Mobile Opportunistic Traffic Offloading

(MOTO)

D2.2.1: General Architecture of the Mobile Offloading System Release A

Document information	
Due Date	October 31, 2013
Subsmission Date	October 15, 2013
Status	Edition
Editor	TCF
Contributors	TCF, CNR, INNO, UPMC, FON, AVEA, CRF, INT

Contents

1 Executive summary

This document IS release *A* of deliverable D2.2, *General Architecture of the Mobile Offloading System*, whose purpose is to provide the description of MOTO's architecture, based on output of Task 2.1, reported in D2.1, *Use Cases and Requirements*. First, it reminds the project purpose, its context, and the technical proposition. Then, it studies the related state of the art by providing an overview of related projects, software, and services.

For the description of the MOTO architecture, which represents the main part of this document, we have decided to:

- Summarize the uses cases.
- Identify the actors and their roles.
- List the users and system requirements extracted from the use case scenarios.
- Present the system architecture.
- Make the description of the architecture as clear as possible by mapping all the use cases identified in Deliverable *D2.1* on top of the architecture.

Before concluding, the document describes how the MOTO project tackles a number of fundamental research challenges by identifying, describing, and proposing directions to the main problems that have a direct impact on the project outcomes.

2 MOTO's proposition

2.1 Context

Over the latest few years, we have witnessed the widespread diffusion of smartphones, tablets, and other mobile devices with diverse networking and multimedia capabilities. According to Cisco, global mobile data will experience a growth of more than 26 times in only five years for the period 2010-2015 [1]. This poses dramatic challenges to mobile telecom operators all over the world. Major operators in the US [2] and Europe [3] are experiencing severe problems in coping with the mobile data traffic generated by their users. Considerable progress is constantly made at the physical layer to increase raw bitrates, and clearly LTE and LTE-advanced will help in this direction, but this is neither sufficient nor cost-efficient to accommodate all the increase in data service demand. This is because the trend of the traffic demand is exponentially increasing [1, 4], while the improvements at the physical layer are bounded by the famous Shannon theorem and by the fact that the licensed spectrum is a limited and scarce resource [5]. Moreover, provisioning "additional" 4G infrastructure (even in the "lightweight version" of LTE relays) bears significant costs both at the deployment and the management phases. As a result, it is expected that the amount of traffic generated by 4G users will be about

one order of magnitude larger than the bandwidth operators will be able to deliver. The operator will need to decide to either drastically reduce the quality of service (QoS) for all the users, or block a significant fraction of the users to provide acceptable QoS to a few. Both alternatives are largely sub-optimal and generate user dissatisfaction.

Mobile operators are investigating different alternatives to add new capacity to their wireless infrastructures to cope with the explosive growth in data service demands, but at a much lower cost per bit. The first approach has been to consider the upgrade to new radio-access technologies, such as 3GPP LTE and LTE-Advanced standards. This can be considered as straightforward solutions to increase the network cellular capacity because they significantly increase the spectrum efficiency, and can reduce operational costs thanks to the use of simplified and more flexible network architecture [6]. In parallel, IEEE Working Groups are also developing several wireless broadband standards, such as 802.16j, 802.16m and 802.11n, which aim at fulfilling ITU's requirements for telecommunication-advanced systems (a.k.a. 4G), namely peak data rates of 100 Mbit/s mobile and 1 Gbit/s fixed. To attain such high data rates, there have been considerable research efforts to enhance LTE technology with more advanced multi-antenna technologies, coordinated multipoint transmission/reception and carrier aggregation techniques, and to exploit multi-user diversity through OFDMA schemes [7]. However, all these advanced technologies have almost reached their theoretical limits. Recent studies indicate that these spectral efficiency enhancements are significantly lagging behind with respect to the rate traffic growth [1].

As a consequence, more disruptive innovations in the architectural model of broadband wireless networks have to be explored to help network providers meet the exponential growth in mobile data traffic demand. Heterogeneous Network (HetNet) deployments have recently attracted a growing attention with the objective to improve system capacity by increasing network efficiency [8]. HetNet is a new multi-tier paradigm for cellular networking where the traditional deployment of macro/micro cells, namely base stations with similar characteristics, is overlaid with a myriad of low-power and low-cost devices with heterogeneous characteristics and constraints (e.g., antenna patterns, transmit power levels, air interfaces, and backhaul connectivity to the data network.) such as picocells, femtocells and relays, as well as radio remote heads (RRHs), deployed on coverage holes or capacity-demanding hotspots [8]. This multi-tier structure enhances the network capacity thanks to the reduced distance between the access network and the end terminal improving these spatial spectrum reuse. However, HetNet performance is limited due to interference between devices operating simultaneously in the same spectrum. Various studies have proposed quite sophisticated interference mitigation techniques for heterogeneous networks, supporting device synchronization, intra-tier and cross-tier interference coordination through power control and frequency planning, and duty cycling for controlling device density [9]. Moreover, HetNet by pushing continuous miniaturization of cells adding more base stations with smaller coverage radii, in turn unveil a prohibitively expensive deployment in the long term due to the cost of installing and maintaining new sites and backhaul links, and the unmanageable interference from nearby cell transmissions. Cost issues can become the central factor driving the selection of solutions for the

new generation of 4G/LTE networks capable of serving growing demand in the densely populated urban areas. In addition, many analysts also fear that higher capacity networks could lead to even higher data consumption over the next few years, making operators' efforts insufficient [1, 3, 5].

Based on the above discussion it becomes apparent that, to boost network capacity further, mobile network operators must firstly *leverage unused bandwidth across different radio access technologies* (first and foremost unlicensed wireless technologies, such as Wi-Fi) to offload a part of the traffic from their cellular access networks. In a further evolution, users can also cooperate with the wireless infrastructure and with each other by leveraging short-range opportunistic communications between nearby terminals to facilitate the content dissemination while reducing the load on the wireless infrastructure of the cellular and Wi-Fi operators. Different offloading techniques have been devised based on the assumptions made about the level of synergy between cellular networks and unlicensed wireless networks, the involvement of the user terminals in the offloading process, and the characteristics of offloaded data. On-the-spot offloading constitutes one class of offloading techniques where the cellular operator uses Wi-Fi infrastructures on demand only when it is available. A recent research study conducted using Wi-Fi connectivity traces in metropolitan areas indicated that on-the-spot offloading could offload about 65% of the total traffic load [10]. Delayed offloading is a relatively newer approach that is based on a concept very close to that of delay-tolerant networks, where applications, such as sharing of user generated content, can tolerate some amount of delays without significantly hurting user experience. In this case, the data transfer can be delayed till the user has a low-cost transmission opportunity with a Wi-Fi network. Other study results have shown [10] that up to 78% of cellular traffic can be offloaded if the data transfer could be delayed for more than one hour.

These initial results are the starting point for the MOTO technical proposition, which is presented in the next section. MOTO goes beyond these solutions, by proposing a more systematic view to the problem of offloading using terminal-to-terminal communications. From an architectural standpoint, MOTO starts with a general conceptual architecture which encompasses the key functional blocks needed to manage an integrated network with offloading capabilities, abstracting away the functions that are not related to any specific wireless technology (cellular vs Wi-Fi, for example). This is the basis for deriving a detailed architecture, presented later on in this deliverable.

2.2 Overview of the technical proposition

As discussed in Section 2.1, different offloading possibilities (on-the-spot, delayed) can be made available to extend capacity or coverage of cellular networks. However, such offloading processes do still consider the mobile terminal and the mobile user as static agents, which benefit from but do not take an active part in the offloading process. **In the MOTO project, we propose a synergic use of a diverse set of complementary offloading techniques, by adding another layer of offloading through direct hop-by-hop communications between terminals**. Such an approach is enabled by

the fact that current mobile users' terminals are equipped with a range of complementary wireless communication technologies, allowing them not only to easily and dynamically connect to different wireless infrastructures, but also to establish direct connections with each other.

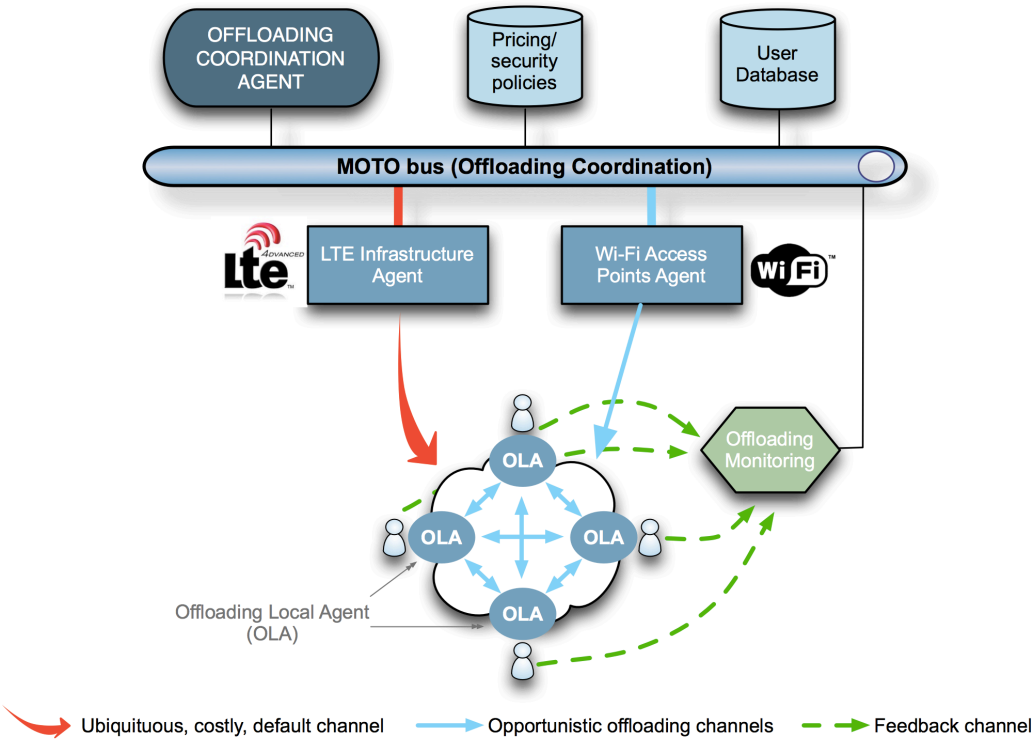


Figure 1: Conceptual MOTO architecture.

As illustrated in Fig. 1, in MOTO the data dissemination process will only partly go through the "costly, default" channel, consisting of the LTE infrastructure (note that the term "costly" in the caption is used to denote that, if all users access content via this channel, the wireless infrastructure easily becomes congested, and this results in additional costs for the operator for overprovisioning it, which eventually results in additional costs also for the users). Part of the users will be reached by exploiting the availability of Wi-Fi access points, as well as by exploiting direct terminal-to-terminal communications, thanks to ad hoc opportunistic technologies. Due to energy saving reasons operators and/or users may want to configure their mobile devices so that the ad hoc wireless interfaces are not continuously switched on, but dynamically alternate between active (energy consuming) and inactive (energy saving) states. Therefore, even in a network with only static nodes, whose wireless ad hoc interfaces are managed according to duty cycling schemes, devices cannot continuously communicate in ad hocmode with each other (even if they are within each other communication range), but communication opportunities arise dynamically, when their ad hoc wireless interfaces happen to be active at the same type. MOTO will thus consider both types of opportunistic networks, i.e., those formed because of real

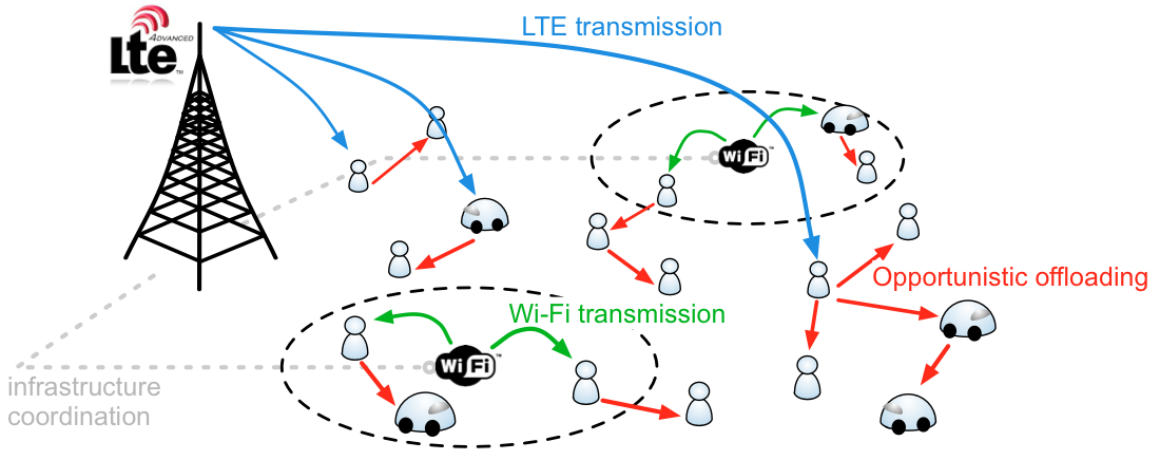


Figure 2: Offloading possibilities in MOTO.

users' mobility and those formed because of duty cycling schemes. Orchestrating the above process requires coordination between the various communication technologies. **In MOTO this will be achieved by developing the conceptual architecture shown in Fig. 2, which is the starting point for designing the operational architecture, main subject of this deliverable**. Specifically, we envision that an overlay control layer, which is logically supported through the "MOTO bus" and the "offloading coordination agent", implements the coordination and inter-technology scheduling policies.

Such an "overlay" layer on top of the various types of networks will work under the control of the operators, such that the offloading process can be dynamically monitored and adjusted, based on its own evolution, and on the dynamic conditions of the networks themselves. The synergic use of different offloading technologies means that a subset of the users will receive the content from one of the wireless infrastructures, and start propagating it epidemically through ad hoc opportunistic technologies that can be controlled by the operator on its customers' devices. In this phase, opportunistic dissemination schemes may also exploit information about preference, behaviours, and mobility patterns of the users, stored in the "user database". With respect to conventional opportunistic data dissemination schemes, MOTO adopts a novel approach, whereby the wireless infrastructures will be used to implement a control loop on the status of the dissemination process. In fact, the wireless infrastructures will be used to monitor the status of the dissemination process (e.g., in terms of the fraction of users that have received contents by a certain time). The "offloading monitoring", part of the control loop, will provide necessary information to the offloading agent to supervise the possible reinjection of copies of the content via the infrastructure whenever it estimates that the ad hoc mode alone will fail to achieve full dissemination within some target delay. Note that, although there are certainly scalability issues that MOTO will address in the design of the control and terminal-to-terminal protocols, the load on the wireless infrastructures posed

by such a control loop will be minimal, as it only requires mobile users to upload short control information (sort of ACKs) when they receive the content they are interested in. Moreover, the availability of wireless infrastructures can be exploited to optimize the ad hoc opportunistic data dissemination process by providing contextual information that is typically not available in opportunistic networks. For example, cellular operators may predict with reasonable reliability future cells and mobility patterns of their users, thus enabling MOTO to predict with some degree of accuracy which pairs of users will happen to be relatively close to each other and therefore could have terminal-to-terminal communication opportunities in the near future. Clearly, this information is one of the basis on which opportunistic data dissemination processes is built.

Last but not least, the MOTO control loop is also used to monitor security issues and guarantee that security profiles agreed by the operators and their customers are preserved also during the terminal-to-terminal dissemination process.

While being an active subject of investigation in the research community, providing effective and efficient architecture and technical solutions for offloading still presents key challenges. To conclude this section, we provide a brief discussion about them. After aving presented the key functional blocks of the MOTO conceptual architecture, this helps clarifying the technical approach taken by the project to implement them.

1. **Mobile traffic offloading management and control:** Mobile data traffic offloading in 4G/LTE networks is most often associated with the ability to redirect traffic generated by cellular customers to Wi-Fi infrastructures managed by the same cellular operator. The general idea of terminal-based offloading is to use terminal-to-terminal direct communications and user mobility to reduce the load on the wireless infrastructures. One major advantage of terminal-based offloading is that there is almost no monetary cost for the mobile operator in using ad hoc communications between mobile devices. On the other hand, there is not yet a clear understanding of how the network operator can control the offloading process and assist the mobile users in the various phases of the opportunistic data dissemination. Most of the existing solutions focus on offloading from the cellular network, and assume that the cellular network is only used to deliver delay-tolerant content to a small fraction of selected users, which can then propagate the content to interested users when their mobile phones are within transmission range of each other.

2. **Offloading strategy coordination:** Currently, significant efforts are undergoing towards an improved interworking between multi-operator infrastructures and an enhanced cooperation between control functions (such as mechanisms for network access control, mobility management, security management, and session management) in mobile, fixed and wireless networks with the objective to provide better services to network customers. The issue is how to orchestrate different forms of offloading in single and multi-operator environments in order to "optimize" the offloading process defining inter-technology scheduling policies for controlling the process between multi-operator infrastructures and opportunistic networks formed by user terminals.

3. **Distributed trust and security:** Existing methodologies for security assurance and policy design have introduced and proposed means to evaluate and maintain necessary security assurance (SA) levels in networked IT systems, mainly targeted at relatively stable big telecommunications systems. The main challenge for distributed trust and security deals with the development of measurement infrastructure for highly distributed opportunistic networking infrastructure that can support security assurance for user-terminal offloading services. The second main challenge is to understand the correct balance between security monitoring functions at terminal and network level and the performance of the service functions to be leveraged by MOTO.

4. **Offloading capacity improvement estimation:** In principle, wireless infrastructure operators will be able to "see" MOTO offloading as a reserve of capacity, to be activated on-demand, in any of the scenarios highlighted above. A significant challenge of this general idea is to quantify the additional capacity that would be available by activating offloading. Addressing this challenge is necessary, as operators will need to know how much capacity they could count on by activating an offloading process, so as to plan what percentage of traffic to divert from the wireless infrastructure, which QoS guarantees could be provided to the part of the traffic that will not be offloaded, and what would be the expected performance of data transfer through the offloading process, e.g., in terms of content delivery time.

5. **Fine-grained mobility and contact opportunity modelling:** The efficiency of opportunistic offloading inherently relies on how the proposed strategies get advantage from the dynamics of the underlying infrastructure. It becomes then fundamental to understand how nodes move around and, most importantly, how they meet creating communication opportunities. In a context where every opportunity for communication counts, it becomes important to capture contact opportunities in a fine-grained fashion and characterize mobility at the microscopic level. Also, in crowded spaces users might switch on and off their devices, thus generating a non-mobility-induced opportunistic network. So the challenge is to tackle the problem from a spatio-temporal viewpoint, by considering contacts not only as individual phenomena but also as an atomic event.

6. **Mobile duty cycling management:** Offloading on mobile terminals can be seen per se as an energy saving opportunity, despite the fact that offloading requires the use of an additional wireless interface for the terminals to be active on the ad hoc opportunistic network. Under very crowded and congested environments, the resulting energy-per-useful-bit received at the application level for terminals not using MOTO offloading is very high due to transmission inefficiencies. In very crowded environments, if all mobile terminals try to establish ad hoc connections at the same time, the interference among mobile terminals will become prohibitive, and the net transport capacity will be dramatically low, thus making the offloading process useless. The challenge is to achieve a right balance in duty cycling manage-

ment, because a too aggressive duty cycling will make the ad hoc network basically useless, as too few communication opportunities will be available.

3 State of the art

The realization of high data rates in LTE technology over an all IP network means an ever increasing load on packet data networks. 3GPP has defined data offloading as a key solution to cope with this challenge. There has been an exponential increase in mobile IP data usage, caused by higher throughputs that cellular technologies offer and the increasing global footprint of mobile networks. Innovative applications in popular areas like social networking, media sharing and newer class of devices like tablets have increased the consumption of data manifold. Estimates say that mobile devices overtook PCs in packet data consumption and this will continue in the future. With such orders of magnitude increase in mobile data consumption, cellular networks are likely to be operating at their capacity limits and hence, operators continuously look for ideas and methods to ensure that their networks do not get overloaded. One of several such methods is data offloading. Mobile data offloading, also referred to as mobile cellular traffic offloading, is the use of complementary network communication technologies to deliver mobile data traffic, originally planned for transmission over cellular networks.

There are three key data offloading areas that 3GPP Rel-10 has been working on. These are LIPA (Local IP Access), SIPTO (Selective IP Traffic Offload) and IFOM (IP Flow Mobility) [11]. Each method has its field application (private local networks rather than macro networks) and its pros and cons. All the three mechanism cater to the basic requirement of data offloading, but have critical differences that in some ways are complementary. They offer different options to operators to suit to their specific requirements.

3GPP is currently focused on improving and optimizing these architectures and describing how these features interact with other legacy features. A more recent approach of using Delay Tolerant Network (DTNs) to migrate cellular data traffic has been proposed by several works [12, 13, 14, 15, 16]. By benefiting from the delay-tolerant nature of non-realtime applications, the service providers can delay and even shift the transmission to DTN. Benefiting from common interests among the users, providers only need to deliver the information to a small fraction of users and then it will be further disseminated by the selected users through DTN communications. This kind of offloading should be encouraged by the operators as it is the quickest way, at the smallest cost, to support the exponential growth of mobile data. Quantitative study are also taken on the perfomance of 3G mobile data offloading through WiFi networks [17]. Building more WiFi hot spots is significantly cheaper than network upgrades and build-out. Many users are also installing their own WiFi APs at homes and work. If a majority of data traffic is redirected through WiFi networks, carriers can accommodate the traffic growth only at a far lower cost and investment. With increased data rates and mobile data usage, coupled with more widespread home and public WiFi network roll outs, the relevance of offloading mechanisms will continue in the coming years and hence, will be a key area of innovation

within the wireless network development community. The MOTO project will advance the stat-of-the-art in this field by delivering and testing operative protocols and algorithms (also supported by foundational results) and building a solid understanding about the mobile traffic that can be offloaded from cellular networks to low-cost communications technologies, under different offloading paradigms, such as offloading across different wireless infrastructure technologies (e.g., from cellular to Wi-Fi), and offloading to mobile terminals (e.g., from cellular or Wi-Fi to mobile terminals). Although diverse offloading paradigms will be considered, MOTO project main emphasis will be on terminal-based offloading, and MOTO project will quantify the impact on the offloading efficiency of user mobility profiles, heterogeneity of network deployments, users' demands, delay and priority requirements of different classes of mobile applications, as well as variable terminal densities induced by duty cycling.

3.1 Related projects

Currently, the french project ANR-CROWD [18] is an on-going collaborative project related to MOTO. As said, wireless traffic demand is currently growing exponentially. This growing demand can only be satisfied by increasing the density of points of access and combining different wireless technologies. The minimizing the load of the LTE network plus energy efficiency, to avoid unsustainable energy consumption and network performance implosion, are one of the CROWD objectives that just meet the concepts of MOTO. Mainly CROWD pursues four key goals: i) bringing density-proportional capacity where it is needed, ii) optimising MAC mechanisms operating in very dense deployments by explicitly accounting for density as a resource rather than as an impediment, iii) enabling traffic- proportional energy consumption, and iv) guaranteeing mobile user's quality of experience by designing smarter connectivity management solutions.

3.2 Software, applications and services

The following related classes of software, application and services have been identified:

- Web caching and Proxy: Web caching can improve the overall performance of World Wide Web in several ways. By placing caches in strategic positions, the core network traffic can be reduced, the load of a content provider can be scaled down and the quality of service, as the user perceive it, can be improved. Dedicated computer systems, called Proxies, are installed at the edges of local or wide area networks. These systems can achieve significant reduction in the network traffic and improvement in the user perceived quality of service, by filtering and serving the Web requests generated inside the entire network they serve. If a user has defined in the browser's settings a particular proxy to be used, every time the user requests a Web page, the browser will send this request to the proxy. If the proxy happens to have the page, the user will be served promptly without the original content provider being contacted. If the proxy cannot serve the request, it will fetch the appropriate Web objects form the original server, and possibly keep a copy for later use.

A caching proxy server accelerates service requests by retrieving content saved from a previous request made by the same client or even other clients. Caching proxies keep local copies of frequently requested resources, allowing large organizations to significantly reduce their upstream bandwidth usage and costs, while significantly increasing perfomance.

- Offline browsing: The browser attempts to fetch pages from servers while only in the online state. In the offline state, users can perform offline browsing, where pages can be browsed using local copies of those pages that have previously been downloaded while in the on-line state. This mechanism can reduce latency perceived by the user, reduce traffic network, reduce server load and improve response time to the users.

- Traffic congestion detection: Cooperative vehicular communications represent a promising technology to improve road traffic safety and efficiency. Through the continuos exchange of messages between vehicles (Vehicle-to-Vehicle V2V communications) and between vehicles and infrastructure nodes (Vehicle-to-Infrastructure), real-time information about the current road traffic condition can be cooperatively collected and shared. Novel techniques are currently being investigated to efficiently detect and characterize road traffic congestion using V2V/V2I communications. These techniques are capable of providing valuable information to road traffic managers about the characteristic of the detected congestion conditions (for example, its location, length and intensity) without deploying any infrastructure sensors and requiring significant communications overhead.

- Content (Information)-Centric Networking: Content-Centric Networking (CCN) is a novel networking paradigm centered around content distribution rather than host-to-host connectivity. This change from host-centric to content-centric has several attractive advantages, such as network load reduction, low dissemination latency, and energy efficiency. An increasing demand for highly scalable, timely and efficient distribution of content and information has motivated the development of architectures that focus on information objects, their properties, and receiver interest in the network to achieve effective dissemination of content and information. One of the main features of these architectures is its ability to cache packets in intermediate routers to take advantage of spatio-temporal locality in serving multiple requests for the same content, reducing thus considerably the network traffic.

3.3 Other solutions

3.3.1 New Cells Deployment

The first obvious solution adopted by cellular providers to face the mobile data growth is to scale the network capacity by building more base stations of smaller cells size. As explained in [19], macro-cell size reduction increases the total available bandwidth, implying a better spatial reuse of each radio channel and a reduced distance between the access network and the end terminal, that in turns means higher data rates within

the same transmit power. The drawback of this strategy is that operators might have to build new radio base stations that considering costs for equipment, site rental, backhaul, power consumption and site acquisition becomes very expensive. In addition according to [20], only a small part of the mobile users (around 3%) consume 40% of all traffic, so the majority of user gets a fractional benefit form scaling as the major consumers will continue to seize the increased bandwidth.

Another possibility for network providers is to expand network capacity using femtocells, to provide indoor coverage. Femtocells are small, inexpensive, low-power base stations that work on the same licensed spectrum as the cellular network, and are generally consumer-deployed. Cellular operators can then reduce the traffic on their RAN when indoor users switch from macro-cells to femtocells. However, since femtocells most often use the same frequency as the macro-network, interference management with the macro network becomes challenging, as pointed out in [21]. There are a few studies in literature that focus on performance of femtocells offloading [22, 23], and others that compare the gains brought by femtocells and IEEE 802.11 offloading [24, 25]. Some other works focus more on energy efficiency topics related to the use of femtocells [26]. In addition, an two surveys on femtocells are provided in [27], and [28].

3.3.2 Technology Upgrade

The wireless spectrum is a scarce and costly resource, and meeting the growing demand for wireless services means that wireless technologies will have to become much more spectrally efficient. Starting from the analog 1G to the 4G, that is OFDMA and IP-based, the cellular technology at each generation has evolved and optimized the usage of the radio spectrum, providing ever greater data rates [29]. Despite this, the theoretical bandwidth that can be allocated in the licensed band is physically limited, and the growth of data consumption will continue to outpace the technology upgrades. Moreover, technology upgrades are costly, because requires new equipment installation; many analysts also fear that higher capacity networks could lead to even higher data consumption over the next few years, making operators' efforts insufficient [30].

3.3.3 Cognitive Radio Integration

Cognitive radio, is a novel technique applied to network equipments that helps in reducing spectrum congestion. Today, the radio spectrum is assigned in a fixed way. However, a large portion of the assigned spectrum is used sporadically. The limited available spectrum and the inefficiency in the spectrum usage necessitate to exploit the existing wireless spectrum opportunistically [31]. Cognitive radios detect unused spectrum and share it, without harmful interference to other users, in order to enhance the overall network capacity. This way operators are able to enhance the QoS of their networks and can avoid some capacity issues [32]. Cognitive radio can be applied also to offloading network deployment [33], where indoor access points or femtocells have the ability to scan the radio channel and estimate which resources are free among the available ones in order to avoid

interference. Cognitive technologies are thus capable of increasing spectrum efficiency and network capacity significantly.

3.3.4 Proactive Caching

Caching is a popular technique, commonly used in web based services in order to reduce traffic volume and improve the user perceived delays and the load on the web servers. Caching techniques stores popular data in the end-user local storage or in a cache proxy located in the network edge. The performance of the caching scheme are bounded by the hit rate of the cache; the higher the hit rate, the better the performance. Some of the classical cache concepts can be re-utilized in mobile networks, to improve performance. In order to avoid peak traffic load and limit congestion in mobile networks, techniques for predicting users' next requests and pre-fetching the corresponding contents are available [34, 35]. Contents can be proactively cached directly on user device, on the cellular base station, or on IEEE 802.11 access point that can help the offloading process. The prediction accuracy became the key factor of the system and is performed using statistical methods or machine learning techniques.

4 Moto architecture

Before describing the architecture, we propose diagram describing the different steps required for the establishment of an offloading scenario. As we can see in Figure 3, the pull scenario requires a few extra steps compared to a push scenario. According to Wikipedia description [36], *push* describes a style of Internet-based communication where the request for a given transaction is initiated by the publisher (or central server). It is contrasted with *pull*, where the request for the transmission of information is initiated by the receiver (or client).

We consider that, in the push scenario, the server providing content knows in advance the list of users to whom the content is intended. Thus, the content server sends to the MOTO framework the content, the list of recipient users and their respective SLA. From that moment, the different MOTO blocks (grouped in the *Offload* box) can implement the offloading mechanism. On the other hand, in the case of a pull scenario, the content server can not know a priori the list of users who have requested one same content. Thus, it is necessary to establish, within the MOTO architeture an element allowing identification of similar requests (the *Request analyzer* box) to identify users to whom the same content should be sent. From there, the same mechanism used in the push scenario (*Offload*) is established. If the request analyzer block does not identify similar content, then this latter is distributed according to the conventional method currently used by cellular networks.

In the remaining part of this section, we provide a complete description of the *offloading* box represented in Figure 3. This description is provided through a short summary of the different use cases detailed in deliverable *D2.1.1*, the description of the actors and their roles in the different use cases, the list of the scenario and architecture requirements, also extracted from deliverable *D2.1.1*, and finally, a detailed description of the designed

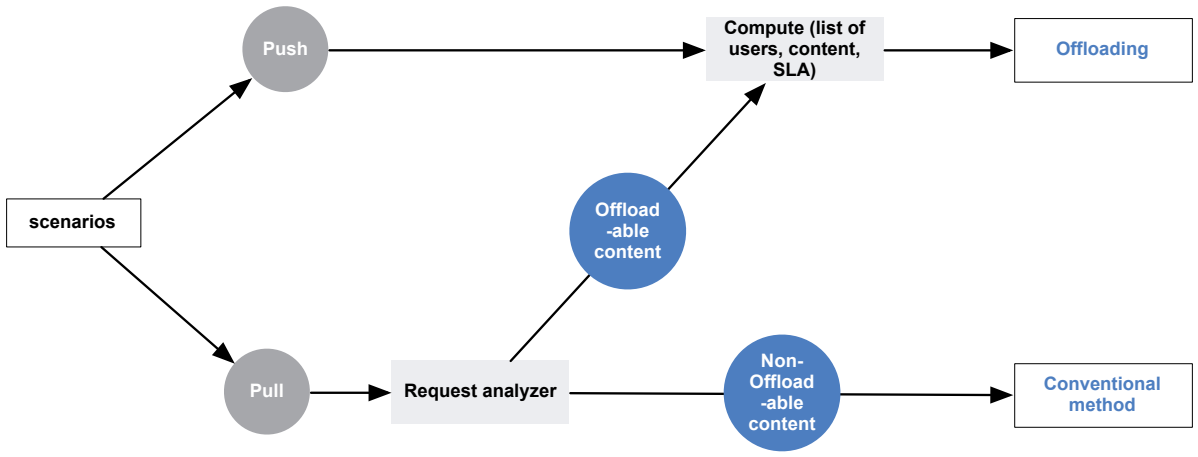


Figure 3: Involved mechanisms depending on push or pull scenario.

architecture. For this latter part, concerning the description of the architecture, we have proceeded as follows:

- We first provide, in Figure 4, the system architecture of the MOTO platform.
- Second, we describe in detail each block composing the architecture.
- Then, we provide for each use case a figure containg the flow of actions between the different blocks to run the whole lifecycle of the use case. This detailed description of every use case allows the reader to completely understand the purpose and functioning of every component of the architecture.
- Finally, we present precisely how the suggested MOTO architecture will be mapped on top of a real mobile/Wi-Fi operators.

The other parts of Figure 3, which are not addressed in this document, are considered as follows:

- Request analyzer: In the case of a pull scenario, this module is in charge of determining if the requested content is eligible to the offloading process or not. The design of this module will be addressed in the scope of *WP3*.
- Compute the list of content, users, SLA: If a content is offloadable, this module will generate the list of users that have requested it, their SLA, and their role in the dissemination of the content. This module will be considered within *WP4*.
- Conventional method: That is the method used nowadays in telecommunications to respond to a requested content, without any offloading process and it represents the default method to apply to disseminate content without any offloading process. Obviously, it will not be considered within the FP7-MOTO project.

4.1 Use case summary

The use cases studied in the MOTO project constitute a very large set. Therefore, the challenge in identifying the scenarios that are to be addressed is to capture the major dynamics that are of interest in deploying MOTO systems. Towards this end, a scenario space has been proposed that spans five dimensions to fully characterise any offloading scenario considered.These dimensions are (i) Network Benefit, (ii) Mobility, (iii) QoS, (iv) End Actors, and (v) Push/Pull implications.[1] The network benefit characterizes the system in terms of contribution to resource efficiency, whether the system is coverage limited, capacity limited (or both). The mobility characterises whether it involves users on the go, users that occasionally move, or users that do not move at all. The QoS dimension refers the delay tolerance of the application to be run by MOTO, and the End Actor dimension determines whether the recipient of the service is an end-user or a machine. Finally, the Push/Pull dimension determines if the content delivery is driven by user or the network.

Following this scenario space classification for offloading services, several scenarios corresponding to different combinations of dimension values could be produced. Based on business potential, MOTO has assigned a high level of precedence to the following three use cases:

1. Medium-Big crowds. Serving a large number of users during the same time period and in a relatively limited area has always been a major challenge to mobile operators. This use case covers medium-big crowds in museums, events, shopping malls, where MOTO aim is to support content sharing reducing the network load, provide Internet access to devices outside coverage of LTE or WiFi networks.

2. Small crowds. This use case is focused on service provisioning in spaces which gather smaller crowds, such as buses, trains, airports. Where MOTO aim is to support specific mobility and location based service requirements.

3. Vehicular. The car industry is witnessing a major business shift from a commodity model towards a service model. Offering new services to car users (driver and passengers) is a key requirement, which demand improved communications systems. MOTO aim is to support ad-hoc service delivery within vehicular environments.

For each of the use cases some scenarios have been proposed as an example. The following table lists these scenarios associated to each use case:

Use case	Scenario Title	Network Benefit	Mobility	QoS	End Actors	Push / Pull

[1]The mobility characterizes whether it involves users on the go (nomadic), users that occasionally move (mobility), or users that do not move at all (quasi-static).

1	Mobile customers accessing the web page of a shopping centre	Both	Nomadic	Medium - High delay tolerance	End user	Both
	Internet access proxing in a congested/no coverage mobile network	Both	Nomadic	Medium delay tolerance	End user	Pull
	Energy-saving Data dissemination with Offloading in Crowds for day-by-day uses (Augmented reality application in a crowded museum)	Capacity	Nomadic	Medium - High delay tolerance	End user	Both
	Energy-saving Data dissemination with Offloading in Crowds to handle peak of data traffic demands	Capacity	Nomadic	Medium - High delay tolerance	End user	Both
2	Expanded Coverage and 3G Offloading	Both	Nomadic	Medium delay tolerance	End user	Pull
	Content dissemination based on payment system	Capacity	Mobile	Low - Medium delay tolerance	End user	Pull
3	Vehicle Fleet Management	Capacity	Mobile	High delay tolerance	Machines	Both
	Vehicle Fleet Management	Capacity	Mobile	Low - Medium delay tolerance	Machines	Pull
	Enhancing Traffic Efficiency through Cooperative V2X Communication Systems	Coverage	Mobile	Low - Medium delay tolerance	Machines	Push

4.2 Actors and roles

The actors involved in MOTO are varied and some of them are dependent on the different scenarios outlined in D2.1. Nevertheless, all of them have the following common actors:

- - End users' smart-phones or vehicles, equipped with the MOTO Application for compliance with MOTO Services, including MOTO identity credentials.
- - Network access providers (Wi-Fi, LTE) that constitutes the MOTO Network Service infrastructure.
- - Service Providers Radio Access and Core Network infrastructure, part of MOTO Network Service.
- - MOTO Platform that provides opportunistic MOTO Services for MOTO Clients.
- - Requested content.

4.3 Requirements

This section provides a list of MOTO requirements, which have been collected based on the MOTO use-cases provided in Section 2 of the D2.1. This is a relatively limited list of requirements, which however provides clear boundaries on what the MOTO Platform, the MOTO clients and the MOTO Services are required to do to cover the scenarios described before.

Requirement ID	Description
R - 1	The MOTO Platform MUST be able to monitor and determine what clients are participating and can consume MOTO Services in a certain location and time.
R - 2	The MOTO Platform MUST be able to monitor and determine the fraction of time opportunistic clients are active in the offloaded opportunistic network basing on evolving network conditions, client location, client stored content, etc.
R - 3	The MOTO Platform MUST be able to monitor the performance of provided MOTO Services (e.g., latency, energy consumption, capacity gained through offloading, alarms, etc.), and automatically re-configure the MOTO Services (e.g., the data dissemination protocols) accordingly.
R - 4	The MOTO Platform MUST make available performance information for the MOTO Service provider.
R - 5	The MOTO Platform MUST allow direct communication among MOTO opportunistic clients for MOTO Services provision. The operator MUST NOT force specific opportunistic clients to communicate directly, but opportunistic clients MUST be able to self-organize direct communications.

R - 6	The MOTO Platform MUST allow MOTO Service provider to (re-)allocate the available radio resources when the opportunistic communication is not feasible.
R - 7	The MOTO Platform MUST verify the reputation (acceptable historic trust profile) of users before providing them access to the MOTO Services
R - 8	The MOTO Platform SHOULD be able to implement relevant accounting procedures on seed clients, for what concerns the communications occurring over the cellular infrastructure.
R - 9	The MOTO Platform / MOTO network service SHOULD be able to verify the termination of the link.
R - 10	The MOTO Applications MUST allow MOTO clients to decide whether to participate or not in a MOTO offloading service at a certain point or location.
R - 11	The MOTO Application MUST allow MOTO clients setting their QoE expectations.
R - 12	The MOTO Application MUST allow opportunistic clients to resume content downloading from the WAN (i.e. when the MOTO Service is not anymore available).
R - 13	Even when the MOTO Service is available and correctly functioning, the MOTO Platform MUST implement a control mechanism which provides an upper bound for the content delivery time (i.e., when the opportunistic network is not able to deliver the required content within a certain delay, a backup solution based on the WAN network MUST be available).
R - 14	MOTO Application MUST guarantee privacy of user's data stored in the UE.
R - 15	The MOTO Application MUST request MOTO clients to authenticate before start using MOTO Services.
R - 16	MOTO Application SHOULD enable users to define connection features such as access rights, encryption and signature.
R - 17	The client-pair association MUST be secure, including authentication, encryption and signature when necessary.
R - 18	Clients MUST interchange their credentials so that they can validate each one's real identity in order to establish a connection.
R - 19	Clients MUST be able to send trust feedback about the other clients to the MOTO Platform
R - 20	The system MUST gather historical trust profiles from all clients that have already used MOTO Services
R - 21	MOTO Application SHOULD allow clients to share their resources.

R - 22	When opportunistic client reconnects to MOTO client from regular cellular transmission, opportunistic client's session SHOULD continue seamlessly (IP address preservation).
R - 23	A MOTO Platform SHOULD allow integration / interoperability with other MOTO Platforms managed by other service providers to enable MOTO Service roaming.
R - 24	MOTO Platform SHOULD be able to collect the necessary information to allow billing processes.

4.4 Architecture

Here, we provide, in detail, the required components that allow offloading of the network. We describe the different building blocks, then the software.

The building blocks of the MOTO architecture are shown in Figure 4. In this section, we describe the role of each block. The MOTO platform can be integrated either inside or outside an operator network and interacts with some elements of the operators networks. Whatever the technology used (LTE/WiFi/802.11p), operators' networks typically include the following elements:

- access part of the network, including base stations where user terminals get attached: e-UTRAN (Evolved Universal Terrestrial Radio Access Network) for an LTE network, 802.11a/b/g or 802.11p access points for WiFi or road infrastructure operators respectively.
- localization (LOC): some information about clients' location are available in operator networks. In an LTE network, the HSS (Home Subscriber Server) and MME (Mobility Management Entity) elements manage subscription and localization information (Cell). In WiFi networks, the clients can be localized, and a topology view can be deduced from connectivity information available at the access points (Topo).
- authentication and accounting : authentication functionalities are also common in any operator network infrastructure.
- network monitoring and management tools: allows the operator to monitor the performances (e.g. detect congestion) and manage its network.

Some of these elements will provide information to the MOTO Core services through an API called *Infrastructure API*. This API is typically used to share information regarding localization and authentication of clients, as well as network capabilities and status.

To allow an operator to offload traffic from its network, the MOTO Architecture includes additional functionalities implemented by building blocks providing the Core MOTO Services. These MOTO Services are responsible for coordinating the dissemination of a content. Any application can sollicitate the MOTO platform to deliver a content while offloading the network(s) used by application subscribers, using the *Application*

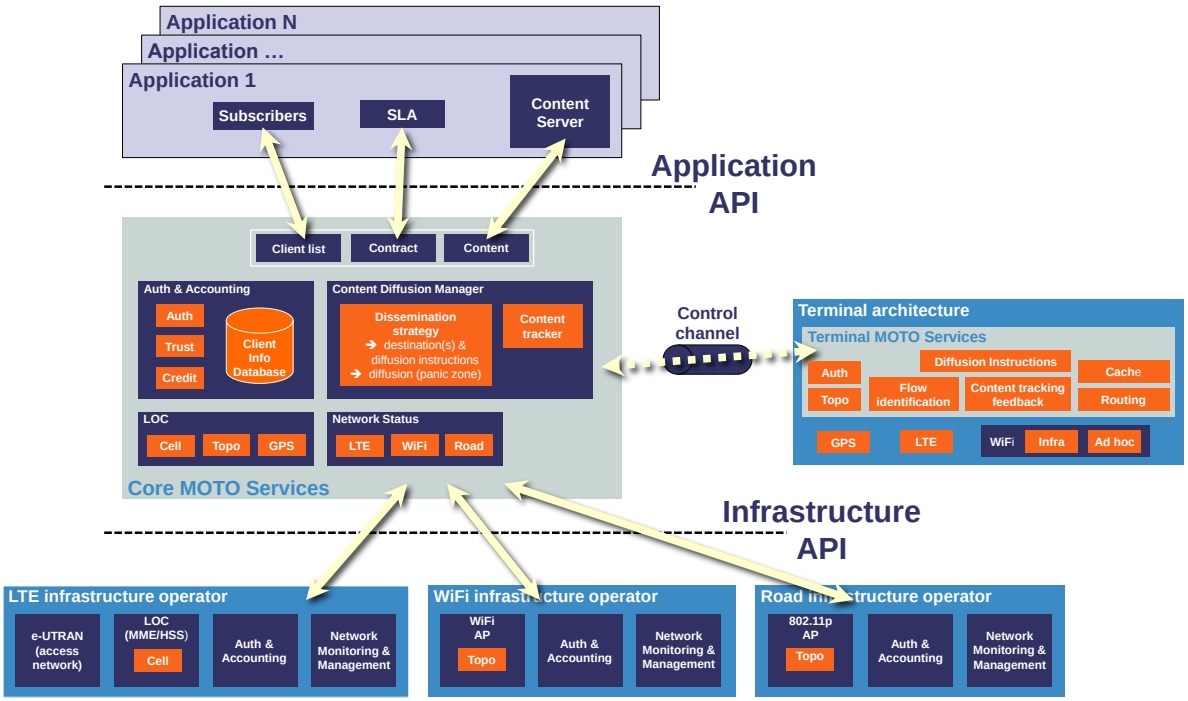


Figure 4: MOTO architecture building blocks and APIs.

API. Through this API, an application sollicitates MOTO by giving the following inputs: the content to disseminate, the list of clients interested in this content (subscribers), and service constraints to be met (SLA, e.g. specifying delay tolerance). From these inputs, the **Core MOTO services** deal with offloading thanks to the following building blocks:

- *client list, contract, content*: to perform offloading, the MOTO Architecture manages the delivery of a content to many clients according to the contract defining conditions for content delivery (e.g. maximum delay for delivery). The list of clients, the conditions that must be fulfilled (e.g. allowed delay tolerance), and the content to disseminate are given by any application that sollicitates the MOTO Services through the *Application API*. The content itself, or a link to the content hosted at the application level can be provided to MOTO.

- *LOC*: the *LOC* component in the operator MOTO Architecture deals with information on the localization of MOTO clients. Such information can be gathered using the *Cell* information provided either by operator networks (Cell information in LTE, topological information on WiFi access points), or by the "Topo" MOTO service running on users' terminals (to get *GPS* or *topological* information monitored on WiFi interfaces).

- *Content Diffusion Manager*: this functional block includes two elements that are the core of the offloading process:

  - *Dissemination strategy*: this function is responsible for piloting the offloading process. It determines, from the list of clients that require the content and from localization and topological information gathered, the dissemination strategy to be applied (e.g. deliver the content to clients A, B and C through the LTE network and ask them to relay the content in their neighbourhood using WiFi with specific routing policies). The dissemination process is monitored (cf. Content tracker) and the dissemination strategy can be updated during the dissemination process. After a given amount of time (panic zone), the traditional diffusion through the cellular network might be used to serve the content to all clients that did not receive it by other means.
  - *Content tracker*: this component receives acknowledgments sent by MOTO clients (cf. Content tracking feedback) when they receive the content. This element thus plays the role of monitoring the content dissemination process.

- *Auth & Accounting*: this module includes authentication, trust and credit management functionalities, as well as a database in which MOTO specific information on clients is maintained (trust and reputation indicators, credentials status).

- *Network Status*: this module allows to maintain information on the status of the available network infrastructures (e.g. remaining capacity for each network) that can be used to elaborate a dissemination scheme. Network status information can be requested by this MOTO component through the *Infrastructure API*, either on a regular basis or only when required.

The MOTO architecture also relies on some elements on the client terminal side:

- LTE: this element allows the terminal to connect to an operator's LTE access network.

- WiFi: this element gives WiFi connectivity to the terminal, either in infrastructure mode, for communications through an access point, and in ad hoc mode (direct communications between terminals).

- GPS: this element allows positionning of the terminal. Localization information is collected by the *LOC* module of the Core MOTO Services.

In addition to these existing blocks, the MOTO Architecture includes **Terminal MOTO Services** represented by several building blocks in the client terminal:

- *Flow identification*: this module is in charge of identifying the flows that are related to MOTO Services in order to process them differently from traditional flows. In fact, receiving MOTO flows might require generating a content tracking feedback, caching and/or relaying it according to routing policies given by the Core MOTO Services (cf. dissemination strategy function in the *Content Diffusion Manager* building block).

- *Topological information* (Topo): this element uses connectivity data to maintain topological information that can be sent to the associated *LOC* module of the Core MOTO Services.
- *Content tracking feedback*: this element is in charge of advertising the Core MOTO Service upon reception of a MOTO content (cf. Content tracker function in the Content Diffusion Manager block). It can also play a role for sending trust reports.
- *Diffusion Instructions*: this element receives instructions from the Content Diffusion Manager (diffusion and/or routing policies to apply).
- *Cache*: this module allows to store MOTO content locally so that it can be directly delivered to other MOTO clients later.
- *Routing*: this module is in charge of executing the routing policies given by the Content Diffusion Manager according to the role of the client and the content dissemination strategies.
- *Auth*: this module is sollicitated for mutual authentication of MOTO clients (for ad hoc communications).

The MOTO Architecture described above is designed to enable efficient offloading of a primary network (e.g. cellular) by exploiting the direct ad hoc connectivity between clients or an alternative infrastructure (e.g. WiFi).

4.5 Instantiation of the MOTO architecture for use cases

In this section, we explain how the MOTO architecture described above can be instanciated to reach the offloading goal for several use cases. We differenciate the elements that are relative to the application from those that play a key role in the offloading process. The later are the building blocks identified in the core MOTO architecture.

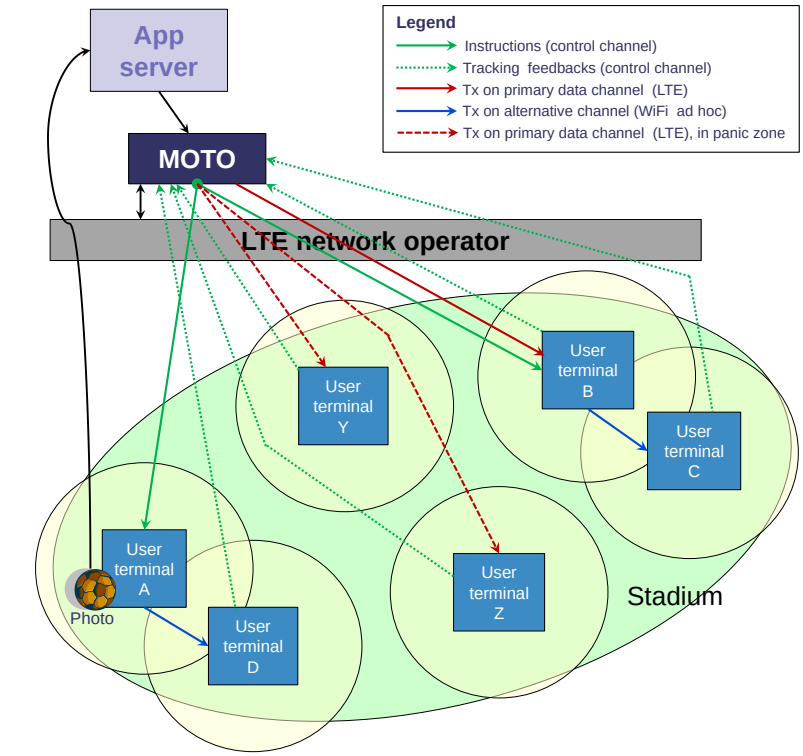
Note that some scenarios later in this section manage the offloading decision operations centrally while others delegate this decision to end users/terminals. Although decentralised decision seems more appropriate, especially for intuitive scalability reasons, we decided to also treat centralized decision scenarios. Especially because, at the best of our knowledge, no previous study makes it clear that centralized decisions are not scalable.

4.5.1 Example use case: photo sharing in a stadium

We study here a first use case as an example: photo sharing in a stadium. We describe how the MOTO architecture building blocks are used for this use case. This photo sharing scenario is interesting because:

- it involves users that subscribed to a photo sharing Internet service, similar e.g. to the "photo flow" Apple application. When a user takes a picture, this picture is sent to the application server who is responsible for sending it to other subscribers (here, we consider subscribers in the same area). Currently, i.e. without MOTO, this application server would use many network resources in operators' networks to disseminate this content.
- it shows that a content (photo taken by one user) is sent to an application server (pull), independently from MOTO services, and then the application server delegates to the MOTO Services the coordination of the content dissemination among several subscribers (push).

We consider several users in a stadium. As represented by circles in Figure 5, some of them can communicate directly (A and D, B and C) while others are isolated (Y, Z).



l

Figure 5: Global picture for the use case on photo sharing in a stadium.

We consider that user A shares a picture that must be sent to all other users. The photo sharing service provider collaborates to offload operators' networks through the MOTO platform. So, the application server does not deal itself with the dissemination process but delegates this task to the MOTO platform. Black arrows in Figure 5 depict interactions between actors, and colored arrows give details on the offloading process

performed by MOTO, given as an example and described above (color-code is explained in the legend).

The photo sharing application server gives inputs (list of clients, content to disseminate, maximum delay to disseminate the content) to the MOTO platform. From these inputs, the MOTO Services coordinate the dissemination according to the sequence represented in Figure 6 (colors refer to the architecture building blocks).

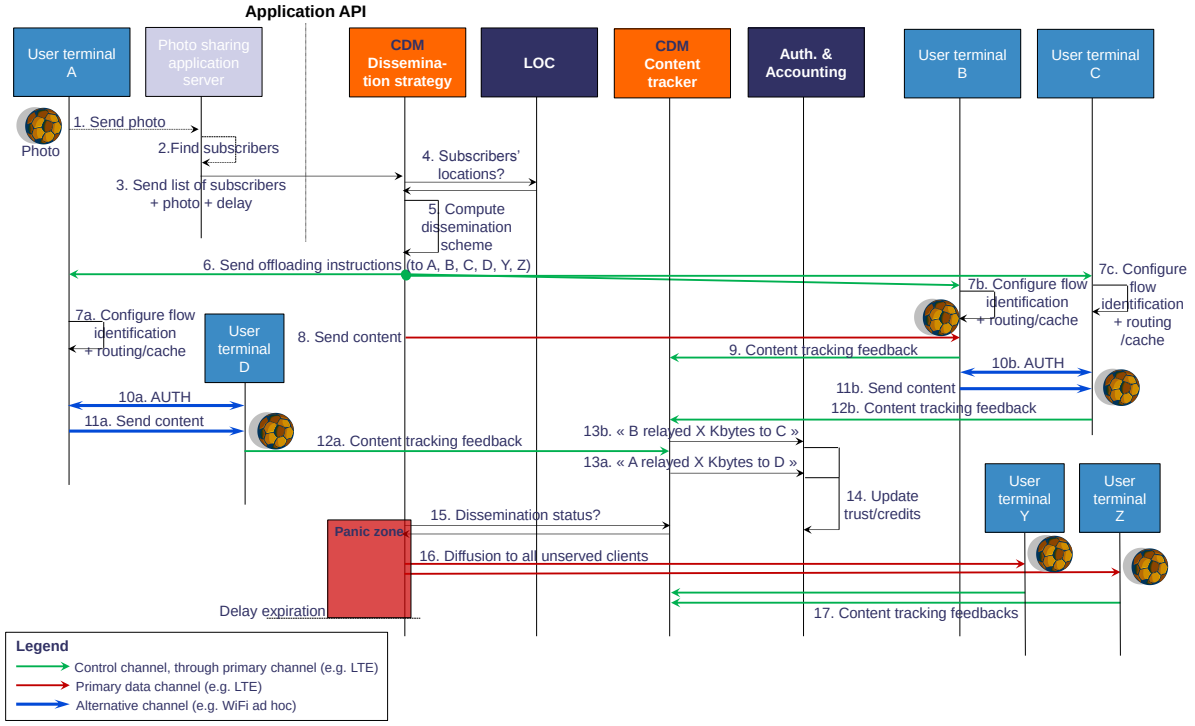


Figure 6: Sequence of interactions between external and internal MOTO elements for the use case "photo sharing in a stadium".

Step-by-step. Explanation of flow chart shown in Figure 6. The legend provides the meaning of arrows' colors.

1. a client of the "photo sharing in a stadium" Internet service takes a picture during a football match with his terminal ("User terminal A"). This photo is sent to the photo sharing application server, through the primary communication channel (e.g. LTE network).

2. the photo sharing application server identifies other local subscribers interested in this content.

3. the photo sharing application server delegates the dissemination of this photo to the MOTO Services. More precisely, it uses the *Application API* to give inputs (list

of subscribers, content to send, maximum delay) to the "Dissemination strategy" functional block of the MOTO Content Diffusion Manager (CDM), in charge of coordinating the dissemination of this content.

4. the *Dissemination Strategy* block gathers information on susbcribers' location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Users' terminals may also feed the LOC module by sending their GPS position).

5. from the information available, the *Dissemination Strategy* function of the CDM elaborates a strategy for disseminating the content. For instance, the resulting strategy can consists in:

   - asking "User terminal A" to send the photo in its neighbourhood ("User terminal D" will be reached) using WiFi ad hoc interface,
   - sending the photo to "User terminal B" through the primary data channel (e.g. LTE) and asking this terminal to relay the photo in its neighbourhood ("User terminal C" will be reached) through its WiFi ad hoc interface.

6. the *Dissemination Strategy* block sends offloading instructions to all user terminals involved in the dissemination process (even those that are potentially not interested in the content but can be used as relays). Here, user terminals A, B, C (represented) and D, Y, Z (not represented) receive offloading instructions. Such instructions include the description of the data flow to be generated/received, the list of nodes the content must be sent to, and the routing (which interface to use) and caching (keep in local cache or not) instructions.

7. according to the offloading instructions:

   (a) "User terminal A" prepares the flow to be sent through its WiFi ad hoc interface,

   (b) "User terminal B" configures its flow identification module to capture the flow it is going to receive from the CDM through the primary channel (e.g. LTE) and trigger MOTO-specific treatment (so that content tracking feedback will be sent and the flow will be relayed).

   (c) "User terminal C" configures its flow identification module to capture the flow it is going to receive and trigger MOTO-specific treatment (so that content tracking feedback will be sent).

   (d) User terminals D, Y, Z configure their flow identification module to capture the flow they are going to receive and trigger MOTO-specific treatment (so that content tracking feedback will be sent).

8. the *Dissemination Strategy* block actually sends the photo to "User terminal B" the primary channel (e.g. LTE).

9. when receiving the photo, "User terminal B" (more precisely, the *Content tracking feedback* block) sends a feedback to acknowledge the reception of the content to the *Content tracker* module of the Content Diffusion Manager.

10. authentication then takes place between user terminals that participate in the dissemination process so that the content is relayed securely:

    (a) authentication between "User terminal A" and "User terminal D",

    (b) authentication between "User terminal B" and "User terminal C"

11. the content is actually relayed through direct WiFi ad hoc connections:

    (a) from "User terminal A" to "User terminal D",

    (b) from "User terminal B" to "User terminal C".

12. user terminals send a content tracking feedback message to acknowledge the reception of the photo to the *Content tracker* block of the Content Diffusion Manager. Such a feedback message can include information about who the content were received from.

    (a) "User terminal D" sends a content tracking feedback message to the *Content tracker*,

    (b) "User terminal C" sends a content tracking feedback message to the *Content tracker*.

13. depending on the information contained in feedback messages, the *Content tracker* can report relaying activities to the Authentication & Accounting module:

    (a) the *Content tracker* reports relaying activities of "User terminal A" to the Auth & Accounting module,

    (b) the *Content tracker* reports relaying activities of "User terminal B" to the Auth & Accounting module.

14. as a result, the Authentication & Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

15. the *Dissemination Strategy* module regularly checks the dissemination status by requesting the *Content tracker*. (Not represented: the dissemination strategy can be updated, e.g. new offloading instructions and the content can be directly sent to other clients. Steps 4 to 14 are thus repeated). When entering in the panic zone (before dissemination delay expires) the *Dissemination Strategy* module checks the dissemination status.

16. if some clients did not received the content when entering the panic zone, the *Dissemination Strategy* block triggers the diffusion of the content to all those clients through the primary communication channel (e.g. LTE).

17. those clients finally acknowledge the reception of the content to the *Content tracker* block of the Content Diffusion Manager.

4.5.2 Medium/Big Crowds Scenarios

4.5.2.a Scenario 1: Mobile customers accessing the web page of a shopping center

In this scenario, the goal is to take benefit of the ad hoc connectivity between some MOTO clients to access a shopping mall's website through other MOTO clients instead of through the WiFi or LTE network infrastructure (cache/proxy).

Application of scenario 1: access to the shopping mall website. The Shopping mall's server collaborates to offload operators' networks through the MOTO platform. So, the server does not deal itself with the dissemination process but delegates this task to the MOTO platform. Thus, when any MOTO subscriber enables the MOTO service in its terminal and authenticates in the MOTO platform, it is provided with the offloading instructions to connect to the shopping mall's website.

Step-by-step. Explanation of flow chart shown in Figure 7:

1. The shopping mall's server provides to the MOTO platform, through the *Application API*, the dissemination strategy it must be followed when MOTO subscribers connect to the service when staying in the shopping mall.

2. A client ("User Terminal A") of the MOTO service authenticates into the MOTO system against Authentication & Accounting module.

3. The client ("User Terminal A") of the MOTO service receives the authentication response.

4. The Authentication & Accounting module notifies the CDM Dissemination strategy module that a new user has authenticated into the MOTO Service.

5. The Dissemination Strategy block gathers information of the subscriber's location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Users' terminals may also feed the LOC module by sending their GPS position).

6. The Dissemination Strategy block requests the Content Tracker module if any user has previously downloaded shopping mall's website.

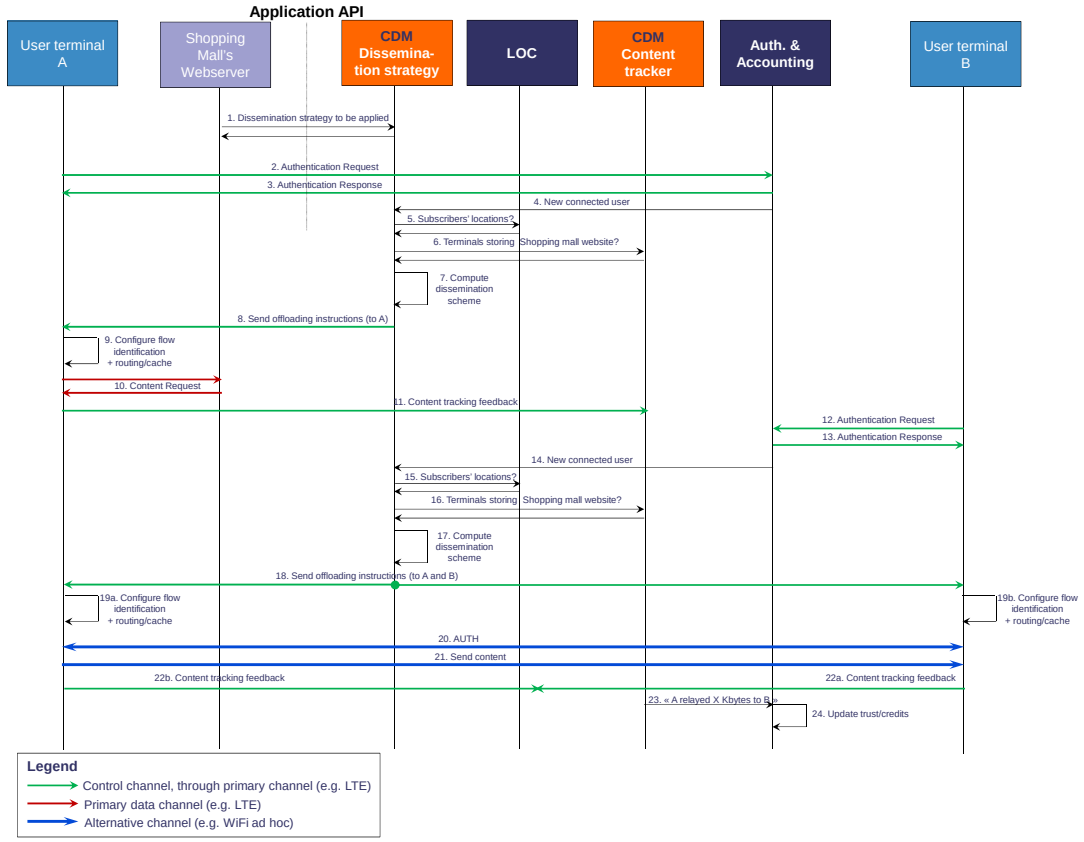


Figure 7: Sequence of interactions between external and internal MOTO elements for the use case "Mobile customers accessing the web page of a shopping center".

7. From the information received from the LOC and Content Tracker modules, the Dissemination Strategy function of the CDM elaborates a strategy for disseminating the content. For instance, the resulting strategy can consist in asking "User Terminal A" to directly connect to the shopping mall's server through the LTE connection to access to the shopping mall's website and caching that content.

8. The Dissemination Strategy block sends offloading instructions to all user terminals involved in the dissemination process (even those that are potentially not interested in the content but can be used as relays). Here, only "User Terminal A" receives offloading instructions since at the moment is the only terminal with MOTO service enabled. Such instructions include the description of the data flow to be generated/received, the list of nodes the content must be sent to, and the routing (which interface to use) and caching (keep in local cache or not) instructions.

9. According to the offloading instructions "User terminal A" prepares the flow to obtain the website from the Internet through its LTE connection and keeps it in the cache.

10. The "User Terminal A" requests the shopping mall's website and receives the requested content.

11. When receiving the content, "User terminal A" (more precisely, the Content tracking feedback block) sends a feedback to acknowledge the reception of the content to the Content Tracker module of the Content Diffusion Manager.

12. A new user ("User Terminal B") of the MOTO service authenticates into the MOTO system against Authentication & Accounting module.

13. The client ("User Terminal B") of the MOTO service receives the authentication response.

14. The Authentication & Accounting module notifies the CDM Dissemination strategy module that a new user has authenticated into the MOTO Service.

15. The Dissemination Strategy block gathers information on subscribers' location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Users' terminals may also feed the LOC module by sending their GPS position).

16. The Dissemination Strategy block requests the Content Tracker module if any user has previously downloaded shopping mall's website.

17. From the information received from the LOC and Content Tracker modules, the Dissemination Strategy function of the CDM elaborates a strategy for disseminating the content. For instance, the resulting strategy can consists in asking "User Terminal A" to send the content in its neighborhood ("User Terminal B" will be reached) using WiFi ad hoc interface.

18. The Dissemination Strategy block sends offloading instructions to all user terminals involved in the dissemination process (even those that are potentially not interested in the content but can be used as relays). Here, user terminals A and B receive offloading instructions. Such instructions include the description of the data flow to be generated/received, the list of nodes the content must be sent to, and the routing (which interface to use) and caching (keep in local cache or not) instructions.

19. According to the offloading instructions:

    (a) "User terminal A" prepares the flow to be sent through its WiFi ad hoc interface

    (b) "User terminal B" configures its flow identification module to capture the flow it is going to receive and trigger MOTO-specific treatment (so that content tracking feedback will be sent).

20. Authentication then takes place between user terminals that participate in the dissemination process so that the content is relayed between them securely.

21. The content is relayed through direct WiFi ad hoc connections from "User Terminal A" to "User Terminal B".

22. User terminals send a content tracking feedback message to acknowledge the reception of the content to the Content Tracker block of the Content Diffusion Manager. Such a feedback message can include information about who the content were received from/to.

23. Depending on the information contained in feedback messages, the Content Tracker can report relaying activities to the Authentication & Accounting module. The Content Tracker reports relaying activities of "User terminal A" to the Authentication & Accounting module.

24. As a result, the Authentication & Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

4.5.2.b Scenario 2: Internet access proxing in congested/no coverage mobile network

In this scenario, the goal is to take benefit of the connectivity of some MOTO clients to provide Internet services to other MOTO clients while the mobile network is congested or does not cover all clients.

Application of scenario 2 : delivery of Internet services.

The aim of this scenario is to expand coverage or to make other terminals behave as proxies in order to reduce the traffic load in a congested network environment. In this case, there could not be an intermediate application in charge of providing the MOTO Platform subscribers' information or the requested content information since it could not be predicted which content the end user is going to request. Thus, in these situations, the LTE operator would be in charge of, through the *Application API*, providing the dissemination strategy that must be implemented in the different possible situations (no coverage, congested network...).

Step-by-step. Explanation of flow chart shown in Figure 8:

1. A client ("User Terminal A") of the MOTO service authenticates into the MOTO system against Authentication & Accounting module.

2. The client ("User Terminal A") of the MOTO service receives the authentication response.

3. The Authentication & Accounting module notifies the CDM Dissemination strategy module that a new user has authenticated into the MOTO Service.

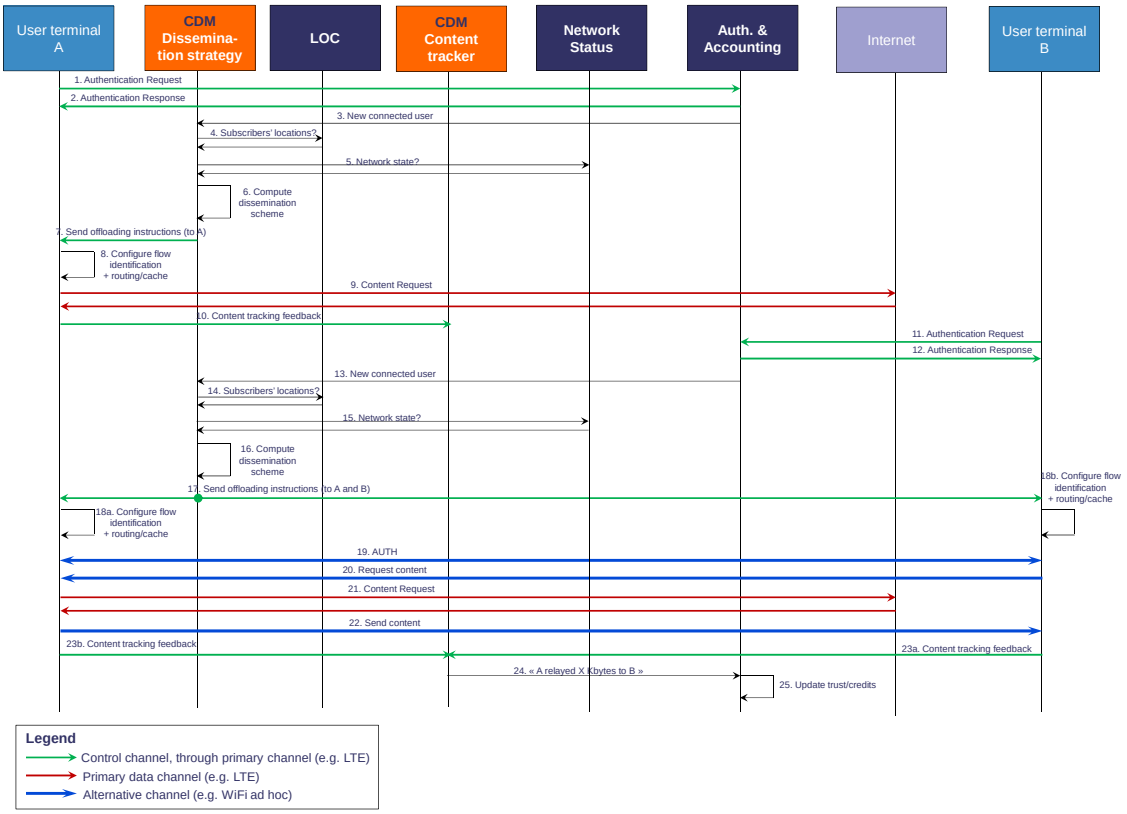


Figure 8: Sequence of interactions between external and internal MOTO elements for the use case "Internet access proxing in congested/no coverage mobile network".

4. The Dissemination Strategy block gathers information on subscribers' location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Users' terminals may also feed the LOC module by sending their GPS position).

5. The Dissemination strategy block of the CDM module gathers information on network congestion from the Network Status module. (Not represented: through the *Infrastructure API*, the Network Status module maintains some congestion information available in operators' networks).

6. From the information received from the LOC and Network Status modules, the Dissemination Strategy function of the CDM elaborates a strategy for disseminating the content. For instance, the resulting strategy can consists in asking "User terminal A" to directly connect to the Internet through the LTE connection and caching the downloaded content. Additionally, it will be notified that it should be listening to other potential MOTO users who need to access to the network through it.

7. The Dissemination Strategy block sends offloading instructions to all user terminals

involved in the dissemination process (even those that are potentially not interested in the content but can be used as relays). Here, "User Terminal A" receives offloading instructions. Such instructions include the routing (which interface to use) and caching (keep in local cache or not) instructions.

8. According to the offloading instructions "User terminal A" prepares the flow to connect to the Internet through its LTE connection and keeps all the downloaded content in the cache.

9. The "User Terminal A" requests some content from the Internet.

10. When receiving the content, "User terminal A" (more precisely, the Content tracking feedback block) sends a feedback to acknowledge the reception of the content to the Content Tracker module of the Content Diffusion Manager.

11. A new user ("User Terminal B") of the MOTO service authenticates into the MOTO system against Authentication & Accounting module. In this case we assume that the user terminal has LTE coverage and authenticates in the MOTO Platform through this channel.

12. The client ("User Terminal B") of the MOTO service receives the authentication response.

13. The Authentication & Accounting module notifies the CDM Dissemination Strategy module that a new user has authenticated into the MOTO Service.

14. The Dissemination Strategy block gathers information on subscribers' location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Users' terminals may also feed the LOC module by sending their GPS position).

15. The Dissemination Strategy block of the CDM module gathers information on network congestion from the Network Status module. (Not represented: through the *Infrastructure API*, the Network Status module maintains some congestion information available in operators' networks).

16. From the information received from the LOC and Network Status modules, the Dissemination Strategy function of the CDM elaborates a strategy for disseminating the content. For instance, the resulting strategy can consists in the following: as the "User Terminal B" is next to the "User Terminal A", who accesses the Internet directly through the LTE network, and because the network is congested, the "User Terminal B" must connect to the Internet through "User Terminal A" using WiFi ad hoc interface.

17. The Dissemination Strategy block sends offloading instructions to all user terminals involved in the dissemination process. Here, user terminals A and B receive offloading instructions. In the case of "User Terminal A" these instructions include the

list of nodes for which it must behave as a proxy, the routing (which interface to use) and caching (keep in local cache or not) instructions. For the "User Terminal B" these instructions include the user terminal it must be connected through and routing and caching instructions.

18. According to the offloading instructions:
    (a) "User terminal A" prepares the flow to be received through its WiFi ad hoc interface and sent through its LTE interface
    (b) "User terminal B" configures its flow identification module to capture the flow it is going to send/receive and trigger MOTO-specific treatment (so that content tracking feedback will be sent) through "User Terminal A".
19. Authentication then takes place between user terminals that participate in the dissemination process so that the content is relayed securely.
20. The content request is sent through direct WiFi ad hoc connections from "User Terminal B" to "User Terminal A".
21. "User Terminal A" relays the content request through its LTE interface to the Internet.
22. The content response is sent through direct WiFi ad hoc connections from "User Terminal A" to "User Terminal B". Both of them store the content in the cache.
23. User terminals send a content tracking feedback message to acknowledge the reception of the content to the Content Tracker block of the Content Diffusion Manager. Such a feedback message can include information about who the content were received to/from.
24. Depending on the information contained in feedback messages, the Content Tracker can report relaying activities to the Authentication & Accounting module. The Content Tracker reports relaying activities of "User Terminal A" to the Authentication & Accounting module.
25. As a result, the Authentication & Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

In the flow chart presented in Figure 8, one specific situation is missing. This situation occurs when a user terminal named C has no LTE coverage. In such case, the user terminal cannot connect to the MOTO platform for authentication through LTE interface. Thus, as User terminal A has been configured to listen for other MOTO clients, user terminal C can authenticate in the MOTO platform through it.

4.5.2.c Scenario 3: Data dissemination with offloading in crowds for day-to-day uses (augmented reality application in a crowded museum)

This scenario entails visitors in a museum, who download on their terminals a mobile guide application, which supports an augmented-reality museum visit.

Application of scenario 3 : augmented reality guide in a museum. In the case of congestion on the LTE network, which is quite likely in crowded environment like museums, the MOTO system allows the users' terminals to receive the additional multimedia content associated to artworks displayed in the museum from nearby visitors rather than remote servers. The application is not necessarily aware of what users' terminals are storing additional multimedia content, but it must be able to interact with the MOTO platform so that the latter is overall aware of the set of mobile terminals that must receive a given content within a specified maximum delay.

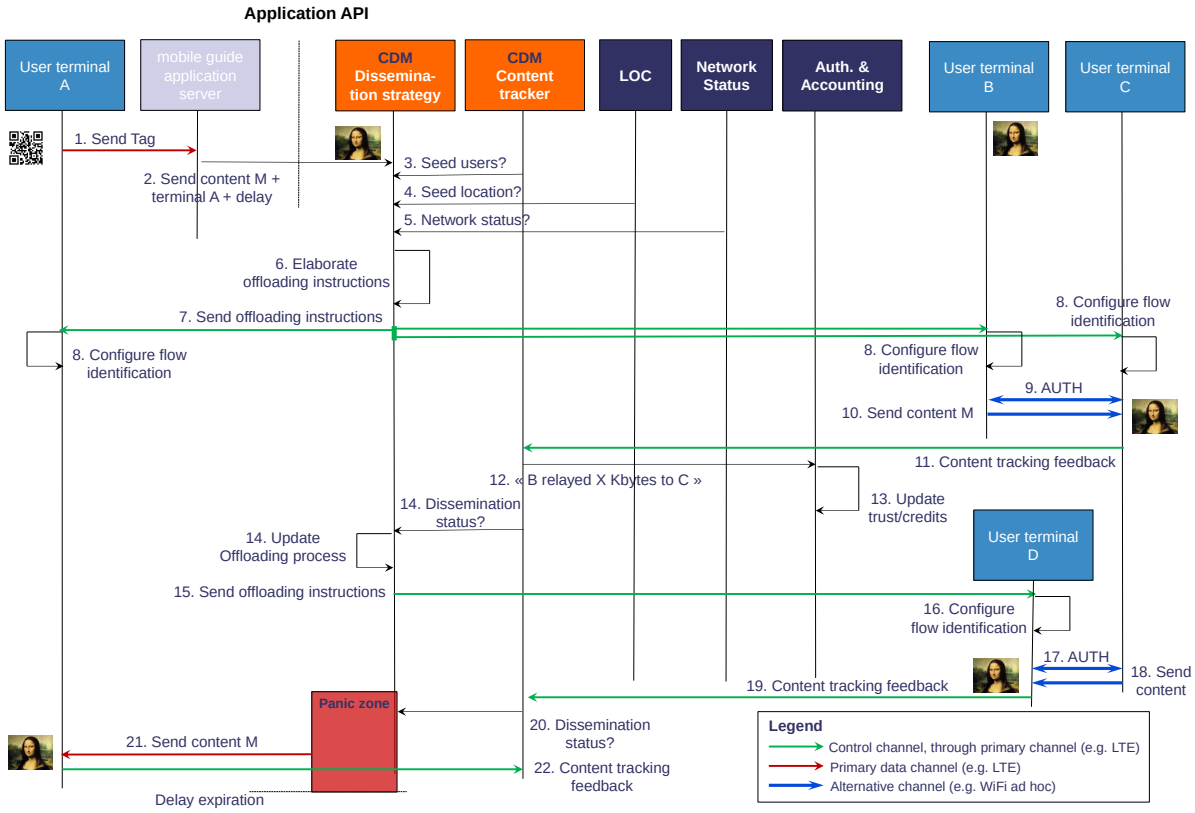


Figure 9: Sequence of interactions between external and internal MOTO elements for the use case "Augmented reality application in a crowded museum".

Step-by-step. Explanation of flow chart shown in Figure 9:

1. A client of the mobile guide application takes a picture of tag (e.g., a QR-Code) associated to an artwork in the museum ("User Terminal A"). This picture is sent to the mobile guide application server through the primary communication channel (e.g. LTE network). The server finds the additional multimedia content M associated to that tag.

2. The mobile guide application delegates the dissemination of this content M to MOTO Services. More precisely, it uses the *Application API* to give inputs (i.e., destination, content to send, maximum delay) to the Dissemination Strategy functional block of the MOTO Content Diffusion Manager, in charge of coordinating the dissemination of this content.

3. The Dissemination Strategy block gathers information on other user terminals storing content M in their local caches from the Content Tracker block of the CDM. Those terminals form the set of candidate seed users for content M (note that this set may be empty if offloading has not yet been activated for content M). Here we assume that User Terminal B is the only seed user at this specific point in time (we assume that User Terminal B had already received content M at some point in time before step 1).

4. The Dissemination Strategy block gathers information on seeds' locations from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in the operators' networks. Users' terminals may also feed the LOC module by sending their GPS position).

5. The Dissemination Strategy block gathers information about the congestion level of the primary and secondary channels of all the user terminals that still need to receive content M, which now also include "User Terminal A", from the Network Status module. This information can be replaced by aggregate information about the congestion perceived by these user terminals, such as the average congestion or some percentiles of the terminals perceiving the most congested conditions. (Not represented: through the *Infrastructure API*, the Network Status module receives information on the channel state maintained by the operators in the Network Monitoring and Management modules. User's terminals may also feed the Network Status module by sending their measurements related to the opportunistic channel).

6. From the information available, the Dissemination Strategy function of the CDM elaborates a strategy for disseminating the content. For instance, assuming, for the sake of simplicity, that "User Terminal A" is the only one that still has to receive content M at this point in time, the resulting strategy can consists in one of the following:

    - sending content M to "User Terminal A" through the primary communication channel,

- asking "User Terminal B" to relay the photo in its neighbourhood through its WiFi ad hoc interface to reach "User Terminal A", and
- C has also requested content M.

Part of the Dissemination Strategy is also identifying additional mobile nodes managed by the operator that are not necessarily interested in content M, but that must take part to the opportunistic offloading content (e.g., to enable content M to reach "User Terminal A" starting from "User Terminal B"). The identification of these terminals is based on aggregate information about the status of the network, and stochastic models about the mobility of the nodes, and the resulting expected features of the opportunistic network. Identifying the precise forwarding actions is responsibility of the user terminals activated for the opportunistic dissemination process, and not of the CDM Dissemination Strategy.

7. The Dissemination Strategy block sends offloading instructions to all user terminals involved in the dissemination process (even those that are potentially not interested in the content but can be used as relays). Here, user terminals A, B, and C (represented) receive offloading instructions. Such instructions include the description of the data flow to be generated/received, the destination(s) of the content M, the data dissemination strategy to be used (e.g., epidemic, social-based).

8. According to the offloading instructions, user terminals A, B, and C configure their flow identification modules to capture the flow they are going to receive and trigger MOTO-specific treatment (so that content tracking feedback will be sent).

9. Authentication then takes place between user terminals that participate in the dissemination process when they encounter (i.e., when the come close enough to establish a single-hop ad hoc connection) so that the content is relayed securely. In this case, authentication procedures take place between "User terminal B" and "User terminal C".

10. If the opportunistic forwarding algorithm running on User Terminals B and C decides so, the content is relayed from "User terminal B" and "User terminal C" through direct WiFi ad hoc connections.

11. "User Terminal C" sends a content tracking feedback message to acknowledge the relaying of the content to the Content tracker block of the CDM. Such a feedback message can include information about the terminal the content was received from.

12. Depending on the information contained in feedback messages, the Content Tracker block can report relaying activities of "User Terminal B" to the Authentication & Accounting module.

13. As a result, the Authentication and Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

14. The Dissemination Strategy block regularly checks the dissemination status by requesting the Content Tracker module. Steps 3 to 5 are thus repeated. Then, the Dissemination Strategy block can decide to update the dissemination strategy, thus repeating step 6.

15. During the content dissemination, a new client ("User terminal D") may send a request to the mobile guide application for the same content M (not represented). The mobile guide application delegates the dissemination of content M to the new client to MOTO Services. Then, the CDM repeats steps 3 to 5. The CDM sends offloading instructions to "User Terminal D" and, eventually, it can decide to update the dissemination strategy (not represented).

16. According to the offloading instructions, "User terminal D" configures its flow identification module to capture the flow associated to content M and to trigger MOTO-specific treatment (so that content tracking feedback will be sent).

17. "User terminal D" encounters "User Terminal C", which has content M in its cache, and authentication procedures take place between "User terminal D" and "User terminal C".

18. If the opportunistic forwarding algorithm running on user terminals D and C decides so, the content is relayed from "User terminal C" to "User terminal D" through direct WiFi ad hoc connections.

19. "User terminal D" sends a content tracking feedback message to acknowledge the relaying of the content to the Content Tracker block of the CDM. Such a feedback message can include information about the terminal the content was received from. Then, steps 12 and 13 are repeated (not represented).

20. When entering in the panic zone (before dissemination delay expires) the Dissemination Strategy module checks the dissemination status.

21. If "User terminal A" did not receive the content when entering the panic zone, the Dissemination Strategy block triggers the diffusion of the content through the primary communication channel (e.g. LTE).

22. "User Terminal A" finally acknowledges the reception of the content to the Content Tracker block of the Content Diffusion Manager.

4.5.2.d Scenario 4: Data dissemination with offloading in crowds to handle peak of data traffic demands

This scenario entails spectators watching a football match in a stadium, who are provided with an application that allows them to get picture or video clips taken from other spectators in the same stadium.

Application of scenario 4 : content sharing (pictures, videos). The MOTO system avoids that locally generated content is delivered through the LTE network, which may generate unsustainable traffic loads due to the density of users and the amount of data to upload and then disseminate in the same cell.

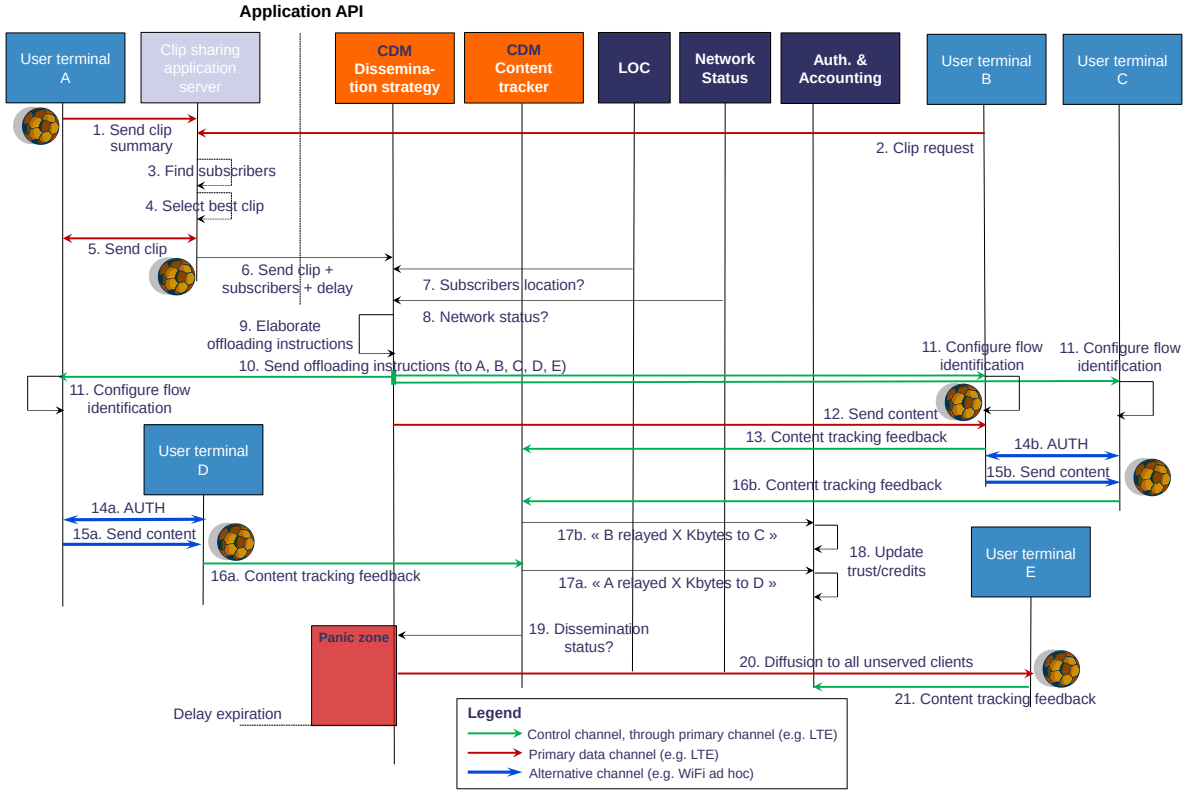


Figure 10: Sequence of interactions between external and internal MOTO elements for the use case "Video clip sharing in a stadium".

Step-by-step. Explanation of flow chart shown in Figure 10:

1. A client "User Terminal A" takes a short video clip of a penalty kick during a football match. A summary of this video clip is sent to the sharing application server, through the primary communication channel (e.g. LTE network). Note that this summary delivers a few bytes of information (e.g., image resolution, clip duration, location). Hence, the LTE network can sustain the simultaneous transmission of several of such summaries.

2. "User Terminal B" sends a request (though its primary communication channel) to the sharing application server for a video clip of the penalty kick. This request may also set minimum requirements for such clip (e.g., resolution, view angle).

3. The sharing application server identifies other local subscribers interested in the same content.

4. The sharing application server selects the video clip that best matches the subscribers' requests. Let us assume that the selected content is the clip taken by "User Terminal A", and let us denote that clip as content M.

5. The sharing application server sends a command to the mobile application running on "User Terminal A" to retrieve the full clip.

6. The sharing application server delegates the dissemination of content M to MOTO services. More precisely, it uses the *Application API* to give inputs (list of subscribers, content to send, maximum delay) to the Dissemination strategy functional block of the MOTO Content Diffusion Manager, in charge of coordinating the dissemination of this content.

7. The Dissemination Strategy block gathers information on subscribers' location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Users' terminals may also feed the LOC module by sending their GPS position).

8. The Dissemination Strategy block gathers information about the congestion level of the primary and secondary channels of the subscribers from the Network Status module (Not represented: through the *Infrastructure API*, the Network Status module receives information on the channel state maintained by the operators in the Network Monitoring and Management modules. Users' terminals may also feed the Network Status module by sending their measurements related to the opportunistic channel).

9. From the information available, the Dissemination Strategy function of the CDM elaborates a strategy for disseminating the content. For instance, the resulting strategy can consists in the following steps:

   - asking "User terminal A" to send the photo in its neighbourhood ("User terminal D" will be reached) using WiFi ad hoc interface,
   - sending the photo to "User terminal B" through the primary data channel (e.g. LTE) and asking this terminal to relay the photo in its neighbourhood ("User terminal C" will be reached) through its WiFi ad hoc interface.

10. The Dissemination Strategy block sends offloading instructions to all user terminals involved in the dissemination process (even those that are potentially not interested in the content but can be used as relays). Here, user terminals A, B, C (represented), D and E (not represented) receive offloading instructions. Such instructions include the description of the data flow to be generated/received, the destination of the content M, the data dissemination protocol to be used (e.g., epidemic, social-based).

11. According to the offloading instructions, user terminals A, B, C and D configure their flow identification modules to capture the flow they are going to receive and trigger MOTO-specific treatment (so that content tracking feedback will be sent).

12. The Dissemination Strategy block actually sends the photo to "User terminal B" through the primary channel (e.g. LTE).

13. When receiving the photo, "User terminal B" (more precisely, the Content tracking feedback block) sends a feedback to acknowledge the reception of the content to the Content Tracker module of the CDM.

14. Authentication then takes place between user terminals that participate in the dissemination process so that the content is relayed securely:

    (a) authentication between "User terminal A" and "User terminal D".

    (b) authentication between "User terminal B" and "User terminal C".

15. The content is actually relayed through direct WiFi ad hoc connections:

    (a) from "User terminal A" to "User terminal D".

    (b) from "User terminal B" to "User terminal C".

16. User Terminals send a content tracking feedback message to acknowledge the reception of the content to the Content Tracker block of the CDM. Such a feedback message can include information about the terminal the content was received from.

    (a) "User terminal D" sends a content tracking feedback message to the Content Tracker.

    (b) "User terminal C" sends a content tracking feedback message to the Content Tracker.

17. Depending on the information contained in feedback messages, the Content Tracker block can report relaying activities of "User terminal A" (14a) and "User terminal B" (14b) to the Authentication & Accounting module.

18. As a result, the Authentication & Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

19. The Dissemination Strategy module regularly checks the dissemination status by requesting the Content Tracker. (Not represented: the dissemination strategy can be updated, e.g. new offloading instructions and the content can be directly sent to other clients. Steps 7 to 19 are thus repeated). When entering in the panic zone (before dissemination delay expires) the Dissemination Strategy module checks the dissemination status.

20. If some clients did not receive the content when entering the panic zone, the Dissemination Strategy block triggers the diffusion of the content to all those clients through the primary communication channel (e.g. LTE).

21. Those clients finally acknowledge the reception of the content to the Content Tracker block of the CDM.

4.5.3 Small Crowds Scenarios

4.5.3.a Scenario 5: Expanded coverage and cellular network offloading

In this scenario, the goal is to use direct communication between MOTO clients in a given locality to share the content of a music playlist.

Application of scenario 5 : music playlist sharing.

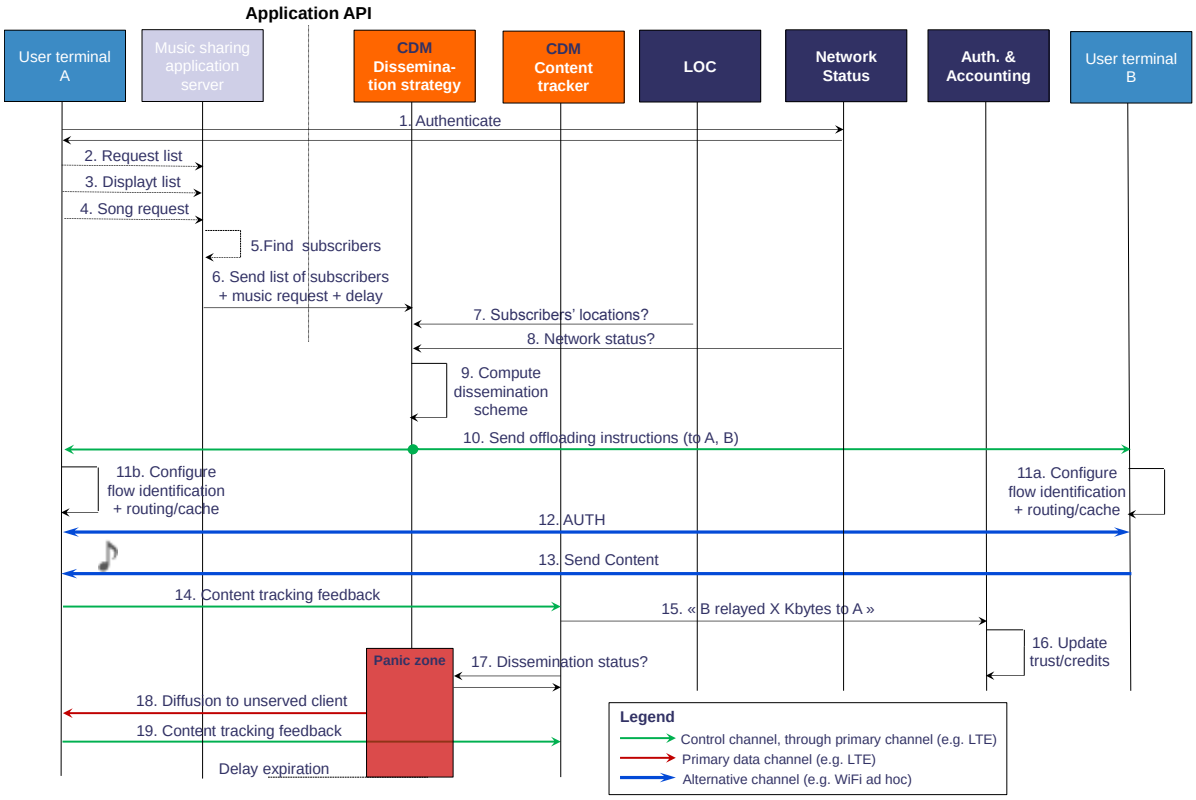


Figure 11: Sequence of interactions between external and internal MOTO elements for the use case "Expanded coverage and cellular network offloading".

Step-by-step. Explanation of flow chart shown in Figure 11:

1. a client ("User Terminal A") of the MOTO service authenticates into the MOTO system with Authentication and Accounting Module and receives the authentication response.

2. "User Terminal A" requests a list of the music playlist from the "music sharing application server".

3. The "music sharing application server" displays the local playlist to client ("User Terminal A") through the primary communication channel (e.g. LTE or Wi-Fi network).

4. "User Terminal A" of the "music sharing in a local jukebox" system requests for a single playlist download command to the music sharing application server.

5. the "music sharing application server" identifies other local subscribers interested in this content.

6. the local music sharing jukebox server delegates the download dissemination of this playlist to MOTO Services. More precisely, it uses the *Application API* to give inputs (list of subscribers, content to receive, maximum delay) to the Dissemination Strategy functional block of the MOTO Content Diffusion Manager, in charge of coordinating the dissemination of this content.

7. the Dissemination Strategy block gathers information on subscribers' location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Users' terminals also feed the LOC module by sending their GPS position).

8. The Dissemination strategy block of the CDM gathers information on network congestion from the Network Status module. (Not represented: through the *Infrastructure API*, the Network Status module maintains some congestion information available in operators' networks).

9. From the information available, the Dissemination Strategy function of the Content Diffusion Manager identifies a strategy for dissemination of the music content from the list of available seed users. For instance, the resulting strategy consists in user "User terminal A" (opportunistic role) downloading music content from "User terminal B" (seed role). For instance, the resulting strategy consists in downloading music content from "User terminal B" for opportunistic client "User terminal A".

10. As a result, the Dissemination Strategy block sends offloading instructions to both "User terminal A" and "User terminal B". Instructions include the description of the music data flow to disseminate, the node the music content must be relayed to, and the routing (which interface to use) and caching (keep in local cache or not) instructions.

11. According to the offloading instructions:
    (a) "User terminal B" prepares the flow to be send through its Wi-Fi ad hoc interface,
    (b) "User terminal A" configures its flow identification module to capture the flow from the "User Terminal B" through alternative channel, e.g. WiFi ad hoc, and triggers MOTO-specific treatment (so that content tracking feedback will be sent and the flow will be offloaded from "User terminal B"). (Synchronization process between "User terminal A" and "User Terminal B" is assumed and both users send their configuration response messages to Content Diffusion Manager (CDM)).
12. Authentication then takes place between "User Terminal A" and "User Terminal B" so that the content is relayed between them securely.
13. "User terminal B" relays the content to "User Terminal A" (e.g. through direct ad hoc connection which is represented with blue line).
14. "User terminal A" acknowledges the reception of the music content to the Content tracker block of the Content Diffusion Manager. Such a feedback message can include information about who the content were received from ("User terminal B" in this case).
15. Depending on the information contained in feedback messages, the Content tracker can report relaying activities to the Authentication & Accounting module (e.g. "B relayed X kbytes to A").
16. As a result, the Authentication & Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (e.g. reduces amount of virtual credits of "User terminal A" and increases virtual credits of "User terminal B").
17. The Dissemination Strategy module regularly checks the dissemination status by requesting the Content tracker. (Not represented: the dissemination strategy can be updated, e.g. relay instructions and the content can be directly sent to new clients.) When entering in the panic zone (before dissemination delay expires) the Dissemination Strategy module checks the dissemination status.
18. if "User terminal A" did not receive the content when entering the panic zone, the Dissemination Strategy block triggers the diffusion of the content by repeating the above steps for new seed clients or through primary communication channel (e.g. LTE)
19. "User terminal A" finally acknowledges the reception of the content to the Content tracker block of the Content Diffusion Manager.

4.5.3.b Scenario 6: Content dissemination based on payment system

In this scenario, the goal is to use WiFi connectivity among MOTO clients in public transportation systems (trains, airports etc.) so that e.g. music or video streaming content can be delivered through other clients' sharing their access to the LTE network. A client that shares its LTE connectivity earns virtual credit to be used later for free phone calls or text messages while opportunistic users pay virtual credits to use seed clients' connectivity.

We consider three users in a train one of them can communicate through LTE connection or WiFi(B) while others only through WiFi connection (A and C). We consider that user A requests a content from a Web Server through its seed user (user B). Black arrows in Figure 12 depict interactions between actors, and colored arrows give details on the offloading process performed by MOTO, given as an example and described above (color-code is explained in the legend).

The web server application gives inputs (list of clients, content to disseminate, maximum delay to disseminate the content) to the MOTO platform. From these inputs, the MOTO Services coordinates the dissemination according to the sequence represented in following figure (colors refer to the architecture building blocks).

Application of scenario 6 : delivery Internet services.

Step-by-step. Explanation of flow chart shown in Figure 12:

1. Web Server Application, through Application API, provides info to CDM to implement right dissemination strategy to be applied.

2. clients of the "MOTO Service" ("User terminal A", "User terminal B") authenticate themselves in MOTO Services using primary channel (e.g LTE).

3. the "Web Server Application" identifies new subscribers of MOTO Services interested in Web Server contents.

4. the Dissemination Strategy block gathers information on subscribers' location from the LOC module. (Not represented: through the Infrastructure API, the LOC module maintains some localization information available in operators' networks. Users' terminals also feed the LOC module by sending their GPS position).

5. from the information available, the Dissemination Strategy function of the Content Diffusion Manager elaborates a strategy for disseminating the content. For instance, the resulting strategy consists in identifying "User terminal B" as the seeder which can perform relay for "User terminal A". We suppose "User terminal A" is an opportunistic client of Moto Service and it has only WiFi connectivity available after receiving offloading instructions. "User terminal B" will execute relay for "User terminal A".

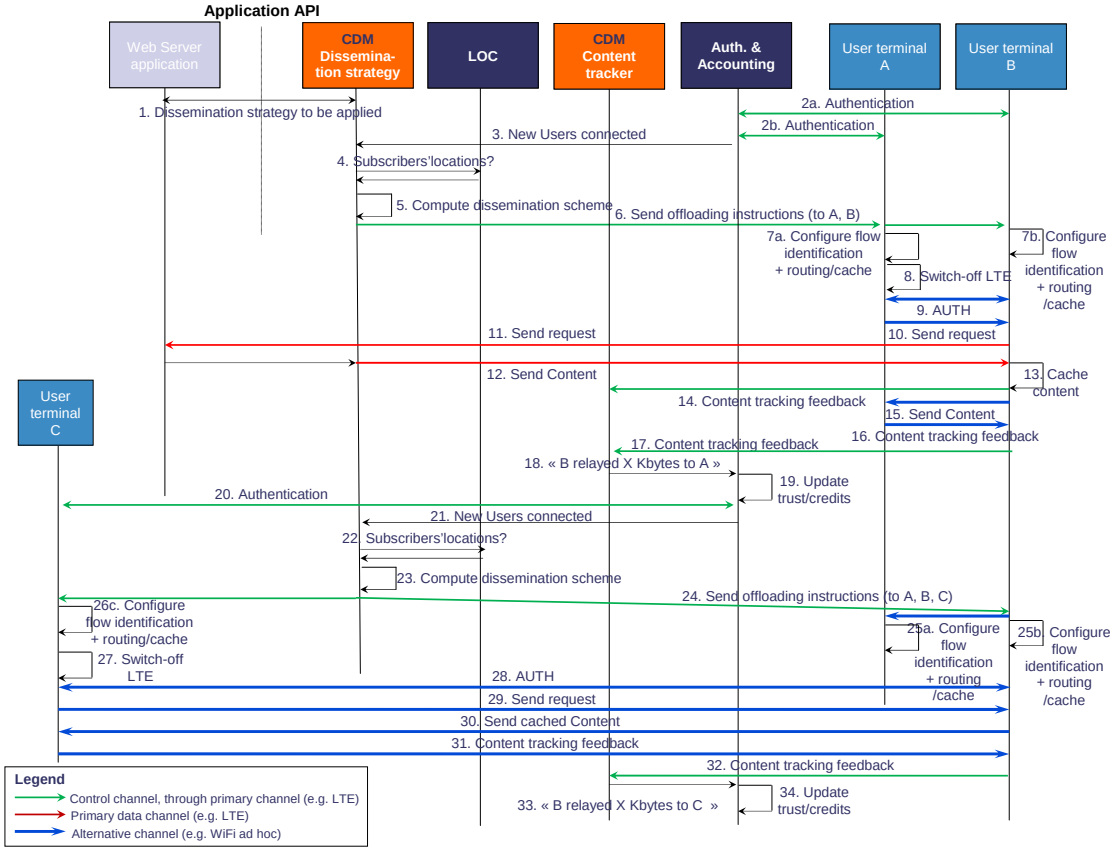


Figure 12: Sequence of interactions between external and internal MOTO elements for the use case "Content dissemination based on payment system".

6. the Dissemination Strategy block sends offloading instructions to all user terminals involved in the dissemination process (even those that are potentially not interested in the content but can be used as relays). Such instructions include, the list of opportunistic and seed nodes interested in MOTO content and the routing (which interface to use) and caching (keep in local cache or not) instructions. A set of instructions to charge the "seed" user to relay any communication with the MOTO platform in addition to the relayed content has to be foreseen. From now on each information from or to "User terminal A" will be sent to "User terminal B".

7. according to the offloading instructions:

   (a) "User terminal B" configures its flow identification module to capture the flow it is going to receive from the CDM through the primary channel (e.g. LTE) and triggers MOTO-specific treatment (so that content tracking feedback will be sent and the flow will be relayed).

   (b) "User terminal A" configures its flow identification module to capture the flow it is going to receive and triggers MOTO-specific treatment (so that content

tracking feedback will be sent).

8. opportunistic client "User terminal A", after receiving offloading instructions, switchs off LTE interface. That can be done automatically by the application using the MOTO services.

9. authentication then takes place between user terminals that participate in the dissemination process so that the content is relayed securely from "User terminal A" to "User terminal B".

10. "User terminal A" requests content through its seed user ("User terminal B") using WiFi ad-hoc connection.

11. "User terminal B" forwards the content request to web server application using primary channel (e.g. LTE).

12. the Web server delegates the dissemination of the content to the MOTO Services Dissemination Strategy block; the content is sent to "User terminal B" through the primary channel (e.g. LTE).

13. "User terminal B", storages the received content in its internal cache.

14. when receiving the content, "User terminal B" sends a feedback to acknowledge the reception of the content to the Content tracker module of the Content Diffusion Manager.

15. "User terminal B" sends the content to its opportunistic client ("User terminal A") using ad-hoc connection.

16. "User terminal A" using ad-hoc WiFi connection sends a feedback to acknowledge the reception of the content to its seeder "User terminal B".

17. "User terminal B" forwards the "User terminal A" feedback to CDM using primary channel (e.g. LTE).

18. depending on the information contained in feedback messages, the Content tracker can report relaying activities to the Authentication & Accounting module:

    - the Content tracker reports relaying activities of "User terminal B" to the Auth & Accounting module,

19. as a result, the Authentication & Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

20. a new opportunistic clients of the "MOTO Service" ("User terminal C) authenticates itself in MOTO Services using primary channel (e.g LTE).

21. the "Web Server Application" identifies new subscriber of MOTO Services interested in Web Server contents.

22. the Dissemination Strategy block gathers information on subscribers' location from the LOC module. (Not represented: through the Infrastructure API, the LOC module maintains some localization information available in operators' networks. Users' terminals also feed the LOC module by sending their GPS position).

23. from the information available, the Dissemination Strategy function of the Content Diffusion Manager elaborates a new strategy for disseminating the content. For instance, the resulting strategy can consists in identifying in "User terminal B" the seeder which can perform relay for "User terminal C". We suppose "User terminal C" is an opportunistic client of Moto Service and it has only WiFi connectivity available after receiving offloading instructions. "User terminal B" will execute relay for "User terminal C".

24. the Dissemination Strategy block sends offloading instructions to all user terminals involved in the dissemination process (even those that are potentially not interested in the content but can be used as relays). Such instructions include, the list of opportunistic and seed nodes interested in MOTO content and the routing (which interface to use) and caching (keep in local cache or not) instructions. A set of instructions to charge the "seed" user to relay any communication with the MOTO platform in addition to the relayed content has to be foreseen. From now on each information from or to "User terminal C" will be sent to "User terminal B". User terminals B and User terminals C, receive offloading instructions through LTE instead User terminals A receives its offloading instruction through its seed user (e.g. User terminals B).

25. according to the offloading instructions:

    (a) "User terminal A" configures its flow identification module to capture the flow it is going to receive through the ad-hoc channel and trigger MOTO-specific treatment (so that content tracking feedback will be sent).

    (b) "User terminal B" configures its flow identification module to capture the flow it is going to receive from the CDM through primary channel and trigger MOTO-specific treatment (so that content tracking feedback will be sent and the flow will be relayed).

    (c) "User terminal C" configures its flow identification module to capture the flow it is going to receive through the ad-hoc channel and trigger MOTO-specific treatment (so that content tracking feedback will be sent).

26. new opportunistic client "User terminal C", after receiving offloading instructions switch-off LTE interface

27. authentication then takes place between user terminals that participate in the dissemination process so that the content is relayed securely from "User terminal C" to "User terminal B".

28. "User terminal C" requests content through its seed user ("User terminal B") using WiFi ad-hoc connection.

29. "User terminal B" sends the content it has previously downloaded and stored in its internal cache, to "User terminal C", using ad-hoc connection.

30. "User terminal C" using ad-hoc WiFi connection sends a feedback to acknowledge the reception of the content to "User terminal B".

31. "User terminal B" forwards the feedback to CDM using primary channel (e.g. LTE).

32. depending on the information contained in feedback messages, the Content tracker can report relaying activities to the Authentication & Accounting module:

    - the Content tracker reports relaying activities of "User terminal B" to the Auth & Accounting module,

33. as a result, the Authentication & Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

4.5.4 Vehicular Scenarios

4.5.4.a Scenario 7: Vehicule fleet management system

In this scenario, the goal is to opportunistically exploit the intermittent connectivity between MOTO mobile vehicles to optimize the transfer of data collected from sensors and sent towards a centralized server dealing with fleet maintenance.

Application of scenario 7 : Using the MOTO capabilities in this scenario allows to offload the cellular network either by using opportunistic encounters between vehicules or with roadside access points.

Step-by-step. Explanation of flow chart shown in Figure 13:

1. Clients ("Vehicle A", "Vehicle B", "Vehicle C") of the MOTO service register their presence to the Fleet Management application server.

2. The Fleet Management application server updates its database with the list of accepted publishers.

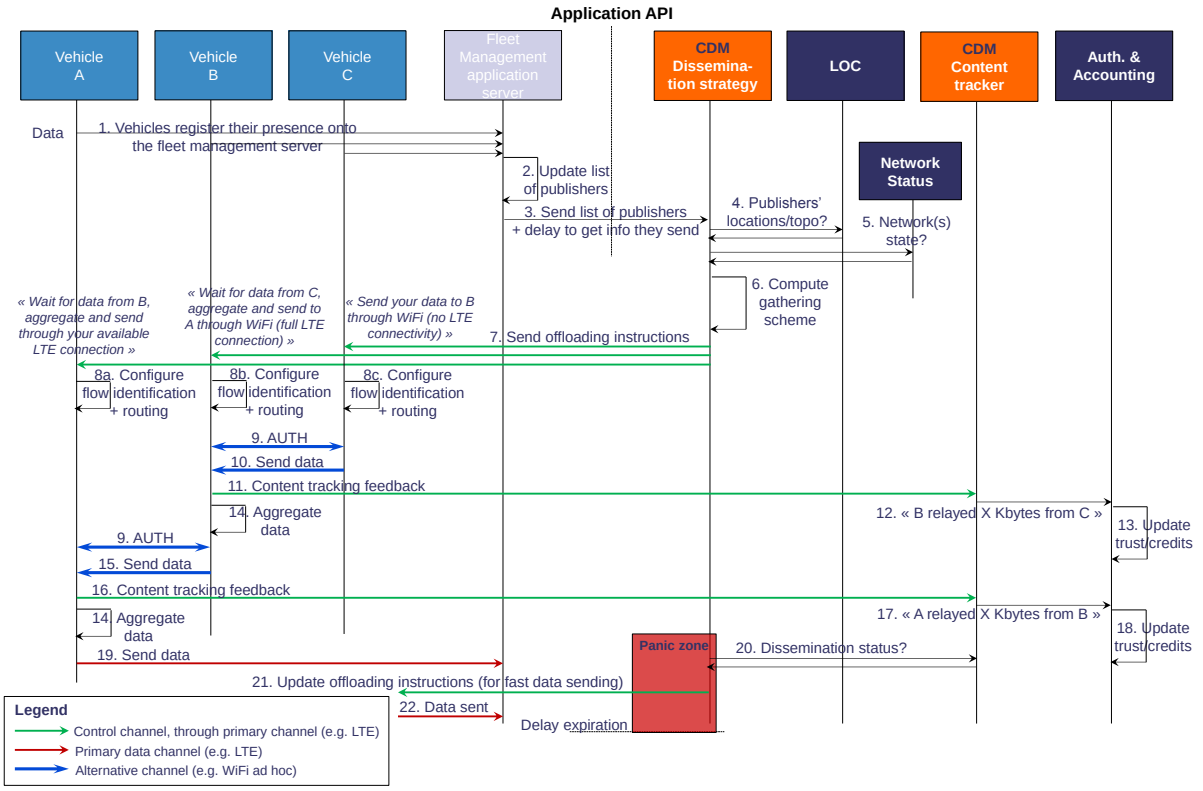


Figure 13: Sequence of interactions between external and internal MOTO elements for the use case "Vehicule fleet management system".

3. The Fleet Management application server transmits to the Dissemination strategy block of the CDM module the list of allowed publishers and the delay tolerance for content reception using the Application API.

4. The Dissemination strategy block of the CDM module gathers information on subscribers' location from the LOC module. (Not represented: through the Infrastructure API, the LOC module maintains some localization information available in operators' networks. Vehicles may also feed the LOC module by sending their GPS position).

5. The Dissemination strategy block of the CDM module gathers information on Network congestion from the Network Status module. (Not represented: through the Infrastructure API, the Network Status module maintains some congestion information available in operators' networks).

6. From the information available (i.e., network status, vehicles' status and location), the Dissemination strategy block of the CDM module configures the gathering scheme from vehicles. For instance, the Dissemination strategy block of the CDM module identifies which vehicles are in good coverage and which are not and defines

the opportunistic data forwarding scheme.

7. Each vehicle is informed about the list of vehicles its content must be relayed to, and the list of vehicles that it will use as a relay (offloading instructions sent from the Dissemination Strategy module of the CDM).

8. Vehicles configure their flow identification module to capture the flow associated to content Mi and to trigger MOTO-specific treatment (e.g., to send content tracking feedback). Likewise, all possible vehicles (e.g., "Vehicle B") that must take part to the opportunistic gathering process are instructed to accept the flow associated to content Mi.

9. When a user (e.g., "Vehicle C") encounters another terminal (e.g., "Vehicle B"), which is listening on the flow identification for content $M1$ but it does not store content $M1$, authentication takes place between them.

10. "Vehicle C" sends content $M1$ to "Vehicle B" (e.g. through direct ad hoc) according to the instructions received from the Dissemination strategy module of the CDM.

11. At content reception, "Vehicle B" sends feedback messages to the Content tracker module of the CDM through the primary communication channel (e.g. LTE). Such a feedback message can include information about which content were received from whom (e.g., in this case content $M1$ was received from "Vehicle C").

12. Depending on the information contained in feedback messages, the Content tracker block of the CDM module can report relaying activities to the Authentication and Accounting module (e.g. "C relayed X kBytes to B"). As a result, the Authentication and Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (e.g. increases virtual credits for "Vehicle B").

13. "Vehicle B" aggregates the data $M1$ received from "Vehicle C" with its own sensed data $M2$.

14. When an user (e.g., "Vehicle B") encounters another terminal (e.g., "Vehicle A"), which is listening on the flow identification for content $M1 + M2$ but it does not store content $M1 + M2$, authentication takes place between them.

15. "Vehicle B" sends content $M1 + M2$ to "Vehicle A" (e.g. through direct ad hoc) according to the instructions received from the Dissemination strategy block of the CDM module.

16. At content reception, "Vehicle A" sends feedback messages to the Content tracker block of the CDM module through the primary communication channel (e.g. LTE). Such a feedback message can include information about which content were received from whom (e.g., in this case content $M1 + M2$ was received from "Vehicle B").

17. Depending on the information contained in feedback messages, the Content tracker block of the CDM module can report relaying activities to the Authentication and Accounting module (e.g. "B relayed X kBytes to A"). As a result, the Authentication and Accounting module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (e.g. increases virtual credits for "Vehicle B").

18. "Vehicle A" aggregates the data $M1 + M2$ received from "Vehicle B" with its own sensed data $M3$.

19. The aggregate data $M1+M2+M3$ is sent by "Vehicle A" to the Fleet Management application server using the primary communication channel (e.g. LTE).

20. When in panic zone and before the deadline, the Dissemination strategy block ask the Content tracker block for the current content dissemination status.

21. If some contents are still missing, the Dissemination strategy block of the CDM module updates instruction at vehicles that store missing contents in order to trigger the transmission through the primary communication channel (e.g. LTE).

22. Triggered vehicles send missing content using the primary communication channel (e.g. LTE).

4.5.4.b Scenario 8: Map-based advanced driver assistance system (ADAS)

In this scenario, the goal is to disseminate map data to vehicles equipped with map-based ADAS. In particular, when several vehicles are located in the same area or are driving towards the same direction or destination, they will likely require the same map information, at least partially. The offloading procedures enabled by the MOTO Platform may be used to avoid overloading the LTE network thanks to the opportunistic network created by direct communication between vehicles.

Application of scenario 8 : Advanced driver assistance.

Step-by-step. Explanation of flow chart shown in Figure 14:

1. A client ("Vehicle A") of the "Map-based ADAS" service sends a request for a specific map. (Not represented: a similar request for the same content comes also from two other clients, namely "Vehicle B" and "Vehicle C").

2. The "Map-based ADAS application server" evaluates all the received requests and it is able to identify the subscribers interested in the same content.

3. The "Map-based ADAS application server" is not able to directly serve all the requests through the primary communication channel (e.g., LTE network). Therefore, it delegates the dissemination of this map to MOTO Services. More precisely, it

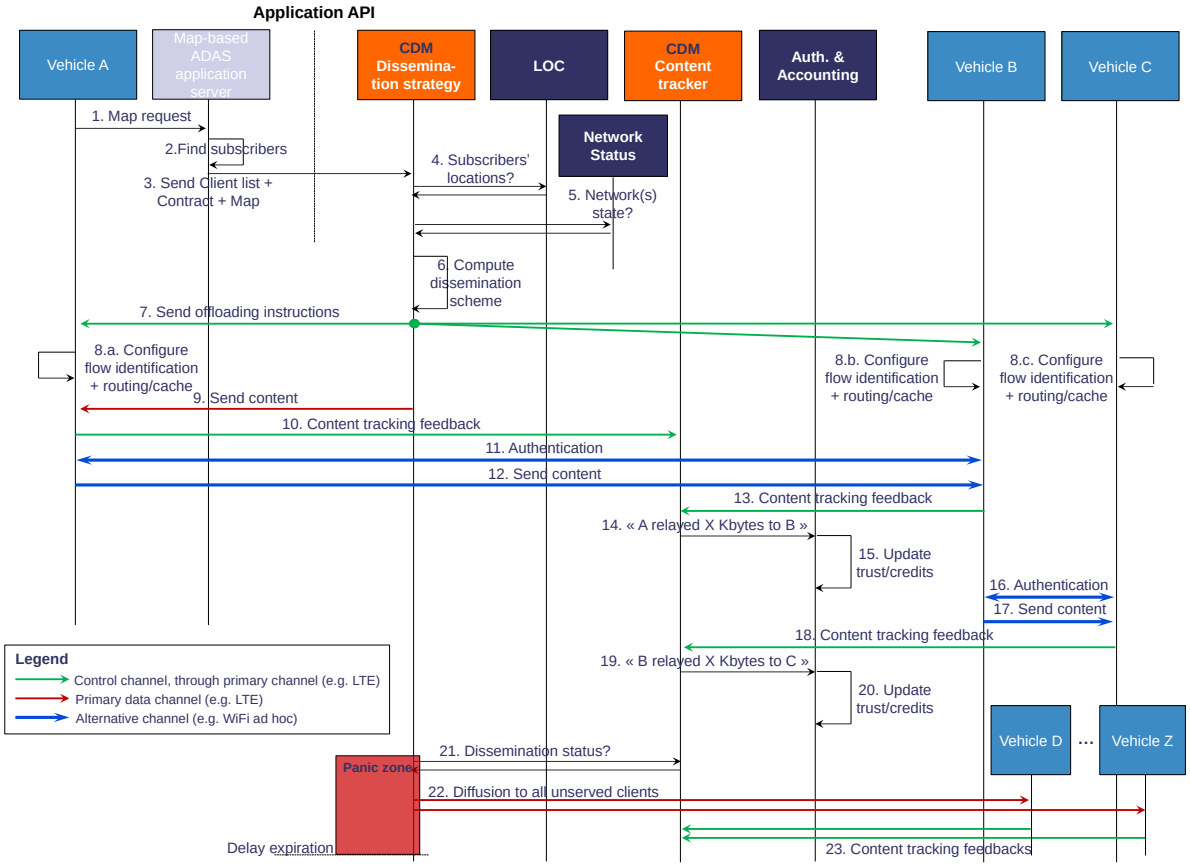


Figure 14: Sequence of interactions between external and internal MOTO elements for the use case "Map-based advanced driver assistance system (ADAS)".

uses the *Application API* to give inputs (client list, contract, content) to the "Dissemination strategy" functional block of the MOTO Content Diffusion Manager, in charge of coordinating the dissemination of this content (i.e., the required map).

4. The "Dissemination strategy" block gathers information on subscribers' location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Vehicles may also feed the LOC module by sending their GPS position).

5. The "Dissemination strategy" block of the CDM gathers information on network congestion from the Network Status module. (Not represented: through the *Infrastructure API*, the Network Status module maintains some congestion information available in operators' networks).

6. From the information available (i.e., network status, vehicles' status and location), the "Dissemination strategy" block of the Content Diffusion Manager identifies that

the three clients are located in the same zone and it elaborates a strategy for disseminating the content. In fact, it is able to define which vehicles can act as seed users and the resulting list of destinations. For instance, the resulting strategy could consist in delivering the map to "Vehicle A" and ask it to relay to "Vehicle B". "Vehicle C" will then receive the same content from "Vehicle B".

7. As a result, the "Dissemination strategy" block sends offloading instructions to all involved clients (i.e., "Vehicle A", "Vehicle B" and "Vehicle C"). Instructions include the description of the data flow to be received, the node the content must be relayed to ("Vehicle B" and "Vehicle C", respectively), and the routing (which interface to use) and caching (keep in local cache or not) instructions.

8. According to the offloading instructions, "Vehicle A", "Vehicle B" and "Vehicle C" configure their flow identification module to capture the flow and trigger MOTO-specific treatment (so that content tracking feedback will be sent and the flow will be correctly relayed to proper receipients).

9. After offloading instructions are sent, the "Dissemination strategy" block sends the map to "Vehicle A".

10. When receiving the content, "Vehicle A" (more precisely, the "Content tracking feedback" block) sends a feedback to acknowledge the reception of the content to the "Content Tracker" module of the Content Diffusion Manager.

11. Authentication then takes place between "Vehicle A" and "Vehicle B", so that the content is relayed between them securely.

12. "Vehicle A" relays the content to "Vehicle B" (through direct 802.11p ad hoc connection).

13. "Vehicle B" acknowledges the reception of the map to the "Content tracker" module of the Content Diffusion Manager. Such a feedback can include information about who the content were received from.

14. Depending on the information contained in feedback messages, the "Content tracker" can report relaying activities to the "Authentication & Accounting" module.

15. As a result, the "Authentication & Accounting" module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

16. Once "Vehicle B" has received partially or totally the map, it can start relaying the content to "Vehicle C". Therefore, authentication takes place between "Vehicle B" and "Vehicle C", so that the content is relayed between them securely.

17. "Vehicle B" relays the content to "Vehicle C" (through 802.11p direct ad hoc connection).

18. "Vehicle C" acknowledges the reception of the map to the "Content tracker" module of the Content Diffusion Manager. Such a feedback can include information about who the content were received from.

19. Depending on the information contained in feedback messages, the "Content tracker" can report relaying activities to the "Authentication & Accounting" module.

20. As a result, the "Authentication & Accounting" module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

21. The "Dissemination Strategy" module regularly checks the dissemination status by requesting the "Content tracker". When entering in the panic zone (before dissemination delay expires) the "Dissemination Strategy" module checks the dissemination status.

22. If some clients did not receive the content when entering the panic zone, the "Dissemination Strategy" block triggers the diffusion of the content to all those clients through the primary communication channel (e.g., LTE network).

23. Those clients finally acknowledge the reception of the content to the "Content tracker" block of the Content Diffusion Manager.

4.5.4.c Scenario 9: Enhancing traffic efficiency through cooperative V2X communication systems

In this scenario, registered users receive in their cars information related to traffic efficiency and management (e.g., traffic signs, road works, speed limits, traffic jam, and road accidents). This kind of information is usually characterized by a limited geographic validity and it is therefore distributed only locally in the directly interested areas. However, its distribution outside those areas would help also other users in improving their driving experience. In such a context, the offloading procedures enabled by the MOTO Platform may be used to increase coverage of the service thanks to the opportunistic network created by direct communication between vehicles.

Application of scenario 9 : road/traffic information sharing.

Step-by-step. Explanation of flow chart shown in Figure 15:

1. The "Cooperative V2X application server" gathers information related to a specific traffic event that has to be sent to registered users located in a certain area. It is therefore able to identify the subscribers interested in the content, limited to the geographic area of interest.

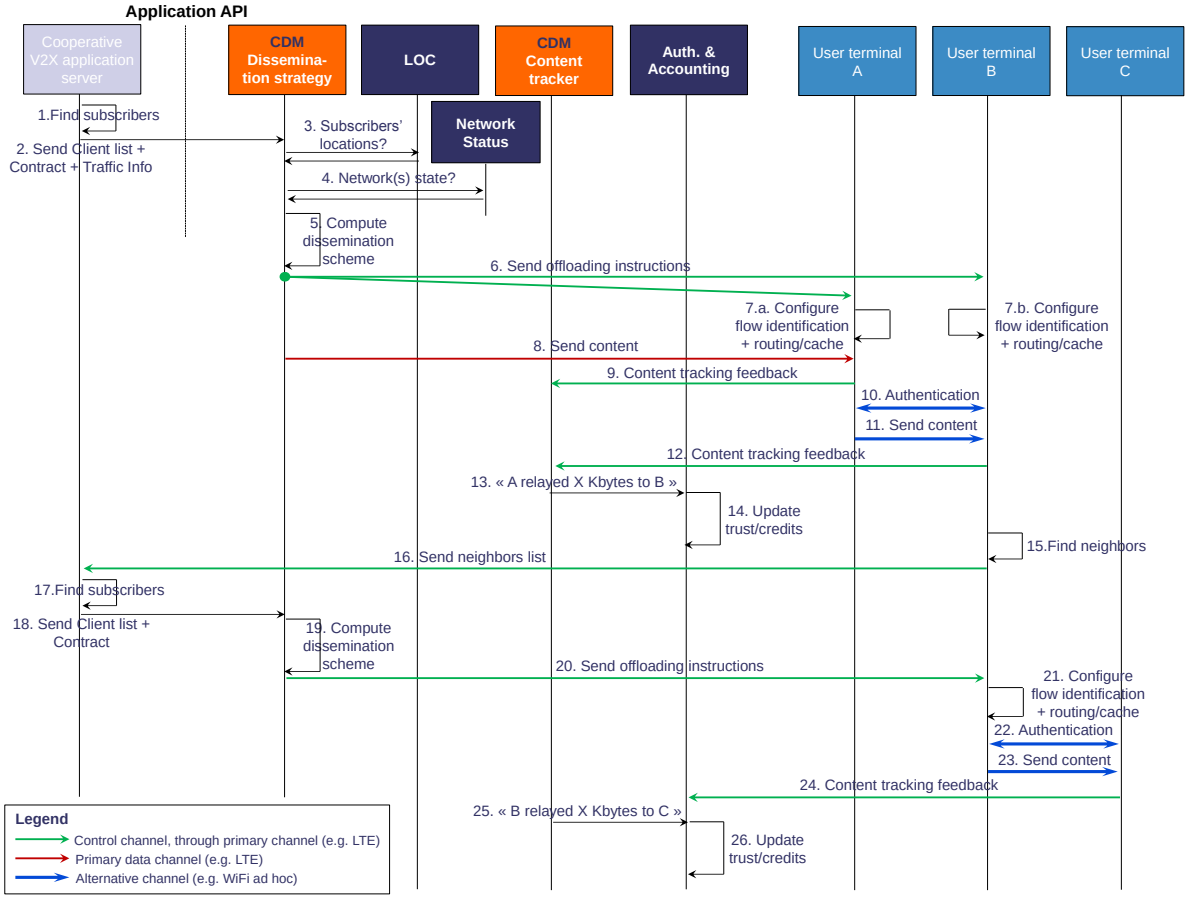


Figure 15: Sequence of interactions between external and internal MOTO elements for the use case "Enhancing traffic efficiency through cooperative V2X communication systems".

2. The "Cooperative V2X application server" delegates the dissemination of this traffic information to MOTO Services. More precisely, it uses the *Application API* to give inputs (client list, contract, content) to the "Dissemination strategy" functional block of the MOTO Content Diffusion Manager, in charge of coordinating the dissemination of the content.

3. The "Dissemination strategy" block gathers information on subscribers' location from the LOC module. (Not represented: through the *Infrastructure API*, the LOC module maintains some localization information available in operators' networks. Vehicles may also feed the LOC module by sending their GPS position).

4. The "Dissemination strategy" block of the CDM module gathers information on network congestion from the Network Status module. (Not represented: through the *Infrastructure API*, the Network Status module maintains some congestion information available in operators' networks).

5. From the information available (i.e., network status, vehicles' status and location),

the "Dissemination strategy" block of the Content Diffusion Manager identifies that two clients are located in the same zone and it elaborates a strategy for disseminating the content. In fact, it is able to define which vehicles can act as seed users and the resulting list of destinations. For instance, the resulting strategy could consist in delivering the traffic information to "Vehicle A" and ask it to relay to "Vehicle B".

6. As a result, the "Dissemination strategy" block sends offloading instructions to "Vehicle A". Instructions include the description of the data flow to be received, the node the content must be relayed to ("Vehicle B"), and the routing (which interface to use) and caching (keep in local cache or not) instructions.

7. According to the offloading instructions, "Vehicle A" and "Vehicle B" configure their flow identification modules to capture the flow and trigger MOTO-specific treatment (so that content tracking feedback will be sent and the flow will be relayed to "Vehicle B").

8. After offloading instructions are sent to "Vehicle A", the "Dissemination strategy" block actually sends the traffic information to "Vehicle A".

9. When receiving the content, "Vehicle A" (more precisely, the "Content tracking feedback" block) sends a feedback to acknowledge the reception of the content to the "Content tracker" module of the Content Diffusion Manager.

10. Authentication then takes place between "Vehicle A" and "Vehicle B", so that the content is relayed between them securely.

11. "Vehicle A" relays the content to "Vehicle B" (through 802.11p direct ad hoc connection).

12. "Vehicle B" acknowledges the reception of the traffic information to the "Content tracker" module of the Content Diffusion Manager. Such a feedback can include information about who the content were received from.

13. Depending on the information contained in feedback messages, the "Content tracker" can report relaying activities to the "Authentication & Accounting" module.

14. As a result, the "Authentication & Accounting" module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

15. Direct ad hoc communication gives the possibility to "Vehicle B" to be aware of its neighbours (thanks to periodic beaconing). Among them, it is also able to discriminate the users potentially interested in the same traffic information just received (the beacon message contains information related to subscribed services). This step gives the possibility to include in the dissemination mechanism also other service subscribers which can not directly reach the "Cooperative V2X application server"

through the network infrastructure (neither LTE nor 802.11p). Such a process identifies "Vehicle C" as interested recipient for the same content already received.

16. The resulting neighbors' list is sent to the "Cooperative V2X application server".

17. The "Cooperative V2X application server" checks the received neighbors' list and it is able to identify the additional subscribers not previously detected (i.e., "Vehicle C").

18. The "Cooperative V2X application server" delegates the dissemination of this traffic information to MOTO Services. More precisely, it uses the *Application API* to give inputs (client list, contract) to the "Dissemination strategy" functional block of the MOTO Content Diffusion Manager, in charge of coordinating the dissemination of the content.

19. From the information available, the "Dissemination strategy" block of the Content Diffusion Manager elaborates a strategy for disseminating the content among neighbors of "Vehicle B".

20. As a result, the "Dissemination strategy" block sends offloading instructions to "Vehicle B". Instructions include the description of the data flow to be sent, the node the content must be relayed to ("Vehicle C"), and the routing (which interface to use) and caching (keep in local cache or not) instructions.

21. According to the offloading instructions, "Vehicle B" configures its flow identification module to capture the flow and trigger MOTO-specific treatment (so that content tracking feedback will be sent and the flow will be relayed to "Vehicle C").

22. Authentication then takes place between "Vehicle B" and "Vehicle C", so that the content is relayed between them securely.

23. "Vehicle B" relays the content to "Vehicle C" (e.g., through direct ad hoc connection).

24. "Vehicle C" stores the information related to the data exchange just happened. Once it is again under network coverage, "Vehicle C" acknowledges the reception of the traffic information to the "Content tracker" module of the Content Diffusion Manager. Such a feedback can include information about who the content were received from.

25. Depending on the information contained in feedback messages, the "Content tracker" can report relaying activities to the "Authentication & Accounting" module.

26. As a result, the "Authentication & Accounting" module keeps track of relaying activities and is able to update information relative to trust or virtual credentials associated to any client (seed or opportunistic for this particular content).

NOTE: The panic zone has not been considered in this scenario. In fact, "Vehicle C" is not under any network coverage and it would not be possible to directly send to it the required content.

5 Research challenges

The realization of the architecture described in this deliverable requires tackling a number of fundamental research challenges. In this section, we identify, describe, and propose directions to the main problems that have a direct impact on MOTO outcomes.

5.1 Understanding contact opportunities

5.1.1 Problem definition

Opportunistic communications are at the core of MOTO targets. Indeed, achieving efficient offloading onto the is only possible if the MOTO offloading coordination agent has sufficient elements to estimate that the mobile network will be able to disseminate data in an appropriate way. This problem is challenging as the offloading process incurs some overhead (signalling and control packets) and a tradeoff existing between offloading gain and overhead. To this end, it is fundamental to understand how nodes meet as precisely as possible. Although the literature in this area is rich, there are several aspects that remain open and that we need to address in the context of the MOTO project. Understanding contact opportunities is tough for several reasons. First, it is important to rely on real contact traces to derive realistic models; in practice, traces are incomplete and very specific to a given scenario (so, the scenario-driven design strategy in MOTO is adapted). Second, obtaining such traces requires a huge amount of work, especially when the experiment must involve a large number of nodes. Third, the operation of the nodes themselves (for example, duty-cycling) has a direct impact on the contact patterns. In the MOTO project, we need to address all these issues so that the consortium has enough substrate to propose adapted offloading solutions.

5.1.2 Research strategy

To address the abovementioned issues, the MOTO project proposes the following research strategies. With regard to the state-of-the-art, although several achievements have been achieved in the latest years, there are still a few divergences in terms of contact and intercontact patterns; to this end, we will dedicate part of the effort to consolidate the area and confirm that we will adopt the right models in our studies. We will also consider proposing proximity metrics that are expected to identify nearby nodes that could potentially communicate through short-range multihop paths, which might be less expensive than most routing strategies specifically designed for opportunistic networks. We also intend to develop prediction strategies to better capture communication opportunities in the vicinity of the network. With regard to the duty-cycling issue, we need first

to formalize the problem, as it has received little (if any) attention from the research community. In particular, we will have to consider the case of deterministic duty-cycling schemes. The next step in this direction would be to validate models when considering the influence of duty cycling. Finally, as experimentations to obtain contact traces are hard and time consuming, we believe it would be useful to investigate techniques to virtually obtain experimentally-inspired mobility traces from a single experience. To this end, we will investigate plausible mobility strategies to help us extrapolate contact traces out of spatial mobility.

5.1.3 Relation with the global architecture and expected impact.

As the topics identified above are not directly related into implementation (in general they are done offline), the resulting models and patterns will be useful to help configurate the parameters in the protocols and algorithms composing the MOTO architecture. In particular, the outcomes will influence the Content Diffusion Manager as well as the forwarding decisions to be made at the terminal level.

5.1.4 Deliverables reporting the results

D3.1, D3.2, D3.3.1, and D3.3.2.

5.2 Data handling and analysis

5.2.1 Problem definition

Analysing some kind of data will happen in several steps of the MOTO project. Among them, we have mobility data, content data, and 3G/4G data, whenever they will be available. At the time of the writing of this deliverable, we have identified at least two types of data: mobility traces provided by FON (association to access points) and contact traces (available to the community through the CRAWDAD repository).

5.2.2 Research strategy

To handle the several types of data within the MOTO project, we will have to adopt specific strategies and apply non-standard data analysis approaches to help achieve the goals of the project. We will make extensive use of curve fitting strategies as well as the representation of data from a network science point of view. Depending on the size of the data, we may be constrained to also adopt sampling techniques to make the problem tractable. In any case, the partners of the project will share their experience with each other and will make processed data available whenever possible. Last but not least, the MOTO project will pay attention to legal issues and will consider the most advanced techniques of data anonymisation.

5.2.3 Relation with the global architecture and expected impact.

As in the previous section, data handling and analysis has an indirect impact on the MOTO architecture. With this regard, the building blocks that will be influenced by the abovementioned work are mainly those composing the core MOTO service.

5.2.4 Deliverables reporting the results

This research topics have a horizontal influence across the tasks of the project. That said, we can only identify the deliverables to which the techniques developed are likely to be explicitely described: D3.2, D4.1, D5.2, D5.3.

5.3 System capacity

5.3.1 Problem definition

Assessing the system capacity in the MOTO scenarios means characterizing the additional capacity that can be obtained by network operators by enabling offloading and thus data dissemination through opportunistic contacts between mobile devices, with respect to what can be obtained by using dissemination solutions based on wireless infrastructures only (primarily LTE). The research challenge is therefore to provide practical decision making tools "in the hands" of the operators, such that they can (i) determine how close their infrastructures are to the saturation limit, given a profile of the traffic load related to disseminating particular contents to their subscribers; and (ii) understand the capacity gain they can obtain by enabling offloading on a given percentage of users available in the area where dissemination takes place.

5.3.2 Research strategy

In order to address this challenge, we have devised a two-step strategy. In a first phase, we need to precisely characterize the saturation performance of wireless infrastructures, both for quasi-static, nomadic and mobile users (thus covering the mobility profiles of the MOTO use cases). While results exist already showing theoretical capacity limits of the physical channel in LTE networks, scant evidence is available characterizing the saturation throughput that can be obtained by LTE users at the application layer (which is what is most important to them). In order to do so, first of all we will run extensive simulations taking the key elements of the scenarios defined in the MOTO use cases to better identify the saturation points of LTE when a large number of users download content simultaneously. Then, we aim at deriving analytical models describing these saturation points. Similarly, we will develop simulation and analytical models assessing the performance gain (in terms of additional capacity) when a given percentage of mobile users takes part to the offloading task, and thus helps the operator's infrastructure in the dissemination process. The final goal is thus to derive analytical and simulation models that can be use by operators to decide whether their infrastructure is saturated (or close

to saturation), and how to configure the offloading process (i.e., how many nodes must be activated) to obtain a target performance in terms of throughput perceived by the users.

5.3.3 Relation with the global architecture and expected impact.

With respect to the architecture presented in this deliverable (Figure 4), these tools can be implemented primarily in the Content Diffusion Manager of the Core MOTO Services block. They need input from the Network Status and LOC modules, in order to understand the current performance perceived by the users, and their mobility patterns (from which the additional capacity gained through offloading depends) - note that this in turns involve also the local modules in the MOTO terminal blocks, as explained in Section 4.4.1. As output, they can be used to activate offloading on MOTO terminals, through the appropriate interfaces between the Core MOTO Services block and the Terminal MOTO Services block.

5.3.4 Deliverables reporting the results

D3.1, D3.3.1, and D3.3.2.

5.4 Inter-technology interactions and conflicts

5.4.1 Problem definition

The MOTO architecture permits co-existence and joint exploitation of multiple wireless infrastructure technologies. In particular, we focus primarily on co-existence between LTE and WiFi networks. These can be either owned by the same operator, or by different operators that sign agreements to improve each other's capacity by jointly exploiting their infrastructures. Through such agreements, for example, WiFi operators can gain in geographical coverage, while LTE operators can gain bandwidth in specific locations. In this perspective, a key research challenge is understanding how traffic requested by the users should be managed in presence of such hybrid infrastructures. Specifically, we are interested in identifying inter-technology scheduling policies, which determine which portions of the download traffic should flow through which infrastructure (both in presence of offloading on mobile nodes or not).

5.4.2 Research strategy

To address this research challenge, we will first perform an extensive analysis of current scheduling techniques used in LTE and WiFi networks. Note that inter-technology scheduling techniques are complementary to intra-technology scheduling, defined within each individual technology, and operate over a much longer time frame. The second step is to identify and test (mostly through simulation) the performance of the inter-technology scheduling, and how they co-exist with intra-technology scheduling policies.

5.4.3 Relation with the global architecture and expected impact.

With respect to the MOTO architecture, these results will help operators to define the input flows to the content diffusion manager of the Core MOTO Services block, i.e. will be part of the definition of the share of traffic to be managed by the Content Diffusion Manager.

5.4.4 Deliverables reporting the results

D3.3.1 and D3.3.2.

5.5 Design of efficient offloading protocols

5.5.1 Problem definition

The development of efficient offloading protocols lies at the core of MOTO objectives. Relying on user mobility, contact opportunities among users, and common interest on some type of data, we can devise offloading protocols that alleviate the load on the operator's cellular infrastructure by reducing redundant traffic. This is made possible by shifting dynamically data on existing complementary wireless technologies (in MOTO we focus primarily on WiFi infrastructure or ad hoc). MOTO enables operators to exploit the unused capacity in complementary networks in addition to what is available in LTE. The emerging research challenges consist in devising effective protocols and algorithms that make an efficient use of this capacity reserve. The goal is to maximize the gain for the operator, in terms of saved bandwidth and network capacity, improving at the same time throughput and data coverage experienced by users. Complex challenges include the identification of users with higher dissemination potential, and to adapt the offloading process to varying network conditions, in order to guarantee optimal offloading performance.

5.5.2 Research strategy

In order to address the above mentioned challenges, we plan to start from existing state-of-the-art strategies for offloading, which we will gradually improve and extend. Several existing studies disclosed alternative solutions when many co-located users are interested in the same contents. The underlying idea is to benefit from node mobility and delay tolerance of a number of content types to shift a portion of the traffic from the LTE channel to an alternative channel. Though, known limitations of existing solutions are that they all need the knowledge of the contact probability of nodes or a training period to identify peculiarities in contact patterns. We will try to make abstraction of these limitations, by focusing more on the evolution of the content diffusion in the network. This will be possible by exploiting the pervasive connectivity offered by LTE. In our vision, when a mobile node receives content from a neighbor, it acknowledges the reception to MOTO coordinator through LTE. This mechanism allows the MOTO coordinator to monitor in real time the content dissemination process evolution and to react in consequence by injecting additional copies of the content in order to boost the content diffusion. We

plan to develop advanced offloading strategies, exploiting the present and past content dissemination status inferred from the acknowledgements, to decide when and to which nodes to inject the content.

5.5.3 Relation with the global architecture and expected impact.

With respect to Figure 4, the offloading protocol is related with the Content Diffusion Manager block of the Core MOTO Services block. Offloading protocols will be in charge of deciding the overall macro-dissemination strategy, which users would be direct recipients of the contents, the content diffusion instruction, and to manage the panic time re-injection. Offloading protocols need input from the Content Tracker block in the CDM, the Network Status and the LOC modules, in order to infer the current content diffusion status, the network status and the position of users.

5.5.4 Deliverables reporting the results

D3.1, D3.3, D4.2, D5.2, and D5.3.

5.6 Distributed trust and security

5.6.1 Problem definition

The MOTO underlying network model is intrinsically dynamic, that is, users and their roles, network topology, offloading technology, etc. are susceptible to change unexpectedly at any moment. The main research challenge related to trust and security in MOTO is the balance between effectiveness of security mechanisms, and their ability to cope with high dynamicity and unsupervised communications.

5.6.2 Research strategy

Our focus is twofold. In the best scenario (a mutual trusted entity exists or has existed in the past), we plan to study two main mechanisms for managing the trust between various elements of the MOTO infrastructure: the secure exchange of credentials, and the trust acknowledgement from previous connections between users. In the worst-case scenario (a mutual trusted entity cannot be guaranteed or has been compromised at some undetermined point in the past), we plan to give mathematical evidence for lower and upper bounds related to the guaranteed level of trust one can enforce in D2D communications. The developed approaches should assess potential implementation of designed protocols for both mobile platforms, which have limited computing and communication power and various operating systems, and PCs and Laptops.

5.6.3 Relation with the global architecture and expected impact.

The positive approach suggests that MOTO users will authenticate with the MOTO platform and receive back a credential that reflects not only their belonging to the MOTO

system, but also relevant security aspects such as the "social" trust level, the connection rights, the validation period, etc. Self-tuned security and trust are expected to impact significantly the opportunistic communication efficiency mechanism. The negative approach can be seen as a risk assessment study, to measure how compromised security impacts the reliability, availability, and capacity of opportunistic network communications.

5.6.4 Deliverables reporting the results

D4.3.

6 Conclusion

This document is dedicated to present the MOTO global architecture. It first reminds the purpose and goals of the FP7-MOTO project and then highlights related projects and associated research work. Following this introduction, the main part of the document is dedicated to a detailed description of the architecture and its instantiation on the different use cases described in Deliverable *D2.1: Use Cases and Requirements*. This deliverable concludes by a description of the fundamental research challenges that have been tackeld to achieve the realization of the architecture design.

References

[1] C. W. Paper, "Cisco visual networking index: Global mobile data traffic forecast update, 2010-2015," February 2011. [Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf

[2] "Customers Angered as iPhones Overload AT&T," http://www.nytimes.com/2009/09/03/technology/companies/03att.html.

[3] "iPhone overload: Dutch T-Mobile issues refund after 3G issues," http://arstechnica.com/tech-policy/news/2010/06/dutch-tmobile-gives-some-cash-back-because-of-3g-issues.ars.

[4] A. Handa, "Mobile data offload for 3g networks," February 2009. [Online]. Available: http://www.docstoc.com/docs/22754490/Mobile-Data-Offload-for-3G-Networks

[5] "Why 4G won't fix your mobile woes," http://www.infoworld.com/d/mobilize/why-4g-wont-fix-your-mobile-woes-297.

[6] M. Rinne and O. Tirkkonen, "Lte, the radio technology path towards 4g," *Comput. Commun.*, vol. 33, no. 16, pp. 1894–1906, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comcom.2010.07.001

[7] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas, "Lte-advanced: next-generation wireless broadband technology [invited paper]," *Wireless Communications, IEEE*, vol. 17, no. 3, pp. 10–22, 2010.

[8] S. ping Yeh, S. Talwar, G. Wu, N. Himayat, and K. Johnsson, "Capacity and coverage enhancement in heterogeneous networks," *Wireless Communications, IEEE*, vol. 18, no. 3, pp. 32–38, 2011.

[9] D. Lopez-Perez, I. Guvenc, G. De la Roche, M. Kountouris, T. Quek, and J. Zhang, "Enhanced intercell interference coordination challenges in heterogeneous networks," *Wireless Communications, IEEE*, vol. 18, no. 3, pp. 22–30, 2011.

[10] K. Lee, J. Lee, Y. Yi, I. Rhee, and S. Chong, "Mobile data offloading: how much can wifi deliver?" *SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 4, pp. 425–426, Aug. 2010. [Online]. Available: http://doi.acm.org/10.1145/1851275.1851244

[11] A. de la Oliva, C. Bernardos, M. Calderon, T. Melia, and J. Zuniga, "IP Flow Mobility: Smart Traffic Offload for Future Wireless Networks," *Communications Magazine, IEEE*, vol. 49, no. October, pp. 124–132, 2011.

[12] M. Barbera, J. Stefa, A. Viana, M. Dias de Amorim, and M. Boc, "Vip delegation: Enabling vips to offload data in wireless social mobile networks," in *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*, June, pp. 1–8.

[13] P. Costa, C. Mascolo, M. Musolesi, and G. Picco, "Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks," *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 5, pp. 748–760, June.

[14] W. Gao and G. Cao, "User-centric data dissemination in disruption tolerant networks," in *INFOCOM, 2011 Proceedings IEEE*, April, pp. 3119–3127.

[15] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in delay tolerant networks: a social network perspective," in *Proceedings of the tenth ACM international symposium on Mobile ad hoc networking and computing*, ser. MobiHoc '09. New York, NY, USA: ACM, 2009, pp. 299–308. [Online]. Available: http://doi.acm.org/10.1145/1530748.1530790

[16] B. Han, P. Hui, V. Kumar, M. Marathe, J. Shao, and A. Srinivasan, "Mobile data offloading through opportunistic communications and social participation," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 5, pp. 821–834, May.

[17] K. Lee, J. Lee, Y. Yi, I. Rhee, and S. Chong, "Mobile data offloading: How much can wifi deliver?" pp. 1–1.

[18] "Consumer Generated Mobile Wireless Media," http://www.anr-crowd.lip6.fr.

[19] J. M. Chapin and W. H. Lehr, "Mobile Broadband Growth, Spectrum Scarcity, and Sustainable Competition," in *TPRC*, 2011, pp. 1–36.

[20] V. Gupta and M. K. Rohil, "ENHANCING WI-FI WITH IEEE802.11U FOR MOBILE DATA OFFLOADING," *International Journal of Mobile Network Communications & Telematics (IJMNCT)*, vol. 2, no. 4, pp. 19–29, 2012.

[21] M. Yavuz, F. Meshkati, S. Nanda, A. Pokhariyal, N. Johnson, B. Raghothaman, and A. Richardson, "Interference Management and Performance Analysis of UMTS/HSPA+ Femtocells," *Communications Magazine, IEEE*, vol. 47, no. September, pp. 102–109, 2009.

[22] D. Calin, H. Claussen, and H. Uzunalioglu, "On Femto Deployment Architectures and Macrocell Offloading Benefits in Joint Macro-Femto Deployments," *Communications Magazine, IEEE*, vol. 48, no. January, pp. 26–32, 2010.

[23] J. Gora and T. Kolding, "Deployment Aspects of 3G Femtocells," in *Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on*, 2009, pp. 1507–1511.

[24] L. Hu, C. Coletti, N. Huan, I. Z. Kovács, B. Vejlgaard, R. Irmer, and N. Scully, "Realistic Indoor Wi-Fi and Femto Deployment Study as the Offloading Solution to LTE Macro Networks," in *IEEEVTS Vehicular Technology Conference. Proceedings*, 2012.

[25] L. Hu, C. Coletti, N. Huan, P. Mogensen, and J. Elling, "How Much Can Wi-Fi Offload? A Large-Scale Dense-Urban Indoor Deployment Study," *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, pp. 1–6, May 2012. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6239916

[26] D. Karvounas, A. Georgakopoulos, D. Panagiotou, V. Stavroulaki, K. Tsagkaris, and P. Demestichas, "Opportunistic exploitation of resources for improving the energy-efficiency of wireless networks," *2012 IEEE International Conference on Communications (ICC)*, pp. 5746–5750, Jun. 2012. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6364906

[27] V. Chandrasekhar, J. Andrews, and A. Gatherer, "Femtocell Networks: A Survey," *Communications Magazine, IEEE*, vol. 46, no. September, pp. 59–67, 2008.

[28] J. G. Andrews, H. Claussen, M. Dohler, S. Rangan, and M. C. Reed, "Femtocells: Past, Present, and Future," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 3, pp. 497–508, 2012.

[29] W. Lemstra and V. Hayes, "License-exempt: Wi-Fi complement to 3G," *Elsevier Telematics and Informatics*, vol. 26, no. 3, pp. 227–239, Aug. 2009. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S0736585308000610

[30] Cisco, "Cisco Visual Networking Index: Forecast and Methodology, 2011–2016," 2012.

[31] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Elsevier Computer Networks*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1389128606001009

[32] K. Berg and M. Katsigiannis, "Optimal cost-based strategies in mobile network offloading," in *Proceedings of the 7th International Conference on Cognitive Radio Oriented Wireless Networks*. Ieee, 2012. [Online]. Available: http://eudl.eu/doi/10.4108/icst.crowncom.2012.248505

[33] P. Grø nsund, O. Grø ndalen, and M. Lähteenoja, "Business Case Evaluations for LTE Network Offloading with Cognitive Femtocells," *Elsevier Telecommunications Policy*, no. October, 2012.

[34] A. J. Mashhadi and P. Hui, "Proactive Caching for Hybrid Urban Mobile Networks," *University College London, Tech. Rep*, 2010.

[35] B. Han, P. Hui, V. S. A. Kumar, M. V. Marathe, S. Member, J. Shao, and A. Srinivasan, "Mobile Data Offloading through Opportunistic Communications and Social Participation," vol. 11, no. 5, pp. 821–834, 2012.

[36] "Push Technology," http://en.wikipedia.org/wiki/Push_technology.