Wireless Offline Offload

Dr. Jani Väre
Video Security&Information
Teleste Corporation
Finland

Kimmo Ylander
Video Security&Information
Teleste Corporation
Finland

Kari Virtanen
Video Security&Information
Teleste Corporation
Finland

***Abstract*—Current requirements for vehicular video security systems are making it more challenging to handle the ever-increasing amount of video data produced by the video security systems installed within vehicles. Due to different standard regulations and recommendations, and quite often because of the requirements set by the operators themselves, recorded data not only needs to be stored temporarily within a vehicle's security system, but also needs to be transferred from vehicles to ground systems for more permanent storage. Since public transport systems are most of the time 'on-the-move', the time available to transfer the data is limited. Hence, for large fleets of vehicles, wireless transfer, i.e. wireless offload, is preferred over manual swapping of hard disks. Wireless offload, in turn, is not always simple; sometimes it is not even possible to provide sufficient wireless infrastructure for carrying out wireless offload in a timely manner. This paper proposes an alternative wireless offload mechanism, one which allows for cost-efficient offload that is less affected by the insufficient wireless infrastructure.**

Keywords—video security; CCTV; vehicular; wireless offload; data storage

I. INTRODUCTION

Video security, perhaps still better known as Closed Circuit Television (CCTV) [1] [2], is also becoming a marketable commodity in public transport. It has been a long journey. Since its initial introduction in 1942 [3], a vast number of different applications have been introduced to resolve different challenges and improve different processes, ranging from military and industrial processes to improving the lives of citizens [4]. A video security system can serve many different needs beyond safety and security, such as optimising operations and making public transport systems more efficient. However, in recent years it has been obvious, especially since 9/11, that improving the security and safety of passengers is at the forefront when the priorities of different subsystems are being considered. Likewise, more video security systems have been installed in different public transport systems in recent years, such as in metro systems and buses, as well as in the surrounding infrastructure, stations and bus stops [5] [6]. Studies have also found that there has been a clear drop in crime rates and that video security systems increase the safety and comfort of passengers taking public transport. The Chicago Transit Authority (CTA) [7] is a good example of a public transport system where video security has helped decrease crime rates significantly [8] [9].

The video security systems used in public transport systems are continually evolving as the technology evolves. Also, different standardization authorities promote different requirements and recommendations, all of which can vary substantially throughout the world. For example, the American Public Transport Association (APTA) [10] requires that all video surveillance cameras installed within rail vehicles have a minimum resolution of 1080p and that video material recorded within the railcar be maintained within the railcar for seven days. In addition, APTA mandates that the storage time for material stored in a static location, i.e. video material that has been moved from the railcar to the central system, is 31 days [11]. However, some organisations may require that the recordings be kept for more than 90 days [12]; for instance, American Homeland Security stipulates that the minimum retention time should be between 3 and 6 months [13].

In order to preserve a reasonable amount of storage space in the vehicles, different mechanisms are used to convey the recorded data to the central systems. One of the most recent advances has been the use of different wireless technologies to transfer the video recordings from vehicles to a ground system. Many companies are using the term 'wireless offload' to describe this type of wireless data transfer, which is somewhat reminiscent of 'mobile data offloading' [14] used in the context of managing the high-capacity data traffic of cellular carriers. For clarity's sake, the term 'wireless offload', which will be used hereafter in this paper, refers to a scenario wherein recorded CCTV data are transferred wirelessly to a ground system from a mobile Network Video Recording (mNVR) unit. The wireless offload principle is described in more detail in section II.

Due to the ever-increasing amount of data stored in vehicles, the requirements for wireless offload are also demanding. In some cases, it is not even possible to offer sufficient wireless capacity due to technical limitations or simply because of the high cost of building an infrastructure that would support a sufficient wireless link required for so much data. In order to overcome the problem mentioned above, this paper proposes an alternative method to that of wireless offload, which we call wireless offline offload. The principle behind wireless offline offload is discussed in section III. In Section IV, wireless offload and wireless offline offload are compared. Finally, conclusions are drawn in section V.

II. WIRELESS OFFLOAD CONCEPT

Figure 1 shows a system diagram of the wireless offload concept. The different components are represented by the letters a) to e). The components ranging from a) to c) are located within the vehicle, whereas those from d) to e) are located within the ground system. The VMS systems within the vehicles and ground system are interconnected and in principle part of same modular system. A description of each component is provided below:

a.) **Cameras:** A video security system in the vehicle typically consists of multiple cameras, which are connected and controlled via the Video Management System (VMS), as represented by letter b)

b.) **Mobile video recording and management system:** A Mobile Network Video Recorder (mNVR) contains VMS and storage space for the video recordings provided by the cameras represented by letter a). VMS may be controlled remotely via any end user that has access and user rights with the VMS. A VMS system located within the vehicle initiates or receives wireless offload requests from the VMS system located in the ground system. The VMS located in the vehicle keeps track of the offloaded data and is interconnected with the VMS located in the ground system.

c.) **Mobile Offload node:** The wireless client located within the vehicle is controlled by the VMS (b). The purpose of this particular wireless client is to establish and maintain a wireless connection with the wireless client located in the ground system (d).

d.) **Static offload node:** The wireless client located within the ground system is controlled by the VMS (e). The purpose of this particular wireless client is to establish and maintain a wireless connection with the wireless client located within the vehicle (c).

e.) **Static Video recording and management system**: The video recording system contains VMS and storage space for the video recordings offloaded from the vehicle. It typically also contains other video recordings recorded by the ground system. The VMS located within the ground system may be controlled remotely by any client integrated with the VMS network. The VMS initiates or receives wireless offload requests from the VMS located in the vehicle. It also keeps track of the offloaded data via the VMS in the vehicle and takes care of the inventory and permanently stores the data offloaded into the ground system.

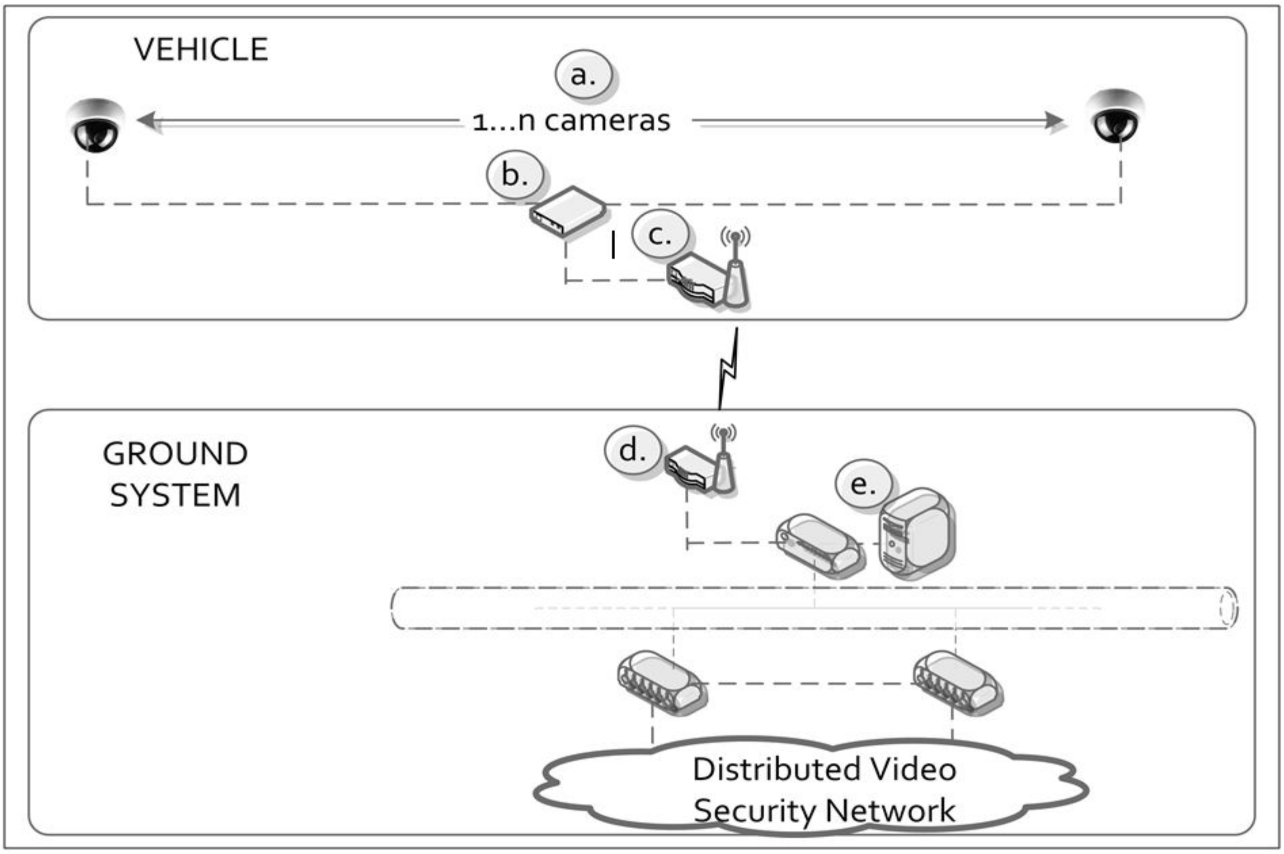

Fig.1. System diagram of the wireless offload concept.

III. WIRELESS OFFLINE OFFLOAD

The wireless offline offload concept is based on the idea that instead of offloading the video data from the mNVR using the method described in section II, all data could be offloaded to the passengers' personal devices within the vehicle using passenger Wi-Fi. Hence, according to the wireless offline offload concept, the passengers' devices function as an additional link in the end-to-end offload system. The motivation for passengers to allow their devices to act as such intermediate carriers in the offline process between the vehicle and ground system could, for example, include a credit-based rewarding system or free tickets for public transport.

The wireless offline offload concept is depicted in Fig.2. The mobile video recording and management system (b) assigns and offloads data to the passengers' devices (f) inside the vehicle via the mobile offload node (c). The passengers' devices may include, e.g. a smart phone, tablet or laptop. Next, the offloaded data are transferred outside the vehicle (f), where the next step in the offload process takes place, i.e. the data are offloaded to the static video recording and management system (e) through the static offload node (d), when a proper network is available. Each offload assignment has an expiration time; if it is not delivered in time, it is then discarded and the assignment is renewed. Hence, (b) and (e) track the offload assignments and renew them when needed.

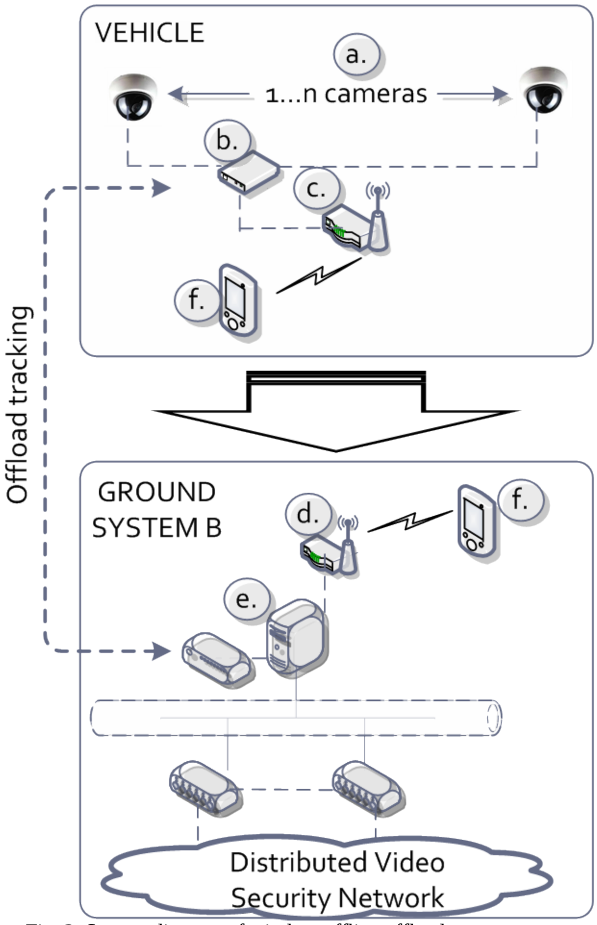

Fig. 2. System diagram of wireless offline offload concept.

Next, Fig.3 shows a sample scenario involving an offload assignment and how the offload process is tracked from the vehicle to the ground system when passengers A and B are offline nodes and are delivering data to the data centre. Passenger A successfully completes the offload assignment by offloading the requested data block before the expiration time. Passenger B, in turn, fails and the offload assignment is renewed in another passenger device. The four steps are as follows:

Step1: Module b) assigns offload data to passengers A and B.

Step2: Passenger A succeeds and passenger B fails to offload the data to the ground system (e) before the expiration time.

Step3: Module e) sends an acknowledge message to module b); the message confirms that the offload assignment of passenger A has been accepted and that the offload assignment of passenger B has failed.

Step4: Module b) reassigns the data previously assigned to passenger B to another passenger.

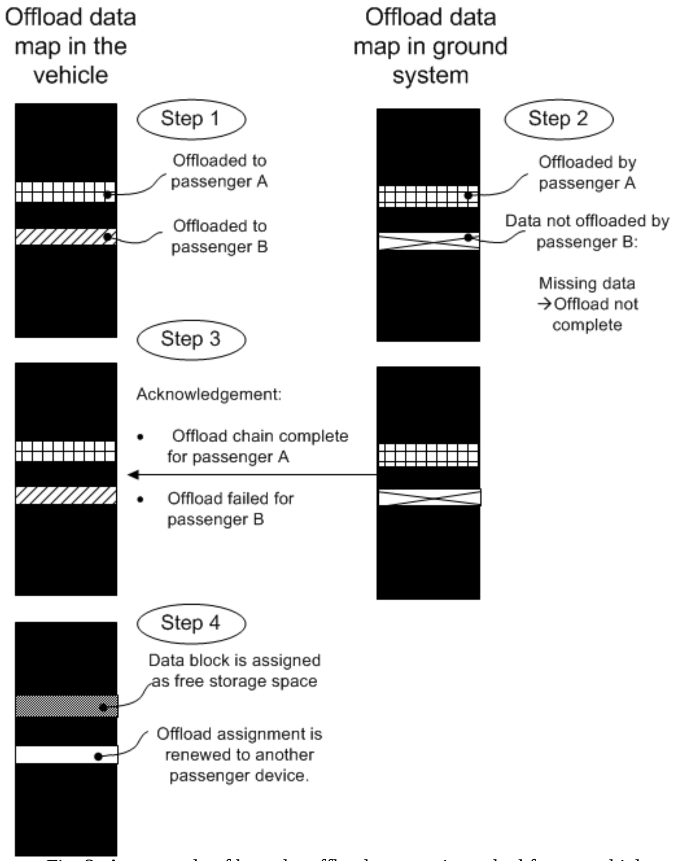

Fig. 3. An example of how the offload process is tracked from a vehicle to the ground system in a scenario involving an offload assignment, where passenger A succeeds and passenger B fails to deliver the offload assignment.

IV. COMPARISON OF WIRELESS OFFLOAD AND WIRELESS OFFLINE OFFLOAD

With the wireless offline offload solution, the wireless transmission is isolated inside the vehicle with less interference and potentially a much larger number of receiving nodes. Hence, the main advantage of the wireless offline offload concept when compared with the wireless offload is that it is independent of the wireless network infrastructure outside the vehicle when offloading data. Therefore, offload is always possible when using wireless offline offload, regardless of whether or not a wireless infrastructure exists outside the vehicle or the quality of the existing wireless connection. The wireless offload, in turn, is dependent on the wireless infrastructure outside the vehicle, and hence, it is vulnerable to a larger amount of source interference with the possibility of only being able to access a few static offline nodes.

This section compares wireless offload and wireless offline offload via a sample scenario and configuration, where data are offloaded from one rail car on a train travelling from Turku to Helsinki. The throughput used in the scenario is based on measured maximum throughput from the actual train route, when 802.11n 2x2 MIMO were used at both ends. Section A defines the parameters of the configuration used for the calculations, while the comparison between the two methods is provided in section B.

A. The configuration and calculations

TABLE I lists the parameters used to calculate the offloaded and stored data in the case of offload and offline offload.

TABLE I. THE PARAMETERS USED FOR DATA STORAGE AND THROUGHPUT CALCULATIONS

Parameter	Value
Number of cameras	8
Camera resolution	1080p
Bitrate per camera	4 Mbps
Total bitrate	8 x 4 Mbps = 32 Mbps
Max. measured throughput available for offload.	180 Mbps
Number of passengers	20
Train stop time in the station	60 seconds
Offloaded data at each station	10800 Mbits
Total amount of offloaded data	97200 Mbits

Next, the train route from Turku to Helsinki and the duration of time between each stop are depicted in TABLE II.

TABLE II. THE PARAMETERS USED FOR DATA STORAGE AND THROUGHPUT CALCULATIONS

Route	Station	Journey time between stops (seconds)
1.	Turku - Kupittaa	360
2.	Kupittaa - Salo	1560
3	Salo - Karjaa	1500
4.	Karjaa - Inkoo	720
5.	Inkoo - Siuntio	900
6.	Siuntio - Kirkkonummi	660
7.	Kirkkonummi - Espoo	780
8.	Espoo - Pasila	840
9.	Pasila - Helsinki	360

The calculations assume that maximum measured throughput is available at every station. Hence, 10800 Mbits can be offloaded at each station where the train stops for 60 seconds, which equals a total amount of 97200 Mbits of offloaded data throughout the duration of the journey. The total amount of recorded data during the train route, based on the scenario just presented, is 2457260 Mbits, and hence, during a journey with the configurations described above only 39.6% of the recorded data could be offloaded. Fig. 4 depicts the current trend for storing the offloaded data within the recorder of a vehicle after each offload at each station.

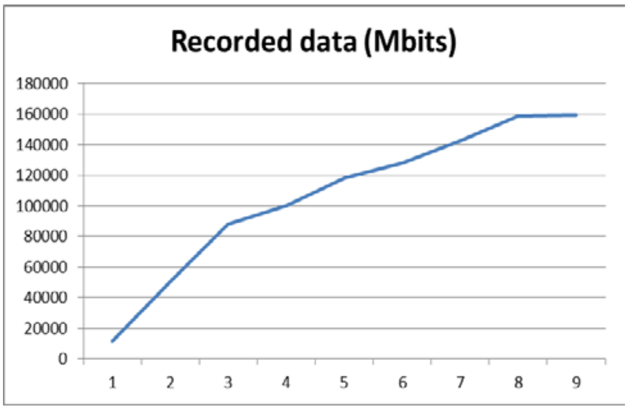

Fig. 4. The current trend for storing the offloaded data within the recorder after each offload at each station.

With the wireless offline offload scenario, data recorded during the duration of the journey are split evenly among the offline clients on the train, i.e. 20 people. In such a system, the offload is not only limited to stops, but can be done throughout the journey; hence, the offload percentage is 100%, which makes it possible to store much larger amounts of data. Fig.5 shows the amount of data stored for each offline client at each stop.

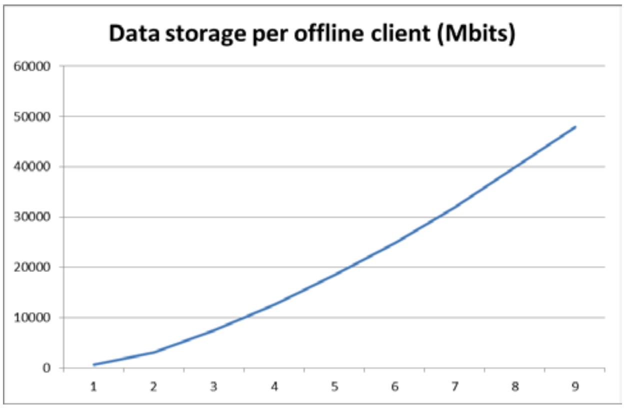

Fig. 5. The data stored on each offline client during the journey from Turku to Helsinki.

B. Comparison

The calculations indicate that the current trend for storing recorded data in the wireless offload is gaining in popularity based on the configurations shown in TABLE I. The throughput used in the calculations is based on the maximum measured value, and it is optimistic given the fact that the wireless network cannot maintain such maximum throughput for the duration of the time available for the offload. To be able to build and guarantee such an optimal wireless network infrastructure, a great deal of investment is required, not only for the HW and SW components themselves but also for the required installations, planning, measurements and testing.

With the offline offload, the wireless infrastructure has no impact on the offload performance so long as there is a sufficient wireless link available inside the vehicle. Hence, the cost of the wireless infrastructure can be minimised throughout the system. The cost can also be reduced because no man hours are required for installing, planning, measuring and testing the system. The core cost of the wireless offline offload is a one-time cost, since it is based by and large on SW. Since wireless offline is a system where sensitive data are distributed throughout a network of ad-hoc mobile nodes, i.e. offline nodes, it requires guaranteed encryption and data privacy.

V. CONCLUSIONS

The calculations for the wireless offload presented in this paper show that alternative solutions are required to overcome the increasing need to deliver CCTV recordings from vehicles to the ground system. As the calculations indicate, approximately 40% of the CCTV data could be offloaded from the vehicle to the ground system based on the scenario described above. However, we assumed that the maximum measured throughput could be guaranteed in all situations. Typically, especially in rail environments and in crowded places, the throughput available for the wireless systems is nowhere near that of the measured maximum in ideal conditions. Also, the cost of implementing and maintaining an ideally operating wireless ecosystem is quite high.

The scenario in chapter III was illustrated by using passengers as conveyors of the offloaded data from vehicle to the ground system. However, same task could be easily assigned to the train staff or e.g. ticket inspectors in the light rail systems and hence, the ‘offload’ failures could be completely avoided.

The novel concept presented here, i.e. a wireless offline offload, offers an alternative or additional solution for situations in which customers need to have CCTV recordings delivered from vehicles to the ground system. When taken further, it can also open up many other opportunities for the operator to communicate and obtain information about passengers and thus reinforce the techno-economical value chain throughout the ecosystem.

REFERENCES

[1] A. R. Matchett, CCTV for Security Professionals. Elsevier Science, USA, 2003.

[2] H. Kruegle, CCTV Surveillance: Video Practices and Technology, Elsevier Inc., USA, 2007.

[3] W. Dornberger, V-2. Ballantine Books, page 14, 1954.

[4] B. Matthews, Video Surveillance and Security Applications: A Manager’s guide to CCTV. Taylor&Francis, July 2015.

[5] V. Ceccato and A. Newton, Safety and Security in Transit Environments: An Interdisciplinary Approach. Palgrave MacMillan, 2015.

[6] http://english.cntv.cn/20140314/103016.shtml
[Referenced 18th August 2015]

[7] http://www.transitchicago.com/
[Reference 18th August 2015]

[8] http://www.nbcchicago.com/traffic/transit/chicago-transit-authority-crime-292174391.html
[Referenced 18th August 2015]

[9] http://www.publicsecurityportal.com/publicsecurity_news.asp?articleid=268793&arttitle=Teleste%20continues%20to%20expand%20CTA%20public%20security%20system
[Referenced 18th August 2015]

[10] http://www.apta.com/
[Referenced 18th August 2015]

[11] APTA, IT-CCTV-RP-001-11 - Technical Recommended Practice for use of IP cameras in transit related surveillance systems. IP Camera and VCA Addendum., USA, March 2014.

[12] http://www.ifsecglobal.com/how-to-achieve-90-days-of-cctv-recording-storage/
[Referenced 19th August 2015]

[13] U.S. Department of Homeland Security, Privacy Impact Assessment for the Security Management CCTV System - DHS/ICE/PIA-030, August 2011.

[14] A. Aijaz, H. Aghvami and M. Amani, “A survey on mobile data offloading; technical and business perspectives”, IEEE Wireless Communications, vol.20, pp. 104-112, April 2013.