distinct classes which relied on the existing media behaviors. Nevertheless, the dynamic security algorithms ought to be applied to augment safety user traffic for diverse confidential media innards. Regarding the conducted tests, SVM performed satisfied learning accuracy that feasibly applies to future media forensics aspects. Afterward, the capability of handling each user traffic slice remarkably outperforms the conventional approach in respect of communication reliability, jitter, delay, and throughput. The proposed scheme is appropriate to cope with the challenging issues in 5G bottleneck environments. To ameliorate both E2E communication QoS/QoE and security aspects, a deep neural network will be applied for deep media innards inspection in the forthcoming research.

Data Availability

The data used to support the finding are included in this paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was funded by BK21 FOUR (Fostering Outstanding Universities for Research) (no. 5199990914048), and this research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2020R1I1A3066543). In addition, this work was supported by the Soonchunhyang University Research Fund.

References

[1] A. Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in fog-to-things communications," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 124–130, 2018.

[2] S. Rathore, J. H. Ryu, P. K. Sharma, and J. H. Park, "DeepCachNet: a proactive caching framework based on deep learning in cellular networks," *IEEE Network*, vol. 33, no. 3, pp. 130–138, 2019.

[3] L. Verdoliva, "Media forensics and DeepFakes: an overview," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910–932, 2020.

[4] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[5] A. S. Mubarak, H. Esmaiel, and E. M. Mohamed, "LTE/Wi-Fi/mmWave RAN-level interworking using 2C/U plane splitting for future 5G networks," *IEEE Access*, vol. 6, pp. 53473–53488, 2018.

[6] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[7] J. Li and Z. Pan, "Network traffic classification based on deep learning," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 11, pp. 4246–4267, 2020.

[8] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[9] X. Wang, Y. Han, V. C. M. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of edge computing and deep learning: a comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 869–904, 2020.

[10] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for Internet of Things (IoT) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[11] M. Saleem and Y. Saleem, "High quality network and device aware multimedia content delivery for mobile cloud," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 10, pp. 4886–4907, 2019.

[12] E. Kim and S. Kim, "An efficient software defined data transmission scheme based on mobile edge computing for the massive IoT environment," *KSII Transactions on Internet and Information Systems*, vol. 12, no. 2, pp. 974–987, 2018.

[13] D. Kim and S. Kim, "Gateway channel hopping to improve transmission efficiency in long-range IoT networks," *KSII Transactions on Internet and Information Systems*, vol. 13, no. 3, pp. 1599–1610, 2019.

[14] M. Mehrabi, D. You, V. Latzko, H. Salah, M. Reisslein, and F. H. P. Fitzek, "Device-enhanced MEC: multi-access edge computing (MEC) aided by end device computation and caching: a survey," *IEEE Access*, vol. 7, pp. 166079–166108, 2019.

[15] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, and M. Conti, "A survey on the security of stateful SDN data planes," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1701–1725, 2017.

[16] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: a survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[17] C. Song, M. Zhang, Y. Zhan et al., "Hierarchical edge cloud enabling network slicing for 5G optical fronthaul," *Journal of Optical Communications and Networking*, vol. 11, no. 4, pp. B60–B70, 2019.

[18] L. Lei, Y. Tan, K. Zheng, S. Liu, K. Zhang, and X. Shen, "Deep reinforcement learning for autonomous Internet of Things: model, applications and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1722–1760, 2020.

[19] N. Jia, S. Fu, and M. Xu, "Privacy-preserving blockchain-based nonlinear SVM classifier training for social networks," *Security and Communication Networks*, vol. 2020, Article ID 8872853, 10 pages, 2020.

[20] N. Slamnik-Kriještorac, H. Kremo, M. Ruffini, and J. M. Marquez-Barja, "Sharing distributed and heterogeneous resources toward end-to-end 5G networks: a comprehensive survey and a taxonomy," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1592–1628, 2020.

[21] M. Wang, Y. Cui, X. Wang, S. Xiao, and J. Jiang, "Machine learning for networking: workflow, advances and opportunities," *IEEE Network*, vol. 32, no. 2, pp. 92–99, 2018.

[22] S. Math, L. Zhang, S. Kim, and I. Ryoo, "An intelligent real-time traffic control based on mobile edge computing for individual private environment," *Security and Communication Networks*, vol. 2020, Article ID 8881640, 11 pages, 2020.

[23] S. Math, P. Tam, A. Lee, and S. Kim, "A NB-IoT data transmission scheme based on dynamic resource sharing of MEC for effective convergence computing," *Personal and Ubiquitous Computing*, 2020.

[24] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of Service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[25] F. A. Lopes, M. Santos, R. Fidalgo, S. Fernandes, and A. Software, "Engineering perspective on SDN programmability," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1255–1272, 2016.

[26] X. Xu, C. He, Z. Xu, L. Qi, S. Wan, and M. Z. A. Bhuiyan, "Joint optimization of offloading utility and privacy for edge computing enabled IoT," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2622–2629, 2020.

[27] J. Navarro-Ortiz, P. Romero-Diaz, S. Sendra, P. Ameigeiras, J. J. Ramos-Munoz, and J. M. Lopez-Soler, "A survey on 5G usage scenarios and traffic models," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 905–929, 2020.

[28] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: the communication perspective," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2322–2358, 2017.