Case Study for a HighLy Portable Mesh nEtwork (H.L.P.-M.E.)

L. P. O. Sousa[1], S. J. Bachega.[3], J. Martins Jr.[4], A. C. Oliveira Jr.[2], M. A. Batista[2], T. A. Santos Filho[2], S. F. da Silva[2] and D. M. Tavares[2]
[1]Industrial Mathematics Department, Federal University of Goiás (UFG), Catalão, Goiás, Brazil
[2]Computer Science Department, Federal University of Goiás (UFG), Catalão, Goiás, Brazil
[3]Production Engineering Department, Federal University of Goiás (UFG), Catalão, Goiás, Brazil
[4]Computer Engineering Department, College of Campinas (FACAMP), Campinas, São Paulo, Brazil

Abstract— *In this paper, we explore a prelude implementation for a portable wireless mesh network, intended to enable multimedia communication with no onsite infrastructure. This is intended as a perimeter network for the fast and secure communication of devices (e.g. robots, IP cameras, notebooks, wifi sensors, etc.) in an environment with no network coverage (e.g. due to a natural disaster, as communication support during a sting operation etc). This kind of environment must be simple to configure, and it must support some kind of mesh network implementation for easy deployment. We estimate that by owning such communication infrastructure, for instance, law enforcement agencies would be able to perform a diverse scope of operations in an easy and efficient manner, preferably in the context of a MAN, which must be independent of landlines, and would allow for the transmission of multimedia data seamlessly (e.g. audio, video, GPS coordinates etc).*

Keywords: portable wireless mesh network, B.A.T.M.A.N.

1. Introduction

Wireless Mesh Networks or WMNs are computer networks that interconnect a set of nodes, where each node is capable of forwarding packets, until they reach a given destination. Therefore, each node can act as a router or client allowing for more mobility and flexibility regarding the infrastructure organization [1].

Mesh routers are capable of communicating heterogeneous networks, like sensor networks (assuming one of the mesh nodes acts as a sink) and usual wifi devices. Besides, one of the nodes can share Internet access to a whole section of the mesh (depending on the size of the mesh network). Mesh nodes can also automatically establish a backbone network and keep the connectivity among mesh clients [2]. In comparison to a conventional router, a mesh router achieves the same range at a lower transmission power, thanks to multi-hop communication. Mesh clients usually have only one network interface and act as both end users (i.e. with Internet access) and routers [3]. Mesh nodes traditionally use the IEEE 802.11 standard [4] in order to communicate.

After the rise of Wi-Fi, lots of applications that partly used landlines were developed. Using as motivation the need to improve the services offered by wireless networks and also to reduce the dependency of landlines, the mesh concept emerged [5]. This technology is already in widespread use, for example, in community or food squares, airports, shoppings, hotels, isolated places (e.g. mountainous regions), universities etc. There are scenarios where this technology is used in a more broad fashion, as in the Dharamsala community in India, where a mesh network was deployed. According to [6], even with a mountainous terrain and with more than two thousand computers interconnected, the performance was satisfactory in the devised tests. Microsoft's Self Organizing Wireless Mesh Networks project uses the user's computer with a Windows driver, which creates a virtual layer between the network and data link layers. This project also has a framework to manage mesh network failures. The analysis is done by event simulations allowing the diagnostics of problems and traffic conditions [7]. RoofNet is another project that deploys a mesh network in a densely populated 4 square kilometer area at Cambridge, Massachusetts, using volunteer users and 37 mesh node kits, in order to share a fraction of their DSL lines [8]. According to [9], systems based on mesh architecture are a viable solution when compared to a hypothetical single-hop network. In this sense they increase the connectivity and the data transfer rate.

The rise of wireless mesh networks is due to its advantages when compared to the traditional wireless network model. The main advantage is the easiness of expansion thanks to the possibility of a mesh client acting also as a router. This turns this network model easy to deploy and low cost allowing access to places where cabled networking would be impracticable [6].

The effectiveness of any network architecture, including mesh networks, depends on the routing protocol used. The routing protocol is the responsible for transmitting information from a source to a destination hopping through intermediate nodes [10]. The challenge is to find the most effective route. In this paper we present the behaviour and the features of the Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.) protocol and define as hour

research hypothesis the possibility to implement a highly portable mesh network using off-the-shelf cost effective equipment with minimum downtime for configuration.

In the next sections we will present the theoretical background behind mesh networks, a brief explanation of the B.A.T.M.A.N. protocol, given it is used in our experimental testbed, the application context for our proposal and some final thoughts regarding our proposal.

2. Theoretical Background

A traditional computer network contains a centralised controller for each node. In a mesh network there is no need for a controller, taking into account that the users themselves can expand the coverage area [12]. Therefore, mesh networks present a dynamic feature, in which by adding or removing nodes in the network does not compromise the network connectivity. That happens because the nodes can be connected to more than one node, and that way, the network cost decreases considering there is no need for a more "formal" maintenance policy [5].

The topology of a traditional network obeys a hierarchy where the devices can only be accessed inside of their coverage area. In a mesh network, the network topology is defined in such a way that all the devices in the network can be a part of the transmission path [15], resulting in a more effective transmission. Besides, mesh networks are also fault tolerant [1], due to the mesh nodes' capabilities to act as clients or routers, allowing a variety of paths among nodes during packet transmission. Other mesh network feature is the support to ad-hoc networking, which is an operational mode that provides the ability to self-generation, self-maintenance and self-organization [16]. Note that the main characteristics of mesh networks, like flexibility and lack of a predefined infrastructure, are appropriate to the proposal of this article. In the US, this technology is already being used in military applications, seeking a communication infrastructure that is independent of the traditional landlines and also fault tolerant [18].

A lot of research fields in mesh networks involve the the study of routing protocols. Although there are several protocols, there is no universal choice [10]. The routing protocols operate generally in the network layer, where their main function is to issue packets from a source node to a destination node. The protocol also specifies the way the routers communicates among themselves, giving access between any two nodes in the network [19]. The problem of classic routing protocols is that they were not created considering the features of ad hoc wireless networks. This genre of network changes its topology according to the inclusion/exclusion of nodes, fact that was not envisioned in traditional routing protocols. For instance, Optimized Link State Routing Protocol (OLSR) had to go through some changes in its original specification, due to the specifics of a link state algorithm which has to recalculate all the topology for each node [20].

In this context, our research group studied applications and the principles involved in creating routing protocols applied to mesh networks [13], [14]. Each routing protocol is devised using different principles and features. To help comprehend these differences, the protocols are classified in proactive, reactive and hybrid. The proactive protocols are based on predefined tables that keep track of the routes for any possible destination and are updated at each topology change. Protocols like Wireless Routing Protocol (WRP) and OLSR are examples of proactive protocols. Reactive protocols stipulate that each node only keeps track of its neighbours when there is the need for it to communicate, a bigger delay is only generated if a new path is necessary. Dynamic Source Routing (DSR) is an example of such type of protocol. Hybrid protocols use conveniently the features of both proactive and reactive protocols, in such a way that in a set of nodes, only some of them do a periodic update of the possible destinations. An example of such protocols is Zone Routing Protocol (ZRP) [5], [14]

B.A.T.M.A.N. is a proactive protocol that identifies only the best next hop instead of discovering the complete route [21], [22], [23], [24]. Therefore, there is no need for the global knowledge of all the changes in the network topology. Besides, the overall number of messages that floods the mesh topology is limited, avoiding control traffic overload [20]. Considering the intended scenario (most likely some kind of sting operation performed by the authorities), B.A.T.M.A.N. seems as one of the possibilities for a routing protocol with its performance improved given the use of a limited quantity of mesh nodes for temporary coverage of an area for a short period of time. Internet connection is not an issue for the sake of the depicted scenario. Besides, according to [28], a high node density limits the network ability to cope with a large amount of hops in the transmission path. Therefore, the relatively short number of hops for this kind of deployment favours the use of B.A.T.M.A.N.

2.1 B.A.T.M.A.N. Protocol

B.A.T.M.A.N. routing protocol was devised to operate in non-reliable media with high levels of instability and packet loss, instead of the stable and reliable media used by traditional cabled networks. The protocol's algorithm proposes the decentralization of the knowledge about routes among B.A.T.M.A.N. nodes. These nodes have no information whatsoever regarding the overall network routing, allowing low battery and CPU consumption for each node. Instead of discovering the complete route to the destination node, a router only identifies the best next hop to achieve a given node. A node detects the presence of B.A.T.M.A.N.-Originators, regardless of the number of hops (single-hop or multi-hop) to/from an B.A.T.M.A.N.-Originator. It also keeps track of new B.A.T.M.A.N.-Originators and informs

its neighbours about their existence [25].

Originator Messages (OGMs) inform neighbouring nodes about their existence. The messages must be transmitted in a given time interval (ORIGINATOR_INTERVAL). An OGM packet has a field for: its version, a field to inform if the node is a direct neighbour or not, an unidirectional flag, a desired value for the Time-To-Live (TTL), a gateway flag (to inform if it is a node with Internet access), a sequence number used for the packet identification and an originator address (IPv4 address of the B.A.T.M.A.N. interface on which the OGM has been generated). When a node receives an OGM it must check: if the OGM contains the same version, if the OGM address is not the broadcast address of a B.A.T.M.A.N. interface and if the OGM is defined as a bidirectional link (capable of full-duplex communication) [25].

If the previous conditions are met, OGM information must be updated. If the sequence number of the received OGM packet is more recent than the one seen before, the new sequence number must be defined to the sequence number of the received OGM packet, and the last TTL of this neighbour must be updated. The window of all known links of the OGM packet must be updated to reflect the new boundaries of the classification range, and the sequence number of the received OGM must be added to the window that represents the link that was held. If the link window whose OGM was received contains the sequence numbers bigger than in its range table, this link is said to be the new best binding to the OGM originator; otherwise, there are no changes. When an OGM is retransmitted, its TTL must be reduced (in case it becomes zero, the packet must be discarded) [25].

Each node that receives an OGM must retransmit the message, therefore flooding the network. The network is flooded until each node has received an OGM at least once, or until happens packet loss (that can happen due to interference, collision or traffic congestion), or until its TTL value expires. Using the data obtained from each OGM, it is possible to distinguish new messages from duplicates, assuring that all OGMs are counted only once. The amount of OGMs received is used to estimate the quality of a route (single-hop or multi-hop). That way, B.A.T.M.A.N. protocol allows each node to keep a table with the best neighbouring nodes in the network [25].

3. Application Context

This paper is inserted in the context of a major project called "Mobile mEsh Network to Aid in CountEring drug TRAffiCKing (M.E.N.A.C.E-TRACK)", which is intended to suggest improvements to the communication model used by the Brazilian authorities in order to improve reaction to security threats [12], [13]. The system currently in use by the authorities (based on radio transmitters), although reliable, is too limited considering complex operations, as for example, when tracking tactical teams (personnel and vehicles) in real time, with no possibility to access video feeds and GPS coordinates. The primary intention of M.E.N.A.C.E-TRACK is the creation of a dynamic mesh network, intended to interconnect field personnel to a base of operations whenever possible. This type of network accepts the dynamic disconnection and reconnection of nodes. Therefore, it is paramount to research technologies intended to improve the availability of information resources to the authorities (e.g. audio, video, GPS coordinates etc) similarly to [11].

This paper has a different objective considering the original M.E.N.A.C.E-TRACK concept: we propose the creation of a HighLy Portable Mesh nEtwork (or H.L.P-M.E. for short) using off-the-shelf cost effective equipment with minimum downtime for configuration. The idea behind this proposal is to have a number of pre-configured mesh nodes, which can be deployed in the field, in order to provide an *in promptum* mesh network to be used anywhere, anytime. With this infrastructure it would be possible to share multimedia data (e.g. video feeds, GPS coordinates, audio communication etc) in the field without any dependency on landlines or any preexistent infrastructure.

Considering the intended user is not necessarily a computer network specialist, and public safety has a decreasing budget in Brazil [17], [26], [27], the main prerequisites for the intended system are: it must be cost effective and it must be easy to use and deploy. To achieve the proposed objective, we created an experimental environment using off-the-shelf equipment from Open-Mesh, which provided a standard networked environment (i.e. not tampered with in any way) with native support to mesh networks. The steps intended to achieve the proposed objective are: 1) study the Open-Mesh infrastructure, which use B.A.T.M.A.N. routing protocol and 2) explore several mesh network configurations in order to test the flexibility of the devices in establishing meshes. Section 4 discusses the proposed testbed in detail.

4. Experimental Environment

At this time, we chose to use a manufactured B.A.T.M.A.N. access point (AP) instead of using an open source environment (i.e. proprietary hardware + open source firmware), so we can compare this setting to a previous experimental OpenWrt testbed we used with OLSR [12]. Our main objective does not concern the routing protocol used with OpenWrt *per se*, but the difficulties faced when using a completely configurable open source environment. Using OpenWrt we have complete control over the development/production environment, but it is also true that the configuration downtime and the possibilities for unforeseen situations are more prone to happen. Therefore, we chose a manufactured (proprietary hardware + proprietary software + open source firmware) AP which natively supports the B.A.T.M.A.N. protocol: the Open-Mesh OM2P access point (Fig. 1) [29].

Fig. 1: Open-Mesh AP OM2P.

4.1 AP OM2P

Each AP OM2P is enabled to form a mesh infrastructure. That way, it is possible to install units with traditional access (i.e. as Internet gateways) and add other units that can extend the network coverage. This AP has an external 2.4 GHz antenna with 23 dBm (200 mW) with a RP-SMA standard connector. Other aspect is that it can be managed using a cloud service called CloudTrax, which is provided free of charge by Open-Mesh [30]. The AP also has the ability to use passive power over Ethernet (incompatible with 802.3af). The specifications for the device are in Tab. 1 [31].

Table 1: Features of Open-Mesh AP OM2P.

Speed (max.)	150 Mbps
Radio	802.11b/g/n 2.4 GHz
Range (approx.)	75-150' indoor or 600' outdoor
Processor	400 MHz Atheros AR9331 MIPS 24k
Plug and play	yes
Memory	64 MB DRAM
Ethernet (WAN e LAN)	2 x 100 Mbps

4.1.1 CloudTrax Environment

The CloudTrax environment is a free cloud network controller that helps building, managing and monitoring wireless networks from any place in the world. This controller can manage an unlimited number of APs and networks, simply by registering the devices. Even if the devices lose connectivity with the cloud controller, the registered networks aren't affected. This happens because no network traffic passes through the cloud controller [31]. Another advantage is it provides access to network usage statistics graphics (containing number of users, amount of upload and download traffic, the relationship between each of the nodes and details of each node) [32].

To configure a network it is necessary to create a master login at CloudTrax homepage, which allows the administrator to access the configuration of several networks at one place, to create a network, to add any amount of nodes, to install them physically as gateways (connected via Ethernet) or as repeaters. Among the many configurations we can set, we can manually adjust the transmitting power of the antenna (allowing the AP to work indoors), configure cryptography via WPA/WPA2 or use vouchers to regulate user access and protect network traffic, define download and upload limits, restrict access using MAC filtering and, for a more general configuration, to determine if the network will be public or private [32].

4.2 Experimental Data

The acquired APs OM2P were configured initially in very simple scenarios. These APs use B.A.T.M.A.N. advanced (often referenced as batman-adv), which implements the B.A.T.M.A.N. routing protocol in the form of a linux kernel module operating on layer 2. Batman-adv operates entirely on ISO/OSI layer 2, meaning not only the routing information is transported using raw Ethernet frames but also the data traffic is handled by batman-adv. It encapsulates and forwards all traffic until it reaches the destination, hence emulating a virtual network switch of all participating nodes. Therefore all nodes appear to be linked locally and are unaware of the network's topology as well as unaffected by any network changes [33].

Regarding our first experiment, we configured an AP separately as a gateway and in the second one, we configured one AP as gateway and one as a repeater. As expected, there were no difficulties in this first set of experiments. Notebooks were connected to the SSID of AP N01 and the Internet was accessible. Our objective in this first set of experiments was to try the basic functions of this devices and assess the difficulties in using the CloudTrax environment. The environment is practically self explanatory simplifying the described tasks.

After this first stage, we created scenarios that emphasized the mesh topology. For the second stage, we used three nodes (N01, N02 and N03), each of which presenting specific configurations, depending on the created scenario. The first scenario consisted in the configuration of a mesh with one gateway and two repeaters (Fig. 2).

In Fig. 2, we can verify that N01 is configured as a gateway (N01(g)) and the other nodes are configured as repeaters. This configuration demonstrates a first example of increased network coverage. The CloudTrax controller offers meaningful visual data as shown in Fig. 5. We highlight the hop count each repeater AP performs to the gateway (last column). We only presented here the APs tab of the generated graphics, given the data provided by the other tabs are not useful for the mesh evaluation (except for the network diagram tab – as shown in Fig. 2). The "network map" shows the AP and its current configurations in a Google Map like environment, "all networks map" offers a Google Map like environment with all the CloudTrax managed networks, "clients" show client statistics and "site survey" shows information on neighbouring network APs (e.g. signal strength, channel, SSID, current mode – b/g/n etc).

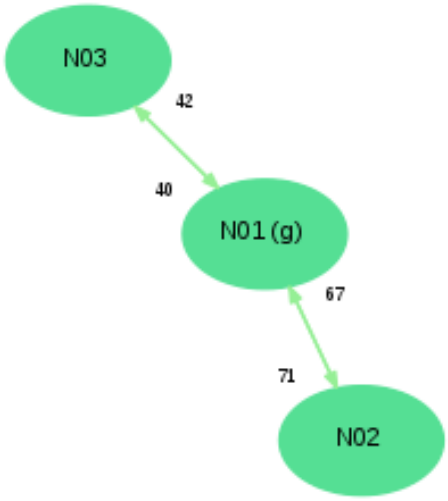

Fig. 2: Network diagram generated in the CloudTrax environment.

Given the natural mesh auto-configuration feature, it is possible to obtain different paths with the same infrastructure. Fig. 3 demonstrates a new organization of the same three nodes. Comparing Fig. 2 and Fig. 3, we can see that in this new organization, the devices connected to the node N02 can now communicate with devices connected to N03 without passing through N01, only because we added a new path between N02 and N03.

Fig. 3: Network diagram after adding a new path between N02 and N03.

In the next experiment we tinkered again with the paths of the mesh testbed and configured one gateway and two repeaters, but now, connecting the gateway to one repeater and this repeater, to another AP also configured as a repeater (Fig. 4).

The network diagram presented in Fig. 4 demonstrates that the APs have the ability to communicate through multiple

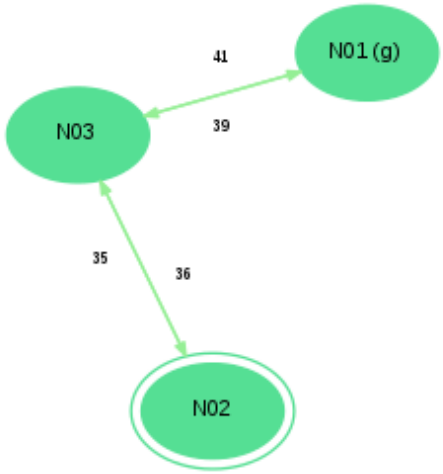

Fig. 4: Network diagram for the new topology of N01, N02 and N03.

hops. Observing the network data presented in Fig. 6, it is clear that node N02 is two hops away from the N01 gateway.

One last thought regarding the presented topologies is that all the links established are bidirectional (i.e. full duplex). All the experimental setups presented were tested connecting devices to each SSID and using the ping tool to verify their connectivity (simultaneously) and verifying mainly if the 1 hop and 2 hop distance did not interfere in the reachability of each device. Besides, we also made another simple test: we disconnected the gateway (i.e. N01) from the Ethernet network, therefore rendering it unreachable from/to the Internet (and therefore, unavailable to CloudTrax). Given we disabled the feature "access point isolation" (which prevents wireless users from accessing each other's computers) in the advanced tab, as the infrastructure was already configured in CloudTrax, it keeps its configured characteristics. Therefore, we still can access the SSID of the mesh network and we can still reach every single device that is using the network locally. Considering this APs are extremely portable, by adding a battery module (like a portable powerbank) in each node, we have an almost zero configuration mesh network environment that is ready for use in any environment (indoor or outdoor), as we intended for this paper.

5. Conclusion

The main objective of this paper was to present the basis for the creation of a HighLy Portable Mesh nEtwork (or H.L.P-M.E.) using an off-the-shelf device, which implements B.A.T.M.A.N. layer 2. Given our experience with OpenWrt, we know it is possible to achieve a similar environment using only open source software (i.e. hardware + open source firmware) but when comparing to the functionalities available in the Open-Mesh OM2P and in the CloudTrax network management tool, we raise questions

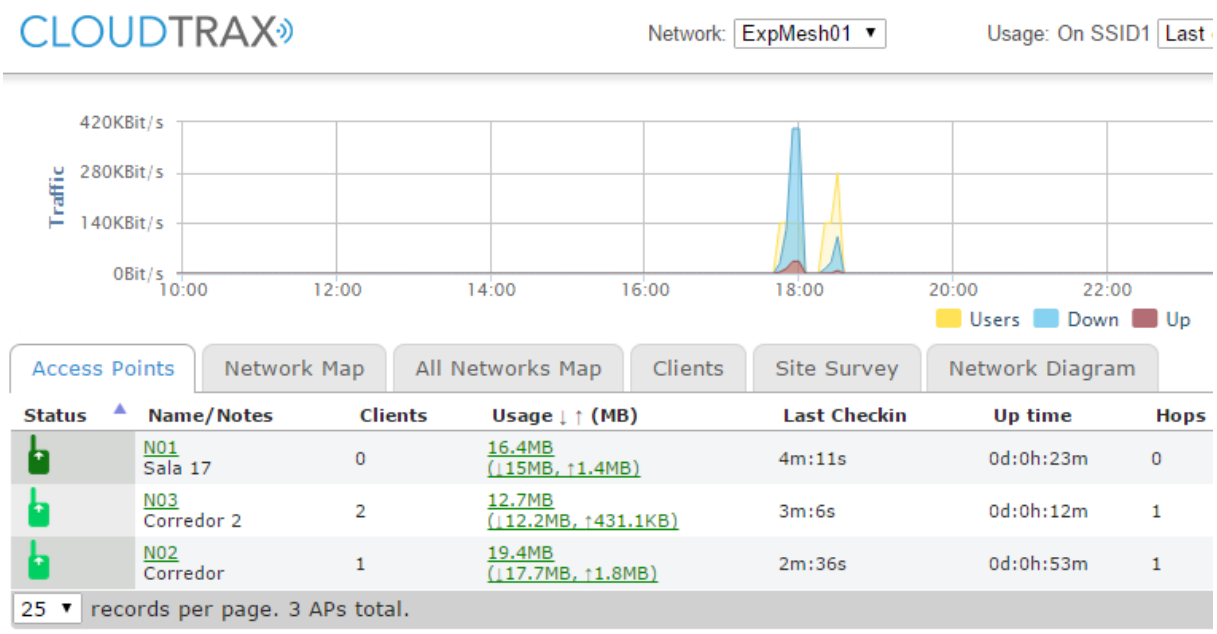

Fig. 5: Network test data CloudTrax graphic.

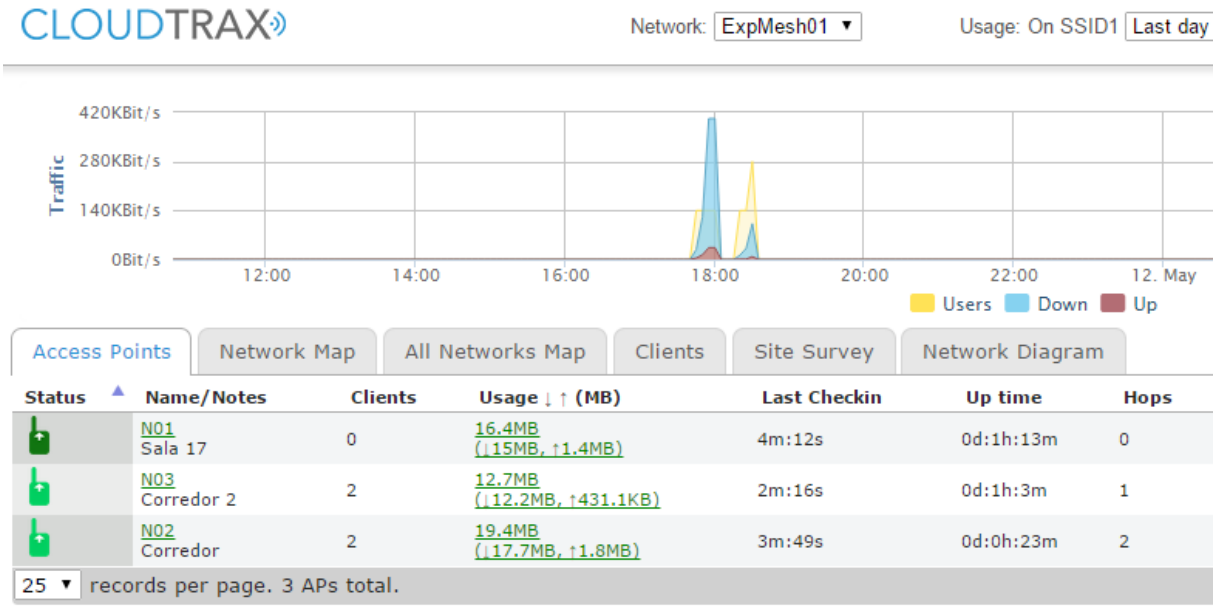

Fig. 6: Network data for the new topology of N01, N02 and N03.

regarding the development time and the amount of training we would need to put the intended audience through (i.e. law enforcement agents) to use effectively the system. Using OM2P + CloudTrax, the creation of the mesh topologies is almost effortless and we see almost now downtime considering the learning curve to use this infrastructure. Using minor adaptations (i.e. adding a portable battery module) the configured mesh topology is available on the go to enable a perimeter network anytime/anywhere as we wanted to demonstrate. Our next experiments will involve field testing with the battery modules and outdoor testing regarding the transmission of multimedia data in real life situations (e.g. as in the fast deployment of the infrastructure in a sting operation).

Acknowledgment

The authors would like to thank DECIT/SCTIE/MS/CNPq/FAPEG for the full sponsorship of this research (edict numbers 006/2012 and 12/2013).

References

[1] R. T. do Valle e D. C. Muchaluat-Saade, "MeshAdmin: An integrated platform for wireless mesh network management", in *Proc. Network Operations and Management Symposium (NOMS)*, 2012, pp. 293–301.

[2] Mi. Kim, I. Ra, J. Yoo, D. Kim, and H. Kim, "QoS Mesh Routing Protocol for IEEE 802.16 based Wireless Mesh Networks", in *Proc. 10th International Conference on Advanced Communication Technology ICACT*, 2008, pp. 812–817.

[3] G. A. Cabral, and G. R. Mateus, "Simulation-Based Optimization for Wireless Mesh Network Planning", in *Proc. 2010 Third International Conference on Advances in Mesh Networks (MESH)*, 2010, pp. 28–34.

[4] *IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Std. 802.11, 2012.

[5] M. M. Farias. "Routing protocol for wireless mesh networks [Protocolo de roteamento para redes wireless mesh]," M. Comp. Science thesis, Informatics College PUCRS [Faculdade de Informática PUCRS], Porto Alegre, Brazil, 2008.

[6] T. M. Cardoso, and P. C. F. Marques, "Mesh network: topology and application [Rede Mesh: topologia e aplicação]", *iTEC Magazine [Revista iTEC]*, vol. IV, n. 4, pp. 16–25, Jul. 2012.

[7] (2015) Microsoft Self Organizing Wireless Mesh Networks, website. [Online]. Available: http://research.microsoft.com/en-us/projects/mesh/

[8] J. Bicket, D. Aguayo, S. Biswas and R. Morris, "Architecture and Evaluation of an Unplanned 802.11b Mesh Network," in *Proc. 11th annual international conference on Mobile computing and networking (MobiCom'05)*, 2005, pp. 31–42.

[9] S. A. Mahmud, Shahbaz Khan, Shoaib Khan and H. Al-Raweshidy, "A comparison of MANETs and WMNs: commercial feasiblity of community wireless networks and MANETs", in *Proc. 1st international conference on Access networks (AcessNets'06)*, 2006, paper 18.

[10] S. Barakovi? and J. Barakovi?, "Comparative performance evaluation of Mobile Ad Hoc routing protocols," in *Proc. 33rd International Convention, MIPRO*, 2010, pp. 518–523.

[11] D. PADI, "Vehicular Information & Communications Technology (VICT) System," in *Proc. 2nd International Conference on Adaptive Science & Technology*, 2009, pp. 390–394.

[12] D. M. Tavares, M. J. Lima, R. V. Aroca, G. A. P. Caurin, A. C. De Oliveira Jr, T. A. Santos Filho, S. J. Bachega, M. A. Batista and S. F. Da Silva, "Access Point Reconfiguration Using OpenWrt," in *Proc. The 2014 International Conference on Wireless Networks (ICWN'14)*, 2014, pp. 254–260.

[13] D. M. Tavares, A. P. Da Silva, S. J. Bachega, R. V. Aroca, J. Ueyama, G. A. P. Caurin and A. C. De Oliveira Jr., "A Practical Evaluation of Smartphone Application on Mesh Networks," in *Proc. The 2014 International Conference on Wireless Networks (ICWN'14)*, 2014, pp. 247–253.

[14] S. J. Bachega and D. M. Tavares, "Simulation of Reactive Routing Protocols in Wireless Mesh Networks: a Systematic Literature Review", in *Proc. The 2014 International Conference on Wireless Networks (ICWN'14)*, 2014, pp. 235–239.

[15] C. L. Chan, S. C. Lee, K. C. Yeong and V. Jeewa, "Innovations to improve wireless mesh network performance: A survey," in *Proc. IEEE Symposium on Wireless Technology and Applications (ISWTA)*, 2013, pp. 80–84.

[16] I. F. Akyildiz and X. Wang, "Innovations to improve wireless mesh network performance: A survey," *IEEE Communications Magazine*, pp. S23–S30, 2005.

[17] (2015) Journal of Brazil [Jornal do Brasil], RJ: cuts of R$ 2,6 billion in the annual budget concerns public safety [RJ: corte de R$ 2,6 bilhões no orçamento anual preocupa segurança pública]. [Online]. Available: http://www.jb.com.br/rio/noticias/2015/01/27/rj-corte-de-r-26-bilhoes-no-orcamento-anual-preocupa-seguranca-publica/

[18] (2015) Mesh Dynamics, Mobile mesh networks for military, defense and public safety. [Online]. Available: http://www.meshdynamics.com/military-mesh-networks.html

[19] P. Garnepudi, T. Damarla, J. Gaddipati and D. Veeraiah, "Proactive, reactive and hybrid multicast routing protocols for Wireless Mesh Networks," *Proc. IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, 2013, pp. 1–7.

[20] (2015) Open-mesh, B.A.T.M.A.N. Protocol concept. [Online]. Available: http://www.open-mesh.org/projects/open-mesh/wiki/BATMANConcept

[21] F. Zeiger, N. Kraemer and K. Schilling, "Commanding mobile robots via wireless ad-hoc networks – A comparison of four ad-hoc routing protocol implementations," *Proc. IEEE International Conference on Robotics and Automation (ICRA)*, 2008, pp. 590–595.

[22] D. Johnson, N. Ntlatlapa and C. Aichele, "A Simple pragmatic approach to mesh routing using BATMAN," in *Proc. 2nd IFIP International Symposium on Wireless Communications and Information Technology in Developing Countries*, 2008.

[23] D. Murray, M. Dixon and T. Koziniec, "An experimental comparison of routing protocols in multi hop ad hoc networks," *Proc. Telecommunication Networks and Applications Conference (ATNAC)*, 2010, pp. 159–164.

[24] R. Sanchez-Iborra and Maria-Dolores Cano, "Qoe-based performance evaluation of video transmission using the BATMAN routing protocol," *Proc. 10th ACM symposium on QoS and security for wireless and mobile networks (Q2SWinet'14)*, 2014, pp. 9–16.

[25] A. Neumann, C. Aichele and S. Wunderlich. (2015) Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.) draft-wunderlich-openmesh-routing-00. [Online]. Available: http://tools.ietf.org/html/draft-wunderlich-openmesh-manet-routing-00

[26] (2015) Sul 21, Civil Police on Strike Against Budget Cuts in RS Public Safety [Polícia Civil paralisa atividades contra cortes na segurança pública do RS]. [Online]. Available: http://www.sul21.com.br/jornal/policia-civil-paralisa-atividades-contra-cortes-na-seguranca-publica-do-rs/

[27] (2015) GoiásReal, Budget cuts in public safety instills violence high tide [Com cortes na Segurança Pública, violência segue em alta]. [Online]. Available: http://www.goiasreal.com.br/noticia/15/com-cortes-na-seguranca-publica-violencia-segue-em-alta

[28] J. Xu, L. Wang, Y. Li, Z. Qin and M. Zhu, "An Experimental Study of BATMAN Performance in a Campus Deployment of Wireless Mesh Networks," *Proc. Seventh International Conference on Mobile Ad-hoc Sensor Networks (MSN)*, 2011, pp. 341–342.

[29] (2015) Open-Mesh, OM2P 150 Mbps Access Point with External Antenna. [Online]. Available: http://www.open-mesh.com/products/access-points/om2p.html

[30] (2015) CloudTrax, Part 1: CloudTrax Guide Overview. [Online]. Available: https://help.cloudtrax.com/hc/en-us/articles/202465650-Part-1-CloudTrax-Guide-Overview

[31] (2015) Open Mesh, OM2P Access Point with External Antenna. [Online]. Available: https://www.open-mesh.com/skin/frontend/default/open-mesh/images/OM-2015-04.pdf

[32] (2015) CloudTrax, Creating your first CloudTrax network. [Online]. Available: http://cloudtrax-static.s3.amazonaws.com/docs/quick_start_guide.pdf

[33] (2015) batman-adv, Doc-overview B.A.T.M.A.N. advanced. [Online]. Available: http://www.open-mesh.org/projects/batman-adv/wiki/Wiki