

Fast and safe emergency communication through network virtualization

Peter Dedecker^{*†}, Jeroen Hoebeke^{*}, Dries Naudts^{*}, Ingrid Moerman^{*},
Joris Moreau^{*†}, Piet Demeester^{*}

^{*}Ghent University – IBBT – IBCN
Department of Information Technology (INTEC)
Gaston Crommenlaan 8 bus 201, 9050 Gent, Belgium
name.surname@intec.ugent.be

[†]University College Ghent
Department of Applied Engineering Sciences
Schoonmeersstraat 52, 9000 Gent, Belgium
name.surname@hogent.be

ABSTRACT

In this paper we introduce the Virtual Private Ad Hoc Networking platform as an integrated solution for emergency communication and applications. This platform creates a virtual logical self-organizing network on top of existing network technologies reducing complexity and facilitating immediate availability. The architecture and its features will be explained in detail and matched against the specific communication needs of emergency applications.

Categories and Subject Descriptors

C.2.1 [Computer-communication networks]: Network Architecture and Design — *Distributed networks, Network topology, Wireless communication*

General Terms

Design, Experimentation, Management, Reliability, Security

Keywords

mobile, broadband, networking, security, wireless, ad-hoc

1. INTRODUCTION

For emergency workers, a permanent connection enabling voice and data communication, is a key element determining the success of the mission. The internet, which is nowadays becoming a large “network of networks” with its broad spectrum of different wired, wireless and mobile communications and technologies, offers ubiquitous connectivity. Nevertheless, it may be clear that these large-scale communication networks are not direct suitable for emergency applications as they require technological skills and very precious configuration and management time.

Reducing this configuration and management complexity must be the key feature of our communication platform.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IWCMC'09 June 21-24, 2009, Leipzig, Germany

Copyright 2009 ACM 978-1-60558-569-7/09/06 ...\$5.00.

However, emergency scenarios don't need this complex internet as such. They just need a permanent secure connection between a dynamic subset of distributed and mobile devices with a limited number of crucial applications, using the available (heterogeneous) infrastructure, appended with their own infrastructure.

Therefore, we see interesting opportunities in the expected evolution towards network virtualization, where a logical structure is built on top of these base networks [5, 4]. Such small and secure logical overlay networks, grouping the previously mentioned subset of devices and making the underlying base network invisible, create a shielded and trusted environment for their participants. Enhancing them with ad hoc protocols and techniques can result in self-creating, self-organizing and self-administering communities, on top of existing network infrastructures, drastically reducing complexity so their users can focus on their main task: the emergency intervention.

Our solution, the Virtual Private Ad Hoc Networking (VPAN) platform as described in [8] and [7], is developed with these key insights as main drive: virtual overlay networks, consisting out of a subset of devices sharing a common trust relationship, provide a secure, transparent and self-administering network built on top of available heterogeneous networks. Applications and services can be given access rights to such an overlay, thereby operating within this secure and confined environment.

In this paper we will first highlight some key features an emergency application requires from its communication solution in section 2. In section 3, the VPAN concept is explained in more detail after which a matching of the VPAN features against the earlier mentioned requirements is done in section 4, providing a concrete example. A conclusion is stated in section 5.

2. EMERGENCY COMMUNICATION REQUIREMENTS

In emergency situations, time is crucial. Especially during the golden hour, every gained minute can save many lives. So efficient communication and data exchange is of great importance. A continuous communication platform providing voice and data allows emergency workers to agree on intervention strategies while on the road, thereby viewing intervention plans and updated stock lists of dangerous goods on a mobile device. Permanent updates of a dynamic geographical information system (GIS) and crisis management

system like developed in the GeoBIPS [2] and ADAMO [1] projects enriches this data exchange and provides the authorities with concise and exact information in real-time.

Upon arrival on site, this communication platform must allow very fast deployment to all individual emergency workers, providing instant ad-hoc usage. No time may be lost setting up complex infrastructures. We can't expect emergency workers to have any technical knowledge, nor do they have time to handle network administration on their devices. Their only focus is the intervention itself. Therefore, ease-of-use stays important.

A first group is sent out to explore the site. Permanent reliable communication with this group, as well as other team members on-site, stays crucial. Our network, growing in space as team members get scattered on location, must be able to handle mobility without user intervention. Self-organization, self-maintenance, self-optimization and self-healing capabilities are necessary. When coverage gets lost, additional communication equipment must be setup, again without technical knowledge or user administration. Also here is communication and data exchange important to provide other team members and especially the commanding officer with a good view off the situation. Streaming video capabilities can be a great help.

Over time, the needs of the emergency network evolve. In the very first phase, rapid deployment, using highly portable, small, lightweight equipment by non-technical users is a key requirement. In this phase most communication is voice-based between the end-user and the headquarters (HQ), while also initial access to the emergency management application is necessary. However, in a second phase, cooperation gains importance as other teams get involved. Commanding officers need permanent communication lines with their colleagues as well as their team members, without both groups getting mixed or overwhelmed with information that wasn't mentioned for them. Different fenced but interoperable communication groups are necessary.

Increased activities demand for increased access to the emergency management application and thus a higher bandwidth. Therefore we must be able to use and combine different available network technologies, like TETRA, WiFi, GPRS, UMTS, WiMAX or even an ethernet or DSL-connection from a nearby building.

Of course, our networking platform must be flexible and future proof in order to support different kinds of applications. No restrictions on the application level are allowed.

Last but not least: security is a key requirement. Emergency communication should be shielded from other applications using the same shared medium. Not only to reduce complexity and information overwhelming to other present teams, but in the first place to protect the intervention and all involved parties from intrusion or information leakage. Eavesdropping paparazzi or sabotage through the used communication platform must be impossible.

3. THE VPAN CONCEPT AND FEATURES

As mentioned in the introduction, the VPAN concept is based on the creation of a virtual overlay network consisting of a selected subset of permanently connected trusted devices. Nodes in the overlay network or VPAN can be thought of as being connected by virtual or logical links. These virtual links correspond to a path in the underlying network, perhaps through multiple physical links. Such an

overlay network drastically reduces size (in terms of connected devices) and complexity. Participating devices can join multiple overlay networks. In each VPAN, a node can share selected services or resources. A graphical illustration of the VPAN concept is given in figure 1 and will be explained in the following paragraphs.

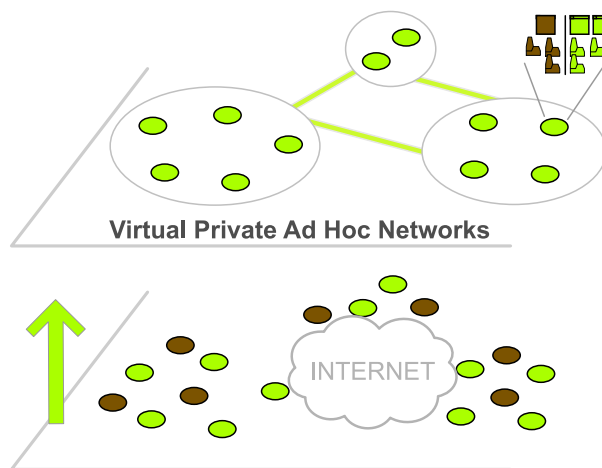


Figure 1: The VPAN concept.

All devices participating in an overlay network must share a common cryptographic trust relationship. In our implementation a public and private key pair with a certificate signed by the certification authority of this particular VPAN is used. These must be installed in advance on all nodes together with the necessary configuration parameters like used routing protocols and VPAN Agent (see further) location. Users do not have to change anything after these initial steps no more.

At first, all devices start sending beacon packets at regular time intervals on their PAN (Personal Area Networking) interfaces which allows them to detect each other. These PAN-interfaces are (preferably wireless) interfaces especially for nearby communication like (ad hoc) WiFi or bluetooth. Upon receipt of such a beacon packet, a challenge-response mechanism is initiated to validate both certificates and negotiate a symmetric session key resulting in a secure link between both nodes. This process is called neighbor detection and illustrated in figure 2.a. All nodes keep track of their neighbors in an internal neighbor table. After a certain timeout (currently 2.5 beacon interval) without receiving beacon packets from a neighbor node, the corresponding node is deleted from the neighbor table and the secure link is considered as broken. Neighbor detection with this beaconing mechanism can occur on different kinds of PAN-interfaces of different technologies.

All these nodes that have (OSI layer 2) link connectivity, set up secure links to each other. Nodes who do not rely on non-trusted nodes for their communication, form a cluster. Within this cluster, all nodes can reach each other using an intra-cluster ad hoc routing protocol. Proactive as well as reactive protocols are available. These ad hoc routing protocols combined with the neighbor detection are the key components to deal with changing topologies within a local cluster. The underlying technology can vary: WiFi, Bluetooth and ethernet are supported. Especially for WiFi interfaces, we developed a wireless autoconfig system which

scans all channels for VPAN ad hoc essids¹. If such a network is found, it is joined. Otherwise, a channel is selected and a new ad hoc essid is created waiting for other nodes.

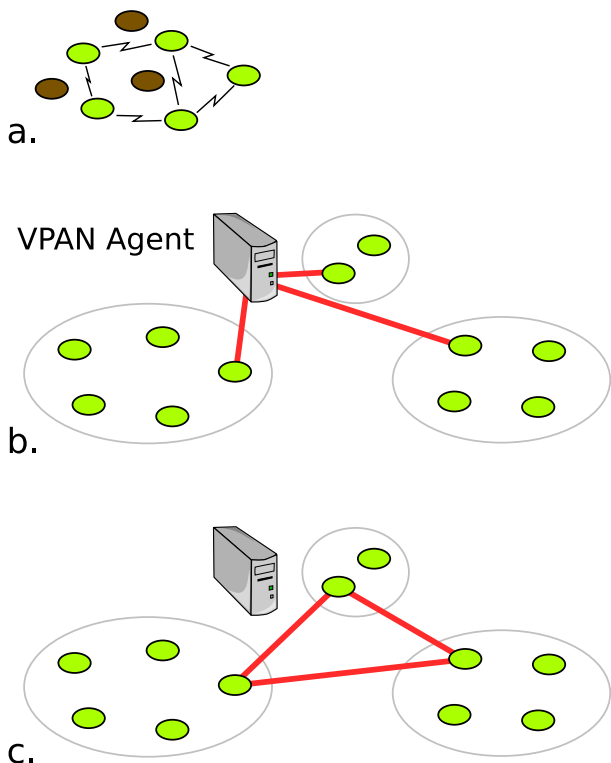


Figure 2: VPAN creation: a. Neighbor discovery; b. Cluster registration; c. Tunnel negotiation

Secondly, clusters on different geographic locations connect to each other using secure IP-tunnels. Network interfaces on nodes connected to the internet and used for inter-cluster communication are called Wide Area Network or WAN interfaces. Also here, the underlying technology doesn't matter as long as it is IP-capable. WiFi, WiMAX, TETRA, UMTS, GPRS, HSXPA or fixed ethernet, DSL or cable connections are possible. These nodes with internet connectivity (which are called gateway nodes) contact a public available VPAN Agent, providing their current public IP address as illustrated in figure 2.b. Of course, also this process is secured based on public key encryption using the corresponding VPAN-certificates. After authentication, the Agent provides the node with all necessary information (public addresses and ports of corresponding gateway nodes) to reach the other clusters. This way, gateway nodes can (proactively or reactively) setup tunnels to all other gateway nodes, establishing the whole VPAN and providing connectivity between all nodes as seen on figure 2.c. The tunneling mechanism is capable of bypassing certain NAT² and firewall obstructions using hole punching mechanisms. When none of these approaches succeed, all inter cluster traffic to that cluster is routed by the VPAN Agent which is always public reachable.

Nodes leaving or joining clusters are signaled by the gateway node to the agent, so other gateway nodes and inter

¹Extended Service Set Identifier: wireless network name

²Network Address Translation

cluster routing protocols can be informed of this topology change. For communication involving two nodes from two different clusters, inter-cluster ad hoc routing protocols are used. A proactive as well as reactive protocol is available and optimized to deal with this hierarchy based logic.

To reduce complexity, private addressing is used in the VPAN. A node is assigned one private IP address, which can be static or dynamically generated but stays the same during the whole VPAN lifetime. Changes in underlying networks and network interfaces aren't reflected in the overlay network's private addresses. These changes are handled by our Universal Convergence Layer, which encapsulates the encrypted VPAN packets into OSI L2 packets who are actually sent out on the PAN-interface(s) with the MAC-address of the corresponding neighbor as destination address.

Thanks to this fixed private addressing, applications don't have to deal with changes in the network (eg. due to mobility) and their connections keep alive. For example when a link break occurs, the neighbor detection mechanism triggers the routing protocol to establish a new route through other hops in the cluster or to set up a tunnel to the cluster when no intra-cluster routes are possible. These route updates are done within most TCP time out intervals, meanwhile buffering packets so no packets and no TCP-connections get lost. Cluster-wide and VPAN-wide broadcasting is supported using pre-defined broadcast addresses.

The VPAN platform also contains a service announcement and discovery protocol. Nodes can share services and resources in a VPAN, which can be discovered and used by other nodes. A graphical user interface is developed which allows sharing and remote launching of services with a single click.

Currently, the VPAN-software is available for different operating systems including Linux, Mac OS X and Windows as well as Maemo, which is a linux variant for the Nokia internet tablets. Also a version for the Neo Freerunner smartphone is under development. The software is deployed on a testbed consisting of multiple clusters and multiple overlay networks, while the used routing protocols are tested on a simulator as well. Currently, the software is being tested on a real large scale using the Virtual Wall and Wireless lab of the i-Lab.t Technology Center [3] at IBBT. Results and details of performance measurements of the VPAN implementation on a small scale can be found in [7].

4. MAPPING THE VPAN TOPOLOGY ON EMERGENCY SCENARIOS

In our view, all emergency workers are organized in teams, using their own VPAN. All nodes used by a certain team have the VPAN software pre-installed and pre-configured. Certain services (eg. location-service providing the current GPS-position) can be shared in the VPAN, next to Voice-over-IP (VoIP) services as well as an emergency management service and GIS-services installed in the backend.

Different teams, eg. the firemen and medical team, use their own VPAN. This way they can share the same medium (eg. a hotspot in the neighborhood) in a secure way, not interfering eachother. Some nodes can participate in multiple VPANs. For example team leaders can participate in an emergency coordination VPAN as well as their own team VPAN. An illustration of this partitioning in VPANs is provided in figure 3.

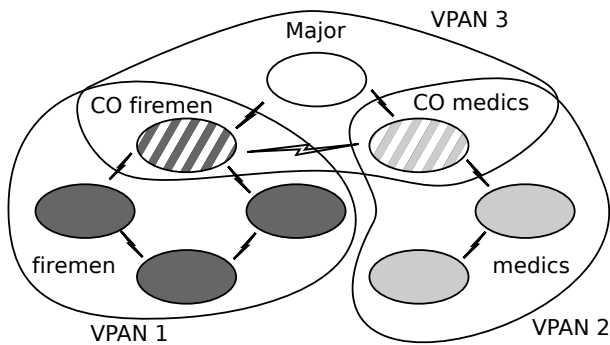


Figure 3: Possible VPAN partitioning

If two teams don't have a pre-configured shared VPAN for their commanding officers, they have to create one. Therefore they log in to a VPAN portal page, create a new VPAN and add their device to the VPAN. The portal automatically configures the VPAN Agent and delivers a configuration package to the users who just have to open this file in order to install the new VPAN. Also here: almost no technical knowledge is required, as can be seen in figure 4.

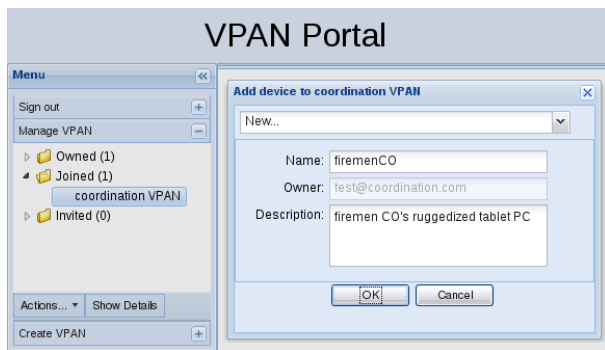


Figure 4: The VPAN portal: adding device to VPAN

When, for example, a fire brigade receives a call, the firemen can immediately leave the headquarters by truck. At the HQ, the responsible person prepares all documents and databases (eg. current stock of dangerous goods) while the firemen in the truck can inspect the emergency entrances of the site on their mobile devices. They are all member of the same VPAN, organized in a mobile cluster after detecting each other by beacons and using their own 3G connection or the TETRA connection of the truck as tunnel interface to the HQ. Of course, all traffic between those devices in the truck remains intra-cluster. All devices stay connected the whole time, but depending on the used routing protocol and its quality of service capabilities, one WAN interface can be preferred over another one [6]. Eventually, the HQ can send a VPAN-wide broadcast stream to all devices using the VPAN-wide broadcast address. Note that all necessary information is received while driving towards the site, saving very precious time. We refer again to the devices, interfaces and management applications developed in the GeoBIPS [2] and ADAMO [1] projects.

Upon arrival, all devices remain interconnected and all services remain available. No deployment time or knowl-

edge is required. Eventually, a gateway node can choose to connect to other available networks (like a WiFi hotspot) in order to gain more bandwidth. However, thanks to the private addressing and self-organization, this has no impact on other nodes. No knowledge is required as the VPAN automatically handles this setup of new tunnels to the agent and backend and immediately routes the traffic through these new tunnels. Other connections (eg. a TETRA connection) can remain active but at a lower usage rate.

A first team can be sent out to explore the site. When those mobile nodes get too far away from the other ones in the cluster, a link break occurs and the cluster splits. Those link breaks are detected, which triggers the routing protocol(s) to setup a new route using a tunnel over the 3G connection to the mobile nodes. The mobile users won't even notice this as their application level connections remain active. During lab tests, a voice over IP (VoIP) connection or video stream was disrupted for a few seconds when switching between wired and WiFi connections. Obviously, this depends on the neighbor discovery parameters³ and the underlying technology. If this 3G connection is insufficient to transfer all necessary data (eg. to send a live video stream to the commanding officer (CO) and HQ to give them an accurate view on the situation inside a building), more bandwidth can be achieved by extending the coverage of the local wireless network. Therefore we can place additional intermediate nodes extending the cluster. [10] describes an easy placement method of these intermediate nodes, also requiring no technical knowledge. An illustration is provided in figure 5.

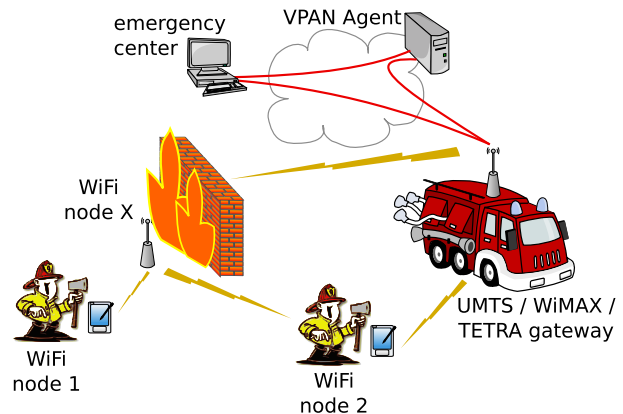


Figure 5: Physical network on-site

During an intervention, each member of the fire brigade has a specific role, requiring different kinds of mobile devices and graphical interfaces. For example the commanding officer (CO) will coordinate the team, but will not take part in explorations. It is essential that he has an overview over the situation and knows the status of the different team members of the fire brigade. In the GeoBIPS project [2] each firefighter is provided with a ruggedized PDA while the CO has a ruggedized tablet PC providing a bigger screen. User friendly graphical interfaces for this special purpose are developed and described in [9].

³Keep in mind that all parameters, for example the link break time out interval, can be adapted in advance resulting in more overhead but also in a more stable connection

If other teams from possible other disciplines arrive, they can share the same access network used by the first team. As all VPAN traffic is encrypted, shielded away from the internet and other VPANs, they won't get overwhelmed with all ongoing information traffic and won't introduce misunderstandings. Also arriving paparazzi equipped with frequency scanners or with access to the used shared medium have no chance to eavesdrop the internal communication. When intermediate nodes disappear (eg. destroyed by fire, water or other problems), the used access network doesn't result in communication drops as the VPAN will re-route all traffic (again) over other (eg. 3G) interfaces.

Through the use of private addressing, all currently available applications can be used. These applications can be limited (by a firewall or the application itself) to only work on the private address range and thus be only available in the overlay network. Launching services (eg. a dangerous goods catalog) is very easy thanks to the built in service discovery framework: applications can be launched with a single click.

A coupling between the local VoIP communication and regular TETRA telephone radios can be made using a VoIP-TETRA gateway on the truck developed in the IBBT ADAMO project [1].

In this example, the VPAN Agent may be a single point of failure, especially in nature disasters. Further research is necessary to create a synchronized distributed implementation with available fallback servers in case of failure on the first server.

5. CONCLUSION

In this paper we described the Virtual Private Ad Hoc Networking technology and matched its features against the requirements of emergency communication networks. The VPAN seems a very promising technology for these applications. Its self-configuring, self-maintaining, self-optimizing and self-healing capacities make it an ideal solution for quick set up in dynamic environments by users without any technical knowledge and who don't have to care about network connectivity. Also the security demand is met in the VPAN platform. Enhanced with other technologies like [10] and [1], a very stable and usefull communication strategy can be developed enhancing better information gathering, more efficient time usage in the golden hour and thus saving many lives and reduce material damage.

6. ACKNOWLEDGEMENTS

This research is partly funded through the ITEA2 UseNet (Ubiquitous M2M Service Networks) project and the Interdisciplinary Institute for Broadband Technology (IBBT) projects GeoBIPS and ADAMO. Peter Dedecker is research assistant at University College Ghent and affiliated researcher at Ghent University.

7. REFERENCES

- [1] IBBT ADAMO website. Advanced Disaster Architecture with Mobility Optimizations. <http://www.ibbt.be/en/project/adamo>.
- [2] IBBT GeoBIPS website. Geographical Broadband Integration for Public Services. <http://www.ibbt.be/en/project/geobips>.
- [3] iLab.t Technology Center @ IBBT. <http://ilabt.ibbt.be>.
- [4] T. Anderson, L. Peterson, S. Shenker, and J. Turner. Overcoming the internet impasse through virtualization. *Computer*, 38(4):34–41, April 2005.
- [5] K. P. Birman. The next-generation internet: Unsafe at any speed? *Computer*, 33(8):54–60, 2000.
- [6] P. Dedecker, J. Hoebeke, I. Moerman, J. Moreau, and P. Demeester. Multipath routing issues in virtual private ad hoc networks. *Personalized Networks, 2009. IEEE CCNC '09. Workshop on*, 2009-Jan 13 2009.
- [7] J. Hoebeke. *Adaptive ad hoc routing and its application to virtual private ad hoc networks*. PhD thesis, Ghent University, 2007.
- [8] J. Hoebeke, G. Holderbeke, I. Moerman, B. Dhoedt, and P. Demeester. Virtual private ad hoc networking. *Wireless Personal Communications*, 38:125–141, 2006.
- [9] K. Luyten, F. Winters, K. Coninx, D. Naudts, and I. Moerman. A situation-aware mobile system to support fire brigades in emergency situations. In *OTM Workshops (2)*, pages 1966–1975, 2006.
- [10] D. Naudts, S. Bouckaert, J. Bergs, A. Schoutteet, C. Blondia, I. Moerman, and P. Demeester. A wireless mesh monitoring and planning tool for emergency services. *End-to-End Monitoring Techniques and Services, 2007. E2EMON '07. Workshop on*, pages 1–6, 2007-May 21 2007.