Multicast and Virtual Road Side Units for Multi Technology Alert Messages Dissemination

Daniel Câmara, Christian Bonnet, Navid Nikaein, Michelle Wetterwald
Mobile Communications Department
EURECOM
Sophia Antipolis, France
{ daniel.camara, christian.bonnet, navid.nikaein, michelle.wetterwald}@eurecom.fr

Abstract—**This paper presents a method to disseminate alert messages in the context of new emerging communication standards, such as LTE and Wave. The applications involving the broadcast of periodic messages, can be described using the MBMS (Multicast/Broadcast Multimedia Service). Public Safety alert systems perform one important task in the context of Public Safety Networks (PSNs). The method proposed here is responsible for delivering alert messages to the greatest number of people in a specified area. To accomplish this task a new method, Virtual Road Side Unit (vRSU) is proposed to help the authorities to reach isolated people. The system works even if the deployed structure is severed damaged, i.e. most part of the regular Road Side Units (RSU) are out of order. In our method nodes work cooperatively to propagate the message to other nodes, when re-propagating messages nodes, vRSUs, behave as regular RSUs.**

Keywords- Public Safety; multicast; alert; LTE; data dissemination

I. INTRODUCTION

Public Safety Networks (PSNs) are networks established by the authorities to either warn the population about an imminent catastrophe or coordinate teams during the crisis and normalization phases. A catastrophe can be defined as an extreme event causing a profound damage or loss as perceived by the afflicted people. PSNs have the fundamental role of providing communication and coordination for emergency operations.

This paper tackles two different, but complementary, aspects of the alert phase. First we consider the problem of decreasing the amount of traffic in the backbone structure. This aspect is important because "historically, major disasters are the most intense generators of telecommunications traffic" [1]. The lighter is the amount of generated traffic the lower is the chances of having a complete overcharge on the deployed structure. The second aspect we consider here is the extension of the network coverage. In an imminent disaster scenario it is crucial to warn all the concerned people as soon as possible. The problem is that even if we use sirens and broadcast mediums, such as radio and TV, it is not guaranteed that all the people will be in the actuation range of such mediums. In the future pervasive wireless world, all roads and cities will be covered by roadside base stations and access will be provided to both pedestrians and vehicular users. However, for the moment, roadside units (RSUs), or Access Points (APs), are not always present, or may have been damaged as a result of a disaster. Furthermore, the public communication networks, even when available, may fail not only because of physical damage, but also as result of traffic overload. Therefore, the regular public networks alone are often not sufficient to allow rescue and relief operations [1].

The set of solutions proposed here relies in multicast, to decrease the number of messages sent in the core network and a new method based on opportunistic networks to spread the message among the possible endangered people. The main contribution of this paper is in the study of how to efficiently send messages in the context of the new emerging technologies, for instance Long Term Evolution (LTE) networks [12] and IEEE 802.11p or Wireless Access in Vehicular Environments (WAVE) [13]. LTE is one of the most promising technologies for the next generation of wireless broadband access networks, and IEEE 802.11p for vehicular environments, being adopted as the access medium for the WAVE (Wireless Access in Vehicular Environments) IEEE P1609 family of standards. The evaluated methods in one hand decrease the load in the backbone and in the other hand are able to spread the alert messages even to people who have no direct access to the backbone structure.

The technique, which we term Virtual Road Side Units (vRSUs), creates a distributed and cooperative cache among the mobile nodes in the affected area. When using the vRSU technique, nodes cooperatively work as virtual access points by re-distribute messages they have received before and which are stored in their own cache: they thus act in a receive-store-and-forward way. This helps to spread the message to nodes that did not have access to it before. The main advantages of the proposed technique are that it does not rely on any specific characteristics of the network, is transparent, and highly improves the efficiency of data dissemination.

This paper is organized as follows. Section 2 presents some background information related to the techniques used in this work. Section 3 presents the vRSU technique, section 4 presents the developed tool to implement the vRSU technique. Section 5 presents the experiments and in section 6 we draw our conclusions.

II. BACKGROUND

The main objective of this study is to cover the biggest number of people that uses heterogeneous devices, so we

need to use technologies that are common to everyone. To enable the alert messages transfer in the biggest number of technologies as possible standardized solutions are required. However, just that is not enough, we need also to reach people that are possibly in areas that are not covered by the deployed infrastructure, or in the case of a disaster, in the area where the infrastructure was damaged.

The design of the core Internet protocols is based on a number of assumptions: these include the existence of some path between endpoints, short end-to-end round-trip delay time, and the perception of packet switching as the right abstraction for end-to-end communications. Furthermore, the efficiency of these protocols is based on assumptions about the resources available to the nodes and the properties of the links between them. Traditionally nodes are considered to be fixed, energy unconstrained, connected by low loss rate links, and communication occurs through the exchange of data between two or more nodes. In our case, unfortunately these are not the expected conditions for the nodes in the networks. For disaster scenarios we are more likely to have charged backbone structures, when available, mobile nodes with intermittent links, very large delays, high link error rates, energy-constrained devices, with heterogeneous underlying network architectures and protocols in the protocol stack, and most importantly, sometimes with the absence of an end-to-end path from a source to a destination. Develop protocols and applications for such environment imply a series of challenges. This leads us to a new approach of designing networks, taking into account several constraints and characteristics, using DTN (Delay/Disruption Tolerant Networks).

In Disruption Tolerant Networks, also called sometimes opportunistic networks, an end-to-end path from source to destination may not exist. In this environment nodes can still connect and exchange information, but in an opportunistic way. DTNs have been developed as an approach to building architecture models which are tolerant to long delays and/or disconnected network partitions when delivering data to destinations. In 2002 the Internet Research Task Force (IRTF) [4], started a new group called Delay-Tolerant Networking Research Group (DTNRG) [5]. The group was first linked to the Interplanetary Internet Research Group (IPNRG) [7], however, it soon became clear that the main characteristics of DTNs, i.e. non-interactive, asynchronous communication, would be useful in a broader range of situations. The main aim of DTNRG is to provide architectural and protocol solutions to enable interoperation among nodes in extreme and performance-challenged environments where the end-to-end connectivity may not exist.

In the PSNs case, if we consider the occurrence of uncovered areas, the only possible communication mode is from one vehicle to another. This work relies on the existence of infrastructure-to-vehicle (I2V) and vehicle-to-vehicle (V2V) communication to spread public safety messages among users over a defined region. The vehicular network research field, and more specifically the Vehicular DTN (vDTN) research field, have attracted great attention in the last few years. Initiatives such as the i2010 Intelligent Car Initiative Intelligent Car (2009) aim to decrease the number of accidents and CO_2 emissions in Europe, utilizing sensors and V2V communication. As part of these projects, cars equipped with wireless devices will exchange traffic and road safety information with nearby cars and/or roadside units. In fact, according to the ETSI 102 638 technical report [2], by 2017 20% of the running vehicles will have wireless communication capabilities. The same report estimates that by 2027 almost 100% of the vehicles will be equipped with communication devices.

VDTNs have evolved from DTNs and are formed by cars and supporting fixed nodes. Fall [8] is one of the first authors to define and discuss DTNs' potential. According to his definition, a DTN consists of a sequence of time-dependent opportunistic contacts. During these contacts, messages are forwarded from their source towards their destination.

The MBMS (Multicast/Broadcast Multimedia Service) is an enhancement of the UMTS (Universal Mobile Terrestrial Service) system [3]. It provides a point-to-multipoint capability for Broadcast and Multicast Services, allowing resources to be shared in the network. In MBMS Bearer Services takes care of the operation of the radio link between the Radio Access Network (RAN) and the Mobile Terminal. It provides the capability to deliver multicast datagrams to multiple receivers, thus minimizing the network and radio resource usage. This architecture introduces a new functional entity, the BM-SC (Broadcast/Multicast Service Centre). It consists of five sub-functions: membership, session and transmission, proxy and transport for signaling, service announcement and security. The MBMS enables a smart usage of radio-network and core-network resources providing a more efficient radio interface. Using this technique multicast packets can be forwarded from one source to many receivers without overloading the network and consuming the scarce radio resources. As the LTE of the cellular systems is enhancing the capacity and efficiency of the RAN, the MBMS is evolving and adapted to benefit from these improvements.

Comparing the MBMS to the one-to-one model of IP unicast, where data packets are sent from a single source to a single recipient. IP multicast provides a more efficient method for many-to-many communication. This concept is becoming more and more important, both in the Internet and in private networks. Multicast allows the source to send a single copy of data, using a single address for the entire group of recipients. Routers between the source and recipients use the group address to route the data. The routers forward duplicate data packets only when required, i.e. the path to recipients diverges.

The most used multicast routing protocols used today is the Protocol Independent Multicast Sparse Mode (PIM-SM). PIM-SM can use either source-based trees or shared trees. Source based tree, or shortest-path tree, it is a spanning tree that provides the shortest path from the root, data source, to each of the leaves, the receivers. In shared trees the multicast groups have a common root, the rendezvous point (RP), regardless of source. The traffic is forwarded down from the shared tree and RP to reach each of the receivers. The shortest path tree has the advantage of being typically

smaller, from the point of view of the leaves, however, the spanning tree typically saves more network resources. Figure 1 presents the main components of the PIM protocol and the messages involved in the registering process. The registering must be renewed periodically. These messages, plus the periodic hello message, are the main responsible for the overhead the multicast imposes to the network.

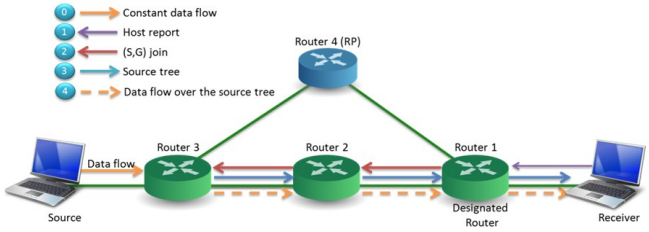


Figure 1. PIM components and register process

III. VIRTUAL ROAD SIDE UNITS FOR MOBILE COMMUNICATION

The main focus of the Virtual Road Side Units (vRSUs) technique is to decrease the areas not covered by roadside APs so as to minimize the problem of intermittent access to mobile nodes. If we are able to decrease this problem, then even stream traffic for mobile users may be enabled. This work is based on opportunistic node contact. The proposed protocol prime for the simplicity as the duration of the contact opportunities between mobile nodes tends to be small. Chaintreau et al. points that for human mobility patterns the contact duration follows a heavy tailed distribution [6] [9]. They observed that the fast contacts are the most common ones among nodes in real world mobility patterns.

The protocol can be summarized as follows. Each node, after receiving a message, caches it and can thus later become a vRSU, acting in a similar way to a relay node. Note however that, instead of just resending the messages, the vRSU stores the message and may send it more than once or not at all depending on the caching strategy and depending on the locations has it passed by. vRSUs strive to supplement the lack of real APs in a given area broadcasting messages received previously from other AP or even vRSUs. A node acts as a vRSU if it is neither in the range of an AP nor of a vRSU and its distance from the nearest AP is $2r$, where r denotes the AP transmission range. This in practice means that a node is allowed to act as a vRSU only when it is at a distance where its MAC layer does not detect any APs above a very low SNR and where it will not interfere with the signal of other APs. We also assume that the MAC layer takes care of solving conflicts and of treats the medium access problem. This application is just one of possibly many others running in the network: this is why the number of messages of the stream application is controlled.

Figure 2 shows a typical scenario where one vehicle receives a message from a real RSU and re-propagates it at another place where there is no RSU available. For all practical purposes we consider that there is no difference between the messages received from a road side AP or a vRSU. The propagation mechanism is cooperative and transparent, from the point of view of the receiver. The system is a best effort one; there are no guarantees that every node will receive all stream packets, but using vRSUs, we aim to increase the chances for timely reception.

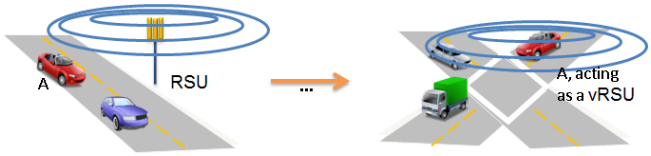


Figure 2. The vRSU technique, nodes that receive a message from a regular RSU, or from a vRSU retransmits it in other areas, where there is no coverage from the regular RSUs. In this scenario node A receives a message from a regular, in order, RSU and re-broadcasts later in a different and uncoverd area. The uncovered areas may be determined by sensing the medium before transmitting.

The proposed technique is powerful and can successfully decrease the uncovered areas, but it has a cost. The cost can be measured in terms of the increase in the number of messages sent through the network. Consider the target message as a limited size stream being generated at a constant bit rate (CBR): this means that during each second n packets, from the total message size ε, are generated from a source and spread through all real APs. Each AP then is in charge of re-broadcasting the received message to the nodes in its area. Assuming that part of the message is transmitted from each antenna just once, the increase in the number of messages sent (im) is upper bounded by:

$$im = \alpha - (nvRSU * \varepsilon), \quad (1)$$

where α is the total number of exchanged messages and may be expressed as:

$$\alpha \leq \beta = (nvRSU * \varepsilon) * t, \quad (2)$$

where β is the maximum number of exchanged messages in each interval of time, $nvRSU$ is the number of virtual roadside units, ε is the size of the warning message and t is the time the warning message is propagated.

IV. THE DEVELOPED TOOL

The objective here is to develop a tool develop a generic tool capable of receiving alert messages from external surveillance networks e.g. SECUNET [14]. SECUNET is the alert network implemented by the RATCOM project to monitor the state of the Mediterranean sea. After receiving the message from the authorities the tool must be able to redistribute it to the nodes in the concerned area regardless the technology such nodes use. In special the tool must be able to implement the vRSU technique to allow an epidemic forwarding of the alert message. Figure 3 presents an example scenario with the main concerned elements. The alert message is received by the server, installed in the backhaul and this node is responsible to retransmit the alert message over the multicast network so that the nodes in the LTE and WiFi networks can receive the alert. The WiFi network represents the WAVE protocol and in this part the messages are retransmitted using the vRSU approach, on the other hand in the LTE part, the tool uses multicast to reach the clients in the connected LTE network.

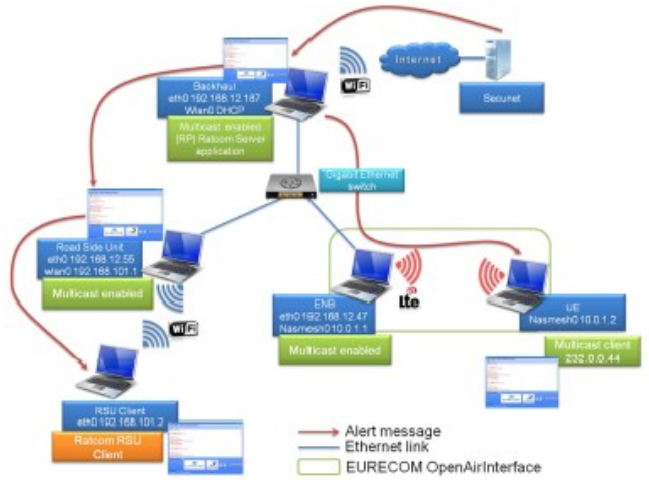


Figure 3. An example scenario where we can see the main components involved in the allert retransmission using the EURECOM allert tool.

We developed the application in java so that it is able to be deployed in a broad range of devices. The tool can use both vRSU and multicast transmit/receive alert messages. The tool is divided in server and client parts. The server is responsible for receive the alerts from the authorities and retransmit it through multicast and vRSU to the near nodes. The clients are responsible for receiving the message, show it to the user and retransmit the message as a vRSU. In this way nodes that are near to one that received the message but are not connected to the main network, will also be able to receive the alert message. Figure 3 shows the window of the server part of the alert message application. As we can see the alert messages are decoded and shown in a comprehensible way to the user. At the same time, automatically, the message is rebroadcasted to the neighbor nodes.

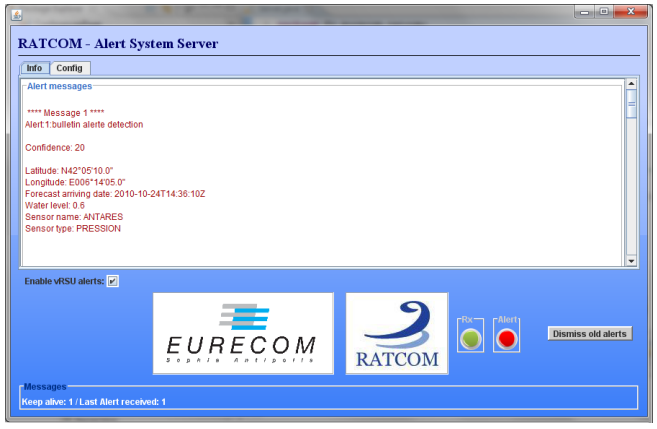


Figure 4. The server window of the alert message tool

The tool has both sides, when running in the main backbone it uses multicast to save bandwidth. However, when running in the mobile nodes it acts as a vRSU to warn the neighbor nodes about the imminent danger. The tool is flexible and easily configurable to receive any kind of alert message. It could even receive regular road alerts, if the deployed RSUs broadcast such messages.

In the tool one can configure the number of times a message will be retransmitted and over which maximum period of time the node should wait until retransmit the message. To collisions the messages have a random back-off that goes from zero to the maximum defined hold time.

V. EXPERIMENTS

The experiments are divided in two parts, in the first part we are interested in verify the impact of multicast over a small network. This will give us an indication of how much we can save using multicast in bigger networks. The developed tool has small data traffic, as it works only with alert messages so the second part will use simulations to evaluate the impact of the vRSU approach in real networks.

The graph of Figure 5 shows the impact of use multicast over an 8 nodes network varying the number of receivers. Even though this is hardly perceived in the graph for one stream the number of messages generated by the use of multicast is slightly bigger than the one generated by the simple transmission of the stream. This is understandable since the multicast protocol has an overhead in terms of messages in the network. However, when we increase the number of receivers the overhead generated by the multicast is largely compensated by the number of saved data messages. On the top of that, the graph shows the number of messages transmitted not the number of bytes, if we considered the number of bytes the difference would be even bigger. Normally the multicast control messages considerably smaller than the data messages. However, here we are considering a small video stream. However, as we can see in the graph of Figure 6 this tendency is not valuable when we are talking about low traffic streams.

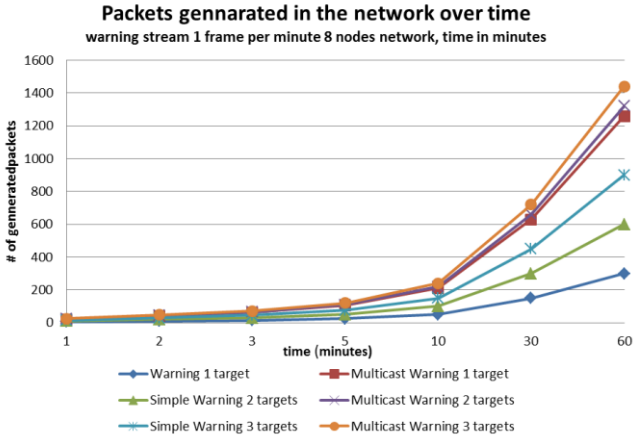


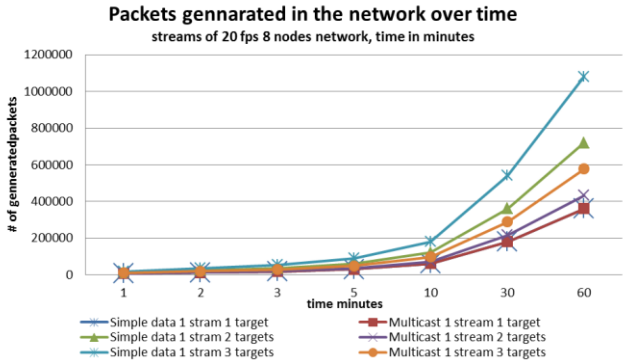
Figure 5. Packets gennrated in a network with 8 nodes and 1 data stream over time.

The warning stream generates one packet at each 1 minute, with or without warning alert, to maintain the multicast running. If we consider this as the data traffic required by the application we can perceive that the use of multicast, only for these alerts, represents a considerable

overhead for the network. In this case it is better to have a mechanism that is on demand, and only when the warning is required the messages are generated. It is exactly what happens with the vRSU part of the tool. In any case even with low data traffic it is important to have the alert network up and running. We could consider that as an insurance, one pays for it even though he/she expects will never need it. In case of a disaster this is the price to pay to be able to efficiently send the important alerts.

Figure 6. Packets gennrated in a network with 8 nodes and 1 warning stream stream over time.

We now present the evaluations made to determine the impact of the vRSU technique over spreading the message



through the network. The simulations were programmed on top of the Sinalgo simulator [10], developed by the Distributed Computing Group at ETH Zurich. All the experiments were conducted using Linux Fedora Core release 6 in an Intel Xeon 1.86GHz machine with 16GB of RAM. The graphs are presented with a five percentile and a confidence interval of 99%. Each point is the result of the mean of at least 34 runs with different network configurations. The scenarios follow a realistic mobility pattern generated with the VanetMobiSim [11] tool.

One of the main objectives of this work is to create techniques that can work even during severe conditions. Considering this, some experiments were conducted to determine the resilience of the vRSU technique in disaster situations. Here we evaluate the impact of disasters in the data transmission when the network is damaged. The tested scenarios evaluate the behavior of regular nodes, before and after the catastrophe. The natural disasters evaluated here are earthquake and flash flooding, whereas the sabotage scenarios are power outage and network random failures. The earthquake is represented by the sudden loss of 80% of the deployed fixed structure. The flash flooding scenario is represented by the removal of all the RSU in a vertical or horizontal direction. In the terrorist attack scenario one RSU nodes is removed randomly at each 3 seconds.

We can perceive in Figure 7 that when no disaster occurred, the number of nodes warned is nearly 100%, regardless of whether vRSUs are used or not. Indeed, the final number of nodes aware of the message is similar, when we do not consider any disaster. We consider transmission cycles of one message per second, i.e. each second the warning message, or a part of it, is broadcasted. The plot shows the time when all nodes in the network received the warning message. Whether all nodes had received the messages or not the simulation experiment stops after 3600 seconds. If any node failed to receive the message within that interval, the registered time is 3600 seconds. Without the use of vRSUs the network needs more than 200 APs to be able to spread the message to all the nodes in less than one hour. With the use of the vRSUs, even in the worst case scenario of an earthquake with only two functional vRSUs remaining, it takes around 20 minutes to spread the warning message over all the nodes in the region.

The tendency is that the time required to spread the warning message decreases when the number of vRSUs increases. However, the gains become comparatively smaller when number of vRSUs increases beyond 50. If we consider the no disaster scenario, if we increase the number of RSUs from 10 to 50 we speed up the message distribution by 28.8%. However, when we increase the number of RSUs from 50 to 500 the gain is 29.8%. I.e. with 50 vRSUs we are able to warn the whole population in 8 minutes, whereas if we increase the number of RSUs to 500, the process will take around 5 minutes. This result is interesting since it shows that the increase in the number of RSUs does not linearly impact the time needed to warn the population over a given target area. This means that we could decrease the number of RSUs, and the cost of the system deployment, without compromising significantly the quality of the service offered.

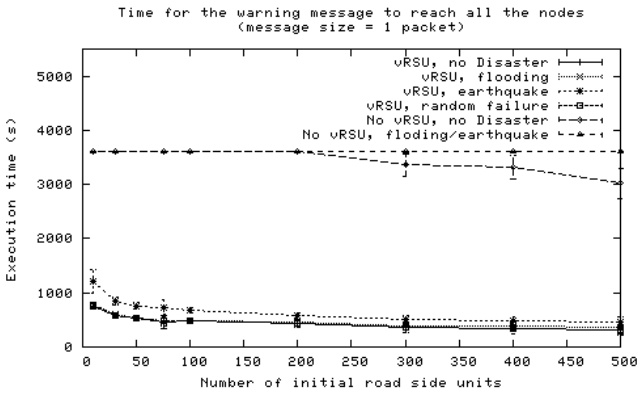


Figure 7. This graph shows the time it takes for the warning message to reach all the nodes in the region. The simulation stops after 3600 seconds, this means that scenarios that had their time registered at 3600 seconds did not deliver the message to all nodes

The experiments show that the proposed method increases the coverage and decreases the time required for all the nodes in the network to receive the message, however this has a cost. One of the ways to measure this cost is counting the number of repeated messages received by the nodes. The graph of Figure 8 shows the average number of repeated messages received by the nodes. The number of duplicated messages is considerably bigger when we use vRSUs. The augmentation in the number of messages is also expected since the algorithm is an epidemic one. However, it is important to call attention to the fact that this traffic occurs in areas that had no communication before.

The number of duplicated messages, observed in the Figure 8, decreases when we increase the number of RSUs. Again, when the area covered by the RSUs increases the areas where vehicles may act as vRSUs decreases. From the same graph we can also observe that, apart from the earthquake scenario, the amount of traffic generated over the different scenarios does not vary significantly. As we can see in formula (2) the overhead is a function of the number of vRSUs not RSUs. The earthquake scenario is a particular case, especially for small numbers of initial RSUs, for two reasons. First because after the disaster the number of APs is extremely small, so the area where vehicles may act as vRSUs is bigger. The second factor is the small diversity of routes, when we have smaller number of APs. A vehicle only starts generating traffic after receiving the first message. When we have a small number of APs the number of sources of traffic is low, and the amount of routes nearby these APs is smaller. Nodes have then more chance of sending the message to nodes that have already received it. The nodes that really need to receive the message are the ones more distant from the AP.

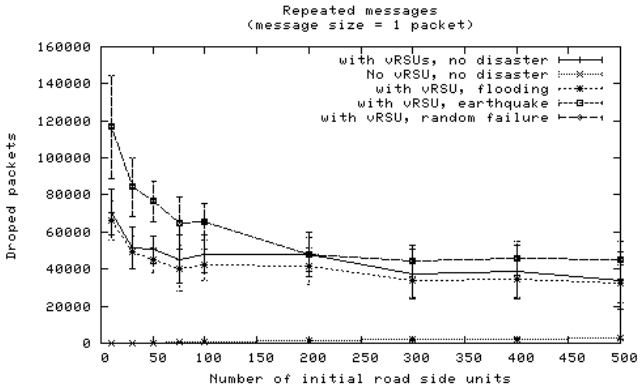


Figure 8. Number of repeated messages received by the mobile nodes during the simulation

VI. CONCLUSION

In this paper we presented a tool for disseminate alert messages over heterogeneous networks. The built application takes advantage of standard multicast as well as a new defined technique based in delay tolerant networks. The experiments show that the technique can reach nodes even if the deployed structure were damaged by a disaster and present uncovered areas.

The tool, successfully received messages over different transmission technologies i.e. LTE, Ethernet and wifi, that was the initial intention of the experiment. The broader is the covered mediums the better will be the chances that, in the future in real disaster situations the users will be able to receive the alert message.

ACKNOWLEDGMENT

This work was partially financed with resources of the Heterogeneous Networks for Public Safety (HNPS) European funded project, within the CELTIC program and with resources of RATCOM project (Réseau d'Alerte aux Tsunamis et submersions CÔtières en Méditerranée)

REFERENCES

[1] A. M. Townsend and M. L. Moss, Telecommunications Infrastructure in Disasters: Preparing Cities for Crisis Communications, Center for Catastrophe Preparedness and Response and Robert F. Wagner Graduate School of Public Service, New York University, May, 2005

[2] ETSI TR102_638, Draft ETSI TR 102 638 V1.0.7, Technical Report, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, June, 2009

[3] 3GPP - 3rd Generation Partnership Project web site, Retrieved Jul 13, 2011, from http://www.3gpp.org

[4] IRTF, IRTF-Internet Research Task Force, Retrieved Jul 13, 2011, from http://www.irtf.org/

[5] DTNRG Delay Tolerant Networking Research Group, Retrieved Jul 13, 2011, from http://www.dtnrg.org/wiki

[6] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass and, J. Scott, Impact of Human Mobility on Opportunistic Forwarding Algorithms, IEEE Transactions on Mobile Computing 6, 6, Jun, 2007

[7] IPNRG, InterPlanetary Internet Special Interest Group, Retrieved October 18, 2009, from http://www.ipnsig.org/home.htm

[8] K. Fall, A Delay-Tolerant Network Architecture for Challenged Internets, In ACM SIGCOMM, Karlsruhe, Germany, August, 2003

[9] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott. Pocket Switched Networks: Real-world mobility and its consequences for Opportunistic Forwarding. Technical Report UCAM-CL-TR-617, University of Cambridge, 2005

[10] Distributed Computing Group at ETH Zurich, Sinalgo - Simulator for Network Algorithms, Retrieved Jul 13, 2011, from http://disco.ethz.ch/projects/sinalgo/

[11] J. Harri, M. Fiore, F. Fethi, and C. Bonnet, VanetMobiSim: generating realistic mobility patterns for VANETs, in Proc. of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET'06), Los Angeles, USA, September 29, 2006

[12] Holma, Harri, Toskala, Antti, LTE for UMTS, Evolution to LTE-Advanced, John Wiley & Sons, 2nd Edition, March 2011

[13] IEEE P1609.0: Standard for Wireless Access in Vehicular Environments (WAVE) – Architecture

[14] Thales Alenia Space, Manuel utilisateur pour les abonnés du réseau Secunet, Référence du livrable RATCOM : SP4D4, 13/10/2010