Towards Smart Networking through Context Aware Traffic Identification Kit (TriCK) in 5G

Lina Xu
School of Computer Science
University College Dublin, Ireland
Email: lina.xu@ucd.ie

Ruifeng Duan
Comnet, School of Electrical Engineering
Aalto University, Filnand
Email: ruifeng.duan@aalto.fi

***Abstract*—In order to distribute diverse traffic flow into proper network interfaces, Access Network Discovery and Selection Function (ANDSF) is proposed by 3GPP, which can distribute every traffic flow to a preferred network interface according to several observed features from that flow. However, the static policies in ANDSF can neither understand the context nor adapt to real time changes. In order to address that problem, in our previous work, we have proposed a server-client based Context aware Traffic identification Kit (TriCK) to dynamically identify traffic, which can extend the functionalities of 3GPP ANDSF. It can classify traffic data not only based on its own characteristics, but also the real time network conditions and the current context. In this paper, we provide an implementation for the network selection component in TriCK based on clustering techniques, with a complexity of $O(n)$. A static version and a dynamic version of the implementation are analysed. The static approach is easy to implement and comprehend. The static solution can distribute the traffic flow according to the traffic characteristics and the network context. The dynamic approach can further balance the traffic load between different network interfaces and therefore provide an overall better transmission quality.**

I. Introduction

In order to address the connectivity and coverage problems in the current wireless communication world, 5G—the ultimate solution is proposed. 5G network is going to be the most powerful and widely used communication means when it can be finalised [1]. Mobile operators now would create a blend of pre-existing technologies covering 2G, 3G, 4G, WiFi and others to allow higher coverage and availability, and higher network density in terms of cells and devices, with the key differentiator being greater connectivity as an enabler for Machine-to-Machine (M2M) services and Internet of Things (IoT) [2]. Meanwhile, many wireless communication means will be available on those devices, including newly proposed M2M solutions, such as LTE-M [3]. New radio interfaces may also be invented to support both 1) low power, low throughput communication with long lifetimes and 2) high frequency, high data rate transmission. This is where an array of antennae supporting High-order MIMO (Multi-Input, Multi-Output) is installed in a device and multiple radio connections are established between a device and a cellular base station [4]. In addition to the fact that the wireless network is more complex, meanwhile, most IoT devices in the networks are in a more diverse scenario, with more than one applications running at the same time. The applications will generate many types of data such as video streaming, web browsing or file downloading. The data flow normally has its own characteristics, which can be interpreted as its specific requirements on the network services, such as delay sensitivity and data rate. In order to achieve Quality of user Experience (QoE) aware communication, we indicate that smart network selection should be implemented for 5G [5].

978-1-5090-4260-9/17/$31.00

For example, in enterprise, a bandwidth management solution is often used to guarantee the network access to business-critical applications [6]. Policies and rules are required to identify the CEO from everyone else, or recognise enterprise preferred network usages from the rest. Other rules such as specifying presenters at meetings to prioritise their network access and usage can also improve QoE. For another example, recently mist-dust-cloud architecture has become popular for IoT backhaul deployment. Many access points in the network are assumed to be multi-interface devices and are responsible for various types of traffic transmission. Selecting proper network interface for data transmission in such a network is essential to guarantee the QoE.

In order to provide smart network interface allocation services, the system needs to know the characteristics of the traffic and the network context. Access Network Discovery and Selection Function (ANDSF) was introduced by 3GPP organisation [7]. It is a core network component that is often utilised to improve user experience [8]. The ANDSF enabled devices can download from the ANDSF server in the core network and communicate with it through interface S14. The ANDSF server maintains a list of wireless communication policies that can be applied into different scenarios. Based on one of the static policies, the end device will be instructed to connect to an indicated network interface which has the highest priority at the current moment. To improve the static traffic analysis method, we have proposed a Cognitive Traffic identification Kit (TriCK) architecture in our previous work [9], as shown in Figure 1. It operates at the client side through a communication interface with the ANDSF server end. It can distribute traffic flow into available network interfaces based on the characteristics of the traffic and the current network context. In this paper, we are focusing on the traffic classification component in TriCK and implement it with two approaches—both static and dynamic clustering, to investigate its performance.

II. The Background—TriCK

TriCK is located in the end devices and it is an extended ANDSF client side with the ability of communicating with the

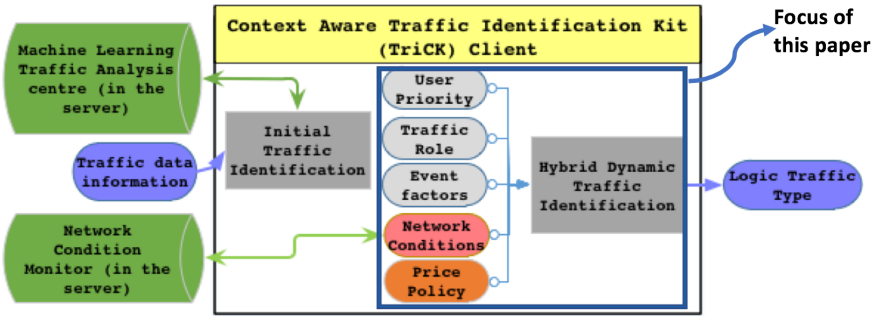

Fig. 1. Cognitive Traffic Identification Kit in Client

ANDSF server. We extract the traffic identification part from the 3GPP static policies into an individual component in the end device. It performs like a functioning box, dynamically analysing the traffic types of the transmission data based on the real network conditions and the specific user scenarios. The client part can conduct a fast and real time estimation on the traffic flow. It aims to classify all the traffic into several logic categories. The logic types can reflect

1) Data flow constraints: Some usages or data traffic from attackers that can harm the networks should be prohibited and not be allocated any network resource.
2) Price Policy: It is essential to maintain the wireless communication cost below the planned budget. For example, we know LTE is a more reliable but also more expensive resource comparing to WiFi, especially for enterprise. To meet users' requirement on cost limit, traffic identification and network selection also demand price control.
3) User priority: Users in the network system normally have a range of priorities and consequently the services provided should be tailored differently.
4) Network conditions: The traffic load through an available network interface is changing constantly. It is beneficial to balance the load in these networks to improve the overall network throughput and the quality of user experience.
5) Other factors: Events like meetings will have an impact on the traffic types and hence affect the network selection results. Taking the LTE and WiFi integrated network as an example again, a specific usage application APP_a from user Alice is normally classified as logic type 1 and routed through LTE. During a meeting time the LTE access point is fully booked for the employees who are attending the meeting. However, Alice is not one of the attendants. As a result, APP_a traffic from Alice at this period of time is identified as type 2 and will be routed through WiFi.

In order to increase the accuracy of the traffic identification results in the IoT devices without causing extra overhead, a new component is also included in the server for the end devices to communicate with. This component is able to perform sophisticated cyclic data analysis on the traffic collected from the device and the networks. The analysis results are available for the end devices to query.

The system architecture for TriCK is shown in Figure 1. The two components in green are located in the server side, which can be seen as the extensions of the existing Evolved Packet Core (EPC) network. One component is the analysis centre and it has three main functionalities. Firstly, it provides an interface for the operators to manage the restrictions or carry out the regulations on the network usages. For example, traffic from virus should be prohibited from the system. Secondly, in order to increase the accuracy of the traffic identification results analysed in the end devices without causing extra overhead, a Machine Learning traffic identification approach is implemented in the server to identify the complex cases that are out of the end devices' computing ability. Therefore, when a device has discovered some suspicious Internet traffic that it cannot determine evidently based on its own knowledge, it will report this information to the server for further confirmation. Currently many available solutions can deliver good results such as [10] and [11]. The server performs sophisticated cyclic data analysis on the traffic collected from the end devices and from the network. The analysis results, referred to as traffic roles in this paper, are available for the devices to query and then store them locally. Thirdly, this server deployed in the core network, cannot only improve the accuracy of the estimation on the traffic roles, but also can be used to monitor the network traffic. Some harmful traffic can be diagnosed and then the end user will be noticed. That traffic can be prohibited from the source without entering the network. The other component added in the server is a network condition monitor. It can monitor the congestion status for each network interfaces and provide feedbacks to the end devices.

When new traffic flow starts, the TriCK client will perform a fast prediction of the traffic role with light computing overhead based on the traffic data information itself and the information queried from the analysis server centre. The connected device will consider other factors along with the traffic role to determine the logic traffic type. Then based on the corresponding predefined policies for this logic type, the policy engine will determine which network interface to use. The logic type is different from the traffic role as we already presented. It is calculated based on not only the traffic role, but also 1) price policy, 2) user priority, and 3) data flow constraints, 4) network conditions and 5) some other factors. The role associated with the traffic will not change once it has been correctly identified by the end device or the server. However, the logic type value may alter depending on the real conditions and user profiles. Correctly identifying the traffic

role is the first step for estimating the logic type. In order to deduce more accurate results for the traffic roles, the IoT devices can query the analysis centre in the core network.

Inside the TriCK client, in order to determine the logical traffic type, five inputs are used, as shown in Figure 1.

1) **User priority:** Each users in the system will be authorised with a priority level since some users may require a better overall service quality than the others. For example, the VIP users may want to experience a faster file downloading than the normal users.
2) **Traffic role:** Traffic role can be considered as the flow's name, character, behaviour or the combination of those values herein. For example, a traffic role can be Lync video conference or Facebook Messenger. More general, it can be video streaming or file downloading. It is also referred to as the real type of the traffic.
3) **Event factors:** Some low priority user's video streaming may normally be allocated to less reliable or low cost radio communication interface. However, during showcase time, this user may demonstrate a product video to the customers. Therefore, $showcase$ as one of the event factors will increase the priority of video streaming and therefore this flow may have a better chance to use more expensive but more reliable network interface. Events like $showcase$ can be detected from the user's calendar.
4) **Network conditions:** Network conditions of the current available interfaces have a direct impact on the user experience. Therefore, in order to meet the applications' requirements, when selecting networks, their conditions, specially the congestion level, should also be considered. We assume that *Alice* is a VIP user in the network system where WiFi and LTE are both available for her. However, currently the WiFi condition is poor. Web browsing traffic for *Alice* at this moment will be routed through LTE. After a period of time, when the WiFi condition is improved, the web browsing traffic from Alice will be routed through WiFi again since it is a low cost solution.
5) **Price policy:** The data transmission over different interfaces generally have different cost. Especially in companies, WiFi is regarded as cheaper solution comparing with WiFi. Each enterprise/company will have their own policies for price control. Every user would like to set a clear budget for the wireless communication. User behaviours can be greatly customised by the price model. When the network condition can meet the transmission requirements, low cost transmission means should be prioritised.

To summarise, the TriCK client end has two basic functionalities. Firstly, it can push traffic data to the traffic analysis centre located in the core network of server side and pull the analysis results to improve the accuracy for traffic role estimation in the TriCK client. Secondly, it can do a fast dynamic identification/classification not only based on the characteristics of the traffic itself, but also price policy, user priority, network conditions, etc. In this paper, we assume that the traffic roles are already known. Clustering techniques are used to implement the classification component in the blue square as shown in Figure 1.

III. Design and Implementation

The main task of TriCK is to select an available network interface for each traffic flow and therefore to maximising the user utility according to the context. Currently five factors are in consideration in the system: user priority, traffic roles, event factors, network conditions and price policy. Among these five factors, user priority, traffic roles and event factors are user centric factors. Network condition is a network centric metric and price policy is a system centric metric. If we have k network interfaces and h traffic flow, finding the optimisation solution is a NP problem. Since the traffic in the system is assumed to have highly dynamic features, current optimisation solution may not be the one for the next second. Therefore, fast decision making on network interface selection is one essential design principle for TriCK. In TriCK system, the idea of logic traffic type is applied. We have implemented TriCK based on the clustering techniques with static and dynamic centroids. The number of logical traffic type is the number of the available network interfaces on the end devices.

If there are k network interfaces are available, then there should be k logic types and therefore k clusters. The network condition and price policy will affect the size of each cluster. The traffic flow can be characterised by their user priority, traffic roles, event factors. The network condition and price policy determine the size of each cluster. All the traffic flow in the same cluster will be allocated to the same network interface, as shown in Figure 2. Each black circle indicates one traffic flow. All the traffic flow will be clustered to join one centroid. Each centroid presents one network interface. The shortest logic distances between the traffic flow and all the centroids will be selected. Re-clustering will happen every n seconds, referred to as a round in this paper.

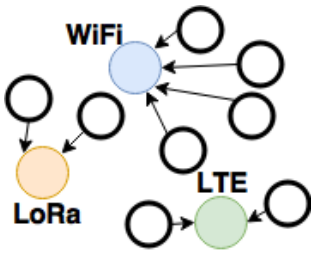

Fig. 2. Traffic flow clustering

In TriCK, five factors are considered when determining the logic traffic type, including user priority, traffic roles, event factor, network condition and price policy. User priority is ranked from 0 to 1. After being identified by the Machine Learning traffic analysis centre, the traffic role will be assigned to a value ranged from 0 to 1 indicating the characteristics of the traffic flow. At the current stage of research, we assume that the traffic roles are already specified in the packets correctly for all the traffic flow. Therefore, the traffic roles are already known without identifying by the analysis centre. Event factor for each traffic flow will also range from 0 to 1. Based on the above interpretation, each traffic flow can be presented as a point in 3 dimensional coordinate system, presented as [*user priority*, *event factor*, *traffic role*]. Every

network interface will also be assigned as a coordinate [x, y, z] according to its characteristics, where x, y and z are in the range (0,1]. They serve the coordinate system as the centroids for clustering. When selecting network interface, the logic distance between each traffic flow and all the centroids will be calculated. The traffic flow will be distributed to the network interface with the shortest logic distance if that network condition can satisfy the flow's requirements. The complexity of this clustering approach is $O(n)$, where n is the number of available interfaces on the device.

Two versions of clustering based network selection algorithms—static centroid and dynamic centroid, are introduced in this paper. In the static centroid algorithm, once the network interface has been assigned to a coordinate, the value will not change. In the dynamic centroid algorithm, the coordinates assigned for the network interfaces will keep updating according to the current network condition. Every traffic flow will reselect network interface through the clustering algorithm at the beginning of each round.

To demonstrate our idea, we assume that three interfaces including LoRa-WAN, WiFi and LTE are available on the tested devices. The lowest user priority is p_1=0.1 and the highest user priority is p_2=1. The levels for event factor are from the lowest e_1=0.1 (no meeting) to the highest e_2=1 (high priority meeting). The values for traffic role of every traffic flow will be marked as one of the three types: r_1=0.1 (low bandwidth IoT traffic), r_2=0.3 (text/picture stream traffic) or r_3=0.8 (video conferencing traffic). With bandwidth reservation mechanism, in our system, LTE is considered as a network interface that can provide better QoE than WiFi. Therefore, in our algorithms, LTE is characterised for usages from high user priority and critical access. However, we assume that the unit throughput on LTE also has a higher cost than WiFi.

Result: Distributed current traffic flow
LoRa = [(p_1+p_2)/2, (e_1+e_2)/2, r_1];
WiFi = [(p_1+p_2)/2, (e_1+e_2)/2, r_2];
LTE = [p_2, e_2, r_3];
foreach *traffic flow f [x,y,z]* **do**
  Calculate distance to LoRa, LTE and WiFi;
  d_1 = distance(LoRa, f);
  d_2 = distance(LTE, f);
  d_3 = distance(WiFi, f);
  d = min(d_1, d_2, d_3);
  if $d = d_1$ **then**
    Distribute f to LoRa;
  else if $d = d_2$ ***and*** *LTE throughput* $<$ *LTE_LIMIT* **then**
    Distribute f to LTE;
  else
    Distribute f to WiFi;
end

Algorithm 1: Network selection clustering algorithm with *static* centroids.

The static algorithm is shown in Algorithm 1. Every traffic will select a network interface with the shortest distance. The centroids for LoRa, WiFi and LTE are initialised as in Algorithm 1. The reason for the settings is that LoRa is prioritised for IoT traffic regardless of the event factor and user priority. WiFi is prioritised for text/picture traffic regardless of the event factor and user priority. The values of x and y in the LoRa coordinator and WiFi coordinator are set to be the middle value between the highest and the lowest. Since in this paper, we assume that LTE financially cost more than LoRa and WiFi, LTE is prioritised for video stream from high priority users with event factor being set. When choosing LTE, the interface will only be allocated to that traffic flow if the total bit rate through LTE is under the maximal limitation LTE_LIMIT. This algorithm will be executed repeatedly for every round.

The dynamic centroid clustering algorithm adopts the same idea as the static one. However, it will update the coordinates for WiFi and LTE, aiming to improve the network selection results and therefore to achieve better network load balancing. In our design, LoRa is specifically for low rate IoT traffic and will not be used for traffic flow with other traffic roles. Therefore, the centroid assigned for LoRa will not change. The algorithm used to update the network interface centroids is shown in Algorithm 2. In the algorithm, the value for λ can be seen as the convergent rate.

Result: Updated centroids for WiFi and LTE
d=centre for all the traffic;
d_1 = centre for all the traffic through LTE;
d_2 = centre for all the traffic through WiFi;
if *WiFi throughput* $>$ *WiFi_LIMIT* $\times$ *0.8* **then**
  d_0 = unit vector from d_1 to d;
  LTE = d_1 + d_0 $\times$ λ;
  d_0 = unit vector from d to d_2;
  WiFi = d_2 + d_0 $\times$ λ;
end
if *WiFi throughput* $<$ *WiFi_LIMIT* $\times$ *0.5* **then**
  d_0 = unit vector from d_2 to d;
  WiFi = d_2 + d_0 $\times$ λ;
end
if *LTE throughput* $>$ *LTE_COST* **then**
  d_0 = unit vector from d to d_1;
  LTE = d_1 + d_0 $\times$ λ;
end

Algorithm 2: Network selection clustering algorithm with *dynamic* centroids.

TABLE I. EXPERIMENTAL PARAMETER SETTINGS

Parameter	Value
WiFi_LIMIT	54 Mbps
LTE_LIMIT	50 Mbps
LTE_COST	40 Mbps
λ	1
Simulation time	30 rounds

TABLE II. TRAFFIC GENERATOR SETTINGS

Factor	Available levels
User Prority	0.1 or 1
Event factor	0.1 or 1
Traffic role	0.1 with mean = 0.0015 Mbps and STD = 0.0015 Mbps
Traffic role	0.2 with mean = 1 Mbps and STD = 0.5 Mbps
Traffic role	0.8 with mean = 4 Mbps and STD = 2 Mbps

TABLE III. TRAFFIC SCENARIO SETTINGS PRESENTED IN THE FORM OF [*user priority*, *event factor*, *traffic role*].

Round 1-3	Round 4-7	Round 8-9	Round 10-13	Round 14-15	Round 16-19	Round 20-21	Round 22-24	Round 25-26	Round 27-29	Round 30
[1, 0.1, 0.1] [0.1, 0.1, 0.1]	[1, 0.1, 0.1] [0.1, 0.1, 0.1] [1, 0.1, 0.3] [0.1, 0.1, 0.3]	[1, 1, 0.1] [0.1, 1, 0.1]	[1, 1, 0.1] [0.1, 1, 0.1] [1, 1, 0.3] [0.1, 1, 0.3]	[1, 1, 0.1] [0.1, 1, 0.1] [1, 1, 0.3] [0.1, 1, 0.3] [0.1, 1, 0.8]	[1, 1, 0.1] [0.1, 1, 0.1] [1, 1, 0.8] [0.1, 1, 0.8]	[1, 1, 0.1] [0.1, 1, 0.1] [1, 1, 0.8] [0.1, 1, 0.8] [1, 1, 0.3] [0.1, 1, 0.3]	[1, 1, 0.1] [0.1, 0.1, 0.1] [1, 1, 0.8] [0.1, 1, 0.8]	[1, 0.1, 0.1] [0.1, 1, 0.1] [1, 0.1, 0.3] [1, 0.1, 0.8] [0.1, 0.1, 0.3] [0.1, 0.1, 0.8]	[1, 0.1, 0.1] [1, 0.1, 0.3] [0.1, 0.1, 0.1] [0.1, 0.1, 0.3]	[1, 0.1, 0.1] [0.1, 0.1, 0.1]

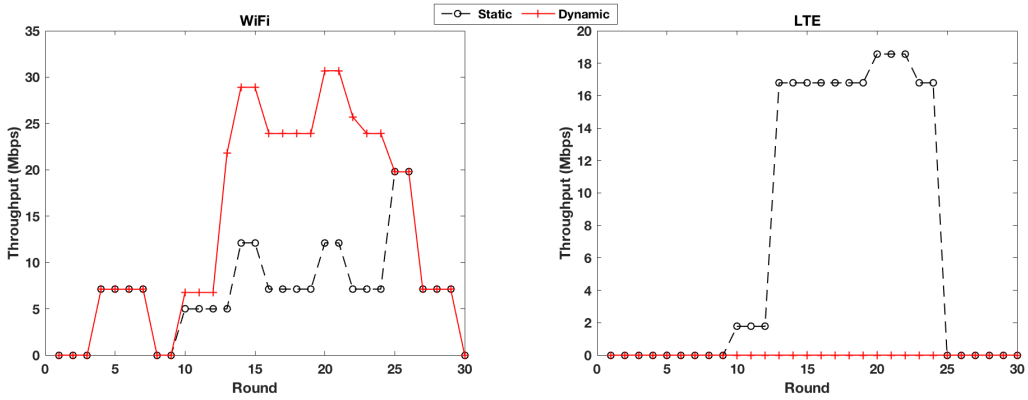

Fig. 3. Low text/picture stream traffic in network. Low utilisation in WiFi network.

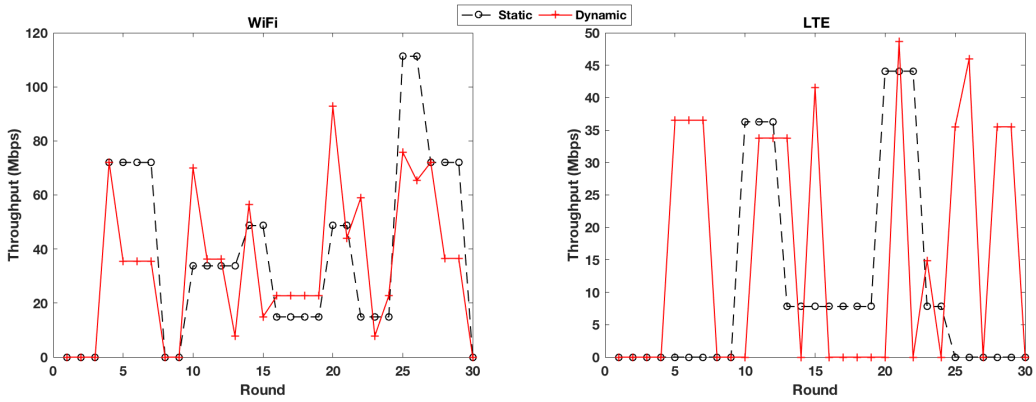

Fig. 4. High text/picture stream traffic in network. Load balance between LTE and WiFi to relieve congestion on WiFi.

IV. EXPERIMENTS AND RESULTS

In this paper, we have used MatLab to construct our simulation. In the experiment, each round is assigned for $n = 30$ seconds. The network interfaces will be re-selected at the beginning of every round. Other setting for the simulation can be seen in Table I. They are the parameters used in Algorithm 1 and Algorithm 2. WiFi_LIMIT and LTE_LIMIT are the maximal bandwidth that the WiFi and LTE network can offer respectively. LTE_COST is the cost control on LTE network usage.

In order to simulate a real world network scenario, we have implemented a traffic generator in MatLab, which can emulate 12 (2 user priority levels $\times$ 2 event factor levels $\times$ 3 traffic roles levels) different patterns of traffic flow as shown in Table III. In the experiments, for each traffic role, we assume that the traffic's bit rate follows a normal distribution based on the central limit theorem. The settings for the traffic in the network for each round is shown in Table III. In different period of rounds, the types of traffic are changing constantly. The number of traffic flow for each traffic type can also be altered based on the settings in each scenario. For example, for Round 1-3, there might be 3 traffic flow for traffic type [1, 0.1, 0.1] and 2 traffic flow for type [0.1, 0.1, 0.1]. Doing this can control the total bit rate in each round for each traffic role.

For the first scenario, low text/picture stream traffic was injected to the system. The total traffic amount for type [x, y, 0.3] in Table III was set below 10Mbps per round, where x and y were set to be any available values in range. The static and dynamic clustering network selection algorithms were applied to manage the network interface allocation for the traffic in Table III. The experimental results are shown in Figure 3. As we can see, the static solution has distributed different traffic based on the user priority, event factor and traffic roles. Both LTE and WiFi network interfaces were utilised. Since the traffic distributed to WiFi network was low, the WiFi network condition was good. It still had a lot of spare bandwidth unused in this scenario. In this circumstance, WiFi can also guarantee the quality of high priority user's video traffic. In order to reduce the finical cost, all the traffic through LTE can be re-allocated to WiFi. With the dynamic solution, we can see from Figure 3 that all the traffic was transmitted through WiFi.

In the second scenario, we have injected a high text/picture stream traffic in the system and the experimental results are shown in Figure 4. We can see that with the static solution, the WiFi network was severely congested near round 5 and 25. However, LTE network has a low utilisation. On the other hand, with the dynamic solution, the congestion can be controlled effectively and efficiently, near round 5 and 25. The two networks can cooperate better and relieve the congestion problem on WiFi network. In summary, the dynamic clustering approach can balance the load between LTE and WiFi networks to a better degree.

TABLE IV. NO. OF ROUNDS WHEN WIFI NETWORK IS CONGESTED

Test 1	Static	Dynamic	Test 2	Static	Dynamic
100%	11	9	100%	19	12
120%	11	7	120%	11	10
150%	4	1	150%	4	6
Test 3	Static	Dynamic	Test 4	Static	Dynamic
100%	15	15	100%	15	11
120%	4	5	120%	13	9
150%	4	3	150%	2	3
Test 5	Static	Dynamic	Test 6	Static	Dynamic
100%	15	10	100%	15	11
120%	15	10	120%	11	8
150%	8	6	150%	4	4

Table IV has detailed the number of rounds when WiFi network were congested in the simulation. When the generated traffic requires 100% of the maximal WiFi capability—WiFi_LIMIT, we considered the network is congested. When the percentage reaches 120%, the network is highly congested. When the percentage is over 150%, the network is seen as seriously congested and the quality of user experience over such a network will not be guaranteed. As we can expect, when the percentage increases, the possibility of packet drop and delay will consequently increase. Table IV has summarised the results for 6 repeated experiments for the high text/picture stream traffic scenario. The dynamic solution in general can reduce the number of rounds of highly congested and seriously congested by leveraging part of traffic from WiFi network to LTE network. Therefore, it can be concluded that the dynamic clustering approach is able to balance the load between network interfaces to a better degree.

V. ANALYSIS AND FUTURE WORK

Based on the proposed idea on our former work–the TriCK architecture, there are many possible approaches to achieve smart and context aware network selection. The realisation of such a implementation requires the cooperation from operators, enterprise/companies and 3GPP organisation. Since the solution is proposed based on the operators existing infrastructure and it is following 3GPP's standards, it is highly practical and realistic in terms of implementation. It is one design principle we always hold.

In this paper, we have provided two implementations with applying clustering technologies. At this stage, the current solutions have several limitations and can be improved from the several following perspectives. First, in the dynamic clustering approach, how to update the centroids assigned for the available network interfaces can be critical for the performance of the algorithm. We have analysed the impact of changing the value for λ. When λ is too high, the network usage can be unstable. When λ is too small, the system cannot adapt to highly dynamic traffic changes effectively due to low convergent rate. We suggest this value should be set according to the using scenario. Secondly, more network interfaces with different characteristics should be considered in the future implementation to adapt to more complex MIMO scenario. Thirdly, other factors such as time of the day, location information can also be included in the traffic coordinate system by increasing the dimensions. At the end, energy consumption will be discussed when evaluating the clustering algorithm in the future model.

VI. CONCLUSION

This paper presents a continuing work based on the network selection solution TriCK. We have proposed two implementations for TriCK utilising clustering techniques— static and dynamic clustering based network selection algorithms, both having a complexity of $O(n)$. It can distribute traffic flow into different network interfaces based on the characteristics of the flow. We have analysed the two algorithms in a simplified MIMO scenario, with LoRa, WiFi and LTE network interfaces available. The dynamic clustering algorithm can achieve an even better load balancing between two network interfaces (WiFi and LTE) according the network condition and the cost control policy. In the future work, the proposed solutions will be extended to adapt to more complex MIMO scenarios.

REFERENCES

[1] A. Gupta and R. K. Jha, "A survey of 5g network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[2] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5g era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, March 2016.

[3] R. Ratasuk, N. Mangalvedhe, A. Ghosh, and B. Vejlgaard, "Narrowband lte-m system for m2m communication," in *2014 IEEE 80th Vehicular Technology Conference (VTC2014-Fall)*, Sept 2014, pp. 1–5.

[4] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5g," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, 2014.

[5] L. Xu, R. Collier, and G. M. P. O'Hare, "A survey of clustering techniques in wsns and consideration of the challenges of applying such to 5g iot scenarios," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1229–1249, Oct 2017.

[6] S. Shenker, "Fundamental design issues for the future internet," *IEEE J.Sel. A. Commun.*, vol. 13, no. 7, pp. 1176–1188, Sep. 2006. [Online]. Available: http://dx.doi.org/10.1109/49.414637

[7] G. A. N. Discovery and S. F. A. M. O. (MO), "http://www.3gpp.org/dynareport/24312.htm."

[8] L. Xu, J. Xie, X. Xu, and S. Wang, "Enterprise lte and wifi interworking system and a proposed network selection solution," in *Proceedings of the 2016 Symposium on Architectures for Networking and Communications Systems*, ser. ANCS '16. New York, NY, USA: ACM, 2016, pp. 137–138.

[9] L. Xu, "Context aware traffic identification kit (trick) for network selection in future hetnets/5g networks," in *International Symposium on Networks, Computers and Communications (ISNCC)*, May 2017, pp. 1–5.

[10] Z. A. Qazi, J. Lee, T. Jin, G. Bellala, M. Arndt, and G. Noubir, "Application-awareness in sdn," in *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, ser. SIGCOMM '13. New York, NY, USA: ACM, 2013, pp. 487–488. [Online]. Available: http://doi.acm.org/10.1145/2486001.2491700

[11] A. Callado, C. Kamienski, G. Szabo, B. P. Gero, J. Kelner, S. Fernandes, and D. Sadok, "A survey on internet traffic identification," *IEEE Communications Surveys Tutorials*, vol. 11, no. 3, pp. 37–52, rd 2009.