An integrated approach to fast and secure emergency communication

Peter Dedecker

Supervisor(s): Jeroen Hoebeke, Dries Naudts, Ingrid Moerman, Joris Moreau, Piet Demeester

I. Introduction

In this paper, we list up the specific requirements of emergency communication. As the internet with its broad spectrum of different technologies and its required technological skills and very precious configuration and management time is not suitable, we introduce the Virtual Private Ad Hoc Networking (VPAN) platform as described in [1] as a solution to these needs.

II. Emergency communication requirements

In emergency situations, time is crucial. 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 stock lists of dangerous goods on a mobile device with real-time updates. On site, fast deployment, is required. Time neither technical knowledge are available to set up complex infrastructures. As a first exploration group is sent out, permanent reliable communication stays crucial and streaming video can deliver better insights. Mobility without user intervention is necessary, next to self-organization, self-maintenance, self-optimization and self-healing capabilities. When other teams arrive on site, commanding officers (CO's) need permanent communication lines with their colleagues as well as their team members, without both groups getting mixed or overwhelmed with information. Over time, more bandwidth will be needed. Therefore we must be able to use and combine different available additional network technologies. Of course, our networking platform must be flexible and future proof with security in mind.

III. The VPAN concept and features

The VPAN concept creates virtual overlay networks 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. In each VPAN, a node shares selected services or resources. A graphical illustration of the VPAN concept is given in figure 1.

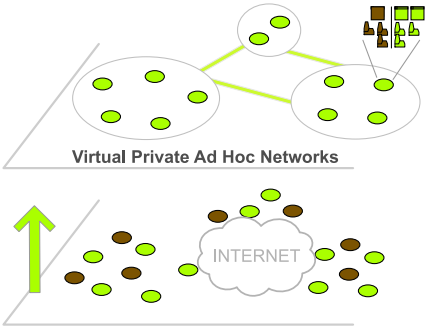

Figure 1. The VPAN concept.

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. E-mail: Peter.Dedecker@hogent.be

All devices participating in an overlay network share a previously installed common cryptographic trust relationship, namely a public and private key pair with a certificate signed by the certification authority of this particular VPAN. Users do not have to change anything after these initial steps no more.

All devices detect their neighbours by sending (OSI L2) beacon packets on different devices to initialize a challenge-response session and set up a secure link and form a cluster in which all nodes can reach each other using an intra-cluster ad hoc routing protocol without non-trusted intermediate nodes. Nodes connected to the internet contact a public available VPAN Agent, providing their current public IP address, in order to set up tunnels to all other gateway nodes and clusters.

Each node is assigned one private static VPAN IP address so applications do not have to deal with topology changes: their connections keep alive and no TCP-connections get lost. A service announcement and discovery protocol enables nodes to share services in a VPAN which can be discovered and used by other nodes.

IV. Mapping the VPAN topology on emergency scenarios

In our view, all emergency workers are organized in teams, using their own (pre-installed) VPAN and shared services like the current GPS-position, Voice-over-IP (VoIP) and GIS-services installed in the backend. CO's nodes participate in their team's VPAN as well as a sort of CO-VPAN.

Thanks to the permanent communication, firemen can immediately leave the headquarters by truck while inspecting the emergency entrances of the site on their mobile devices as they are sent by the HQ-team. They can use their own 3G connection or the TETRA connection of the truck as tunnel interface to the HQ.

On site, no deployment time or knowledge is required. A gateway node can connect to other available networks (like a WiFi hotspot) in order to gain more bandwidth. Additional intermediate nodes can be placed to extend the high bandwidth cluster as they are detected immediately thanks to the neigbour detection mechanism. When link breaks occur or intermediate nodes get destroyed, the routing protocol(s) set up a new route using a tunnel over the 3G connection to the mobile nodes without much interruption.

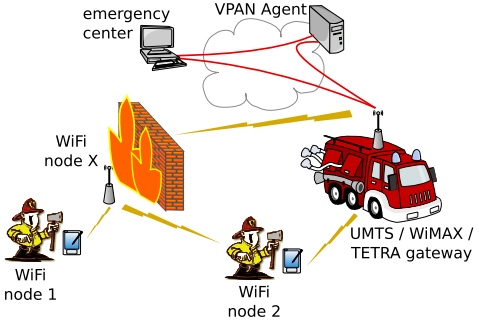

Figure 2. Physical network on-site

Other teams from possible other disciplines can share the same access network used by the first team as all VPAN traffic is encrypted and shielded away from the internet and other VPANs. Through the use of private addressing, all currently available applications can be used and limited (by a firewall or the application itself) to only work on the private address range of the overlay network.

V. Conclusion & status

The VPAN technology seems a very promising technology for emergency applications due to its possibilities for a quick secure set up in dynamic environments by users without any technical knowledge. and who don't have to care about network connectivity. Currently, the VPAN software is implemented and tested while functionality is being added and research on advanced multipath routing is being done.

References

[1] Jeroen Hoebeke, *Adaptive ad hoc routing and its application to virtual private ad hoc networks*, Ph.D. thesis, Ghent University, 2007.