ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/260165109

The serval mesh: A platform for resilient communications in disaster & crisis

Conference Paper · October 2013

DOI: 10.1109/GHTC.2013.6713674

CITATIONS
2

READS
208

6 authors, including:

Romana Challans
Flinders University

9 PUBLICATIONS **11** CITATIONS

SEE PROFILE

Paul Gardner-Stephen
Flinders University

25 PUBLICATIONS **66** CITATIONS

SEE PROFILE

All in-text references underlined in blue are linked to publications on ResearchGate, letting you access and read them immediately.

Available from: Romana Challans
Retrieved on: 01 June 2016

The Serval Mesh: A Platform for Resilient Communications in Disaster & Crisis

Paul Gardner-Stephen, Romana Challans, Jeremy Lakeman, Andrew Bettison
Computer Science, Engineering & Mathematics
Flinders University
Adelaide, Australia
paul.gardner-stephen@flinders.edu.au

Dione Gardner-Stephen
Serval Project Inc.
Adelaide, Australia

Matthew Lloyd
New Zealand Red Cross
Wellington, New Zealand

Abstract— The challenges of many crisis communication needs can be summarised as: the need to allow civilians to safely communicate with one another, and with the outside world, without reliance on any domestic terrestrial infrastructure, or on the import of physical materials. Therefore, any solution should place high precedence on infrastructure-independent operation, and the re-use of existing hardware technology. Expanding on this concept, we present a prototype solution, the Serval Mesh, and briefly discuss the design decisions that were made, and summarise the trial and pilots conducted to date. Together, these show that the Serval Mesh is well placed to provide secure, resilient mobile communications services in a variety of situations, and in conjunction with the air-droppable UHF-packet-radio enabled Serval Mesh Extender concept, to provide such services over longer distances than is possible for Wi-Fi based mobile mesh networks. Thus we argue by example that it is possible to enable effective use of mobile phones during periods of infrastructure-deprivation.

Keywords—MANET; smart-phone; resilience; Serval Mesh.

I. INTRODUCTION

The challenges of many crisis communication needs can be summarised as: the need to allow civilians to safely communicate with one another, and with the outside world, without reliance on any domestic terrestrial infrastructure, or on the import of physical materials. Therefore, any solution should place high precedence on infrastructure-independent operation, and the re-use of existing hardware technology.

The advent of the smart-phone, and its combination of portability, battery-powered operation, substantial computing power, versatile user-interface and rich communications capabilities has created a compelling platform for the creation of crisis communications systems, such as Ushahidi [1]. However, the utility of smart-phones in crisis and conflict situations is hampered by their dependence on fragile cellular infrastructure and a lack of security for the end-user.

Yet, because of the smart-phone's powerful capabilities and ubiquity in high income countries, and increasing penetration into low income populations, it makes considerable sense to explore how the smart-phone can be liberated from its dependence on infrastructure and phone credits, and thus be freed to provide resilient communications capabilities that are well suited to use in crisis situations. One further compelling reason to explore this option is that most individuals are intimately familiar with their personal phone, an important factor for the successful use of any tool under situations of extreme stress and deprivation.

In this paper we explore several critical design decisions, and then describe one model for relieving smart-phones of their infrastructure dependence, and summarise the substantial progress towards and demonstrations of capabilities enabled by the described model as embodied in the Serval Mesh software and Serval Mesh Extender hardware. Detailed explanation of the internal operation of the Serval Mesh itself is beyond the scope of this paper. The interested reader is referred to the Serval Project developer Wiki [2].

II. CRITICAL DESIGN DECISIONS

A. Identification of a suitable communications layer

Smart-phones typically offer three types of radio that can potentially communicate with one another directly, without mediation by cellular infrastructure. These are the multi-band cellular, Bluetooth and Wi-Fi radios. However, at this point in time, it is unfeasible to use either the cellular or Bluetooth radios for widespread phone-to-phone communication.

Reprogramming the cellular radio is problematic, as the handset and chipset vendors consider the necessary information to be proprietary. Furthermore, the sheer number of unique handset types renders this solution essentially intractable if wide support of smart-phones is desired. Transmitting in the cellular bands also presents regulatory problems in contexts where there are functioning carriers and/or regulators. Poor interoperability among devices is an major impediment for using Bluetooth.

Therefore, we have concluded that the Wi-Fi radio is currently the most suitable option for a smart- phone-based solution to the Challenge. Wi-Fi offers comparable or superior range to Bluetooth, as well as much higher data rates. Also,

The authors wish to acknowledge the support of the Awesome Foundation for the Arts & Sciences (Boston Chapter), the NLnet Foundation, the Shuttleworth Foundation, Flinders University, the New America Foundation, the New Eurasia Foundation, Australian National Science Week and other individual and institutional supporters of their work.

most smart-phones allow the Wi-Fi radio to be operated as a Wi-Fi Access Point (AP). This provides the means for groups of smart-phones to communicate directly with one another, without reliance on any infrastructure.

By cycling the Wi-Fi between the AP and client modes, combined with appropriate store-and-forward protocols, it is possible to allow smart-phones to share data with one another [3], even if not directly connected, and even if only occasionally in contact with other smart-phones. Therefore software focuses on forming mesh networks using Wi-Fi in AP and client modes if no better alternative is available.

Wi-Fi also offers a third mode, ad-hoc mode, that allows direct communications among smart-phones that support it. However, only Nokia's Symbian operating system includes full native support for ad-hoc mode, while other platforms require "rooting", "jailbreaking" or the installation of custom firmware. Therefore, despite the excellent suitability of ad-hoc Wi-Fi to crisis communications because of the device mobility and multi-hop mesh networks that it affords, it is not currently available for widespread use. There would be considerable value in enabling ad-hoc Wi-Fi on all mobile operating systems, and it would be of considerable value to the humanitarian community for some party to liaise with Apple, Microsoft, Google and Blackberry and strongly encourage them to enable ad-hoc Wi-Fi on their respective mobile platforms, and to commit to a robust interoperability program. We assume that ad-hoc Wi-Fi will remain unavailable, at least in the short term.

B. *Identification of a suitable protocol and software layer*

The defining characteristics of a suitable protocol and software layer are that they must be able to operate on AP/client Wi-Fi, be highly tolerant to the network partitioning into many isolated segments, and able to form useful mesh networks in such circumstances. IP-based protocols are not well suited to this task, as UDP and TCP both assume end-to-end connections.

Also, end-to-end connections on mesh networks are problematic, because the probability of a packet arriving decreases exponentially with the number of hops, and the useable bandwidth typically worsens by at least 50% for each hop that traffic must traverse after the first. In contrast, single-hop communications among neighbouring nodes on a mesh network can deliver the full bandwidth of the underlying communications medium.

Therefore communications protocols should take advantage of this characteristic. Store-and-forward or bundle-based protocols are the logical choice in this context. Store-and-forward bundle protocols have a further advantage for isolated crisis communications networks in that they can replicate data onto many nodes, where it can be consumed locally.

C. *Software features and applications required for a useful Solution*

Our work has been movitated by a list of the key features that a smart-phone-based software solution should include for maximum usefulness, resilience and flexibility in humanitarian operations, as gleaned in discussions with potential users. These are:

- a store-and-forward bundle distribution protocol as discussed above;
- a maps application that allows individuals to add points of interest that are shared and viewing the geographic position of their colleagues in near-real-time via the mesh;
- a crisis-mapping application that provides similar functionality to, or ideally can interface with Ushahidi;
- secure text and voice messaging applications;
- a mechanism for distributing and updating the above software components in the field; and
- a distributed social networking platform.

Live voice calls are desirable and valuable, but not vital, as they can be substituted by the features listed above. By not including this functionality at this stage, the solution is simplified, as it does not need to be able to stream live data over a mesh network. Live streaming requires a functional end-to-end network, which cannot be guaranteed in a crisis situation.

The key capabilities listed above differ from the existing art in that they are required to be fully distributed, and able to operate independently of any coordinating authority, internet access or any other communications infrastructure. However, infrastructure-independence should not mean infrastructure-ignorance. That is, each of these capabilities should be able to automatically make use of internet connectivity, when and wherever it becomes available if the user desires. It is reasonable to assume that both victims and aid workers in a crisis zone will have a strong incentive to facilitate such connections with the outside world, and will do so by whatever means are at their disposal. But to be clear, such connections are not necessary for our solution to facilitate communications and information sharing among persons within a crisis zone.

D. *Identification of existing partial solutions*

There are several projects that offer some of the features and applications described above. For example FreedomBox [4] and OTI/Commotion [5] offer peer-to-peer communications systems that can operate independently of infrastructure to some extent. Yet these projects do not offer the complete set of functionality and characteristics outlined above. On the other hand, the OTI/Commotion project does offer secure infrastructure-independent voice services in certain situations. On examination, those capabilities are the result of its inclusion of a component sourced from the Serval Project [6-8], which is part of the solution we describe in this paper. Another project, the Village Telco Project explores only fixed-line mesh telephony [8].

The Serval Project is an open-source mesh communications platform that arose in response to the Haiti Earthquake of 2010. The Serval Project's mission is "communications anywhere, anytime", and is based on the methodology described above, resulting in the core assumption being the unavailability of any supporting infrastructure. Having made that assumption of infrastructure-deprivation, the design seeks to recreate many of the functionalities expected of modern smart-phones, as listed in the previous section. The resulting Serval Mesh software and related protocols and software, although in need of refinement, demonstrate the feasibility of this approach and represents in our view the forefront of this field of research. The remainder of this paper describes the Serval Mesh software design, capabilities and testing performed to date.

III. OVERVIEW OF THE SERVAL MESH SOFTWARE

The Serval Mesh software allows off-the-shelf smart-phones to build self-organised mesh networks using Wi- Fi in AP and client modes and a store-and-forward protocol (Serval Rhizome). The Serval Mesh software has a pictorial user-interface, and an already relatively simple installation process. Normally complex processes, such as network address allocation, have been solved in a completely transparent manner, relieving end users from such matters. This is important for increasing the solution's utility among people with low technological literacy. In addition, when the Serval Mesh software installs on a handset, it offers itself for installation onto other phones. In this way, the mesh itself can be deployed in a crisis situation, instead of having to be deployed beforehand. This represents a compelling solution to a common logistical problem in provision of services in crisis situations.

A. Text Messaging & File Distribution

The Serval Project software suite currently includes the ability to make mesh-based telephone calls, send SMS-like short messages (MeshMS), and distribute, share and exchange files, including Serval Mesh software updates. It also comprises a maps application that shares map tiles and points of interest (Serval Maps). There is also already integration with Open Data Kit [9] tools for the collection of forms and other structured data from the field (Serval SAM). Each of these components are complemented by a robust security framework that offers strong protection of private communications.

B. Field Data Collection & Visualisation

Serval Maps and Serval SAM can source map tiles, surveys and other data collection and visualisation elements available on an isolated mesh network and perform rudimentary visualisation of that data, demonstrating the feasibility of infrastructure-free operation. The local-first dissemination behaviour of single- hop bundle-based store-and-forward protocols is well suited this environment, because local information will tend to be available where it is required. We foresee that these tools could be readily refined to provide similar functionality to Ushahidi, but without the requirement to fetch any data over the network at the time of visualisation. Combining the Serval Project's Maps application with the OpenDataKit integration offers the potential to create an integrated, distributed and infrastructure-independent, but not infrastructure-ignorant, crisis mapping platform that directly answers various humanitarian operational needs.

C. Security Framework

Underlying these functions is strong cryptographic protection of communications through the Serval Project's security framework. The Serval Project uses a Diffie-Hellman shared-key agreement to encipher communications between pairs of parties, and to protect data through digital signatures for publicly distributed information. This provides considerably better security than standard cellular communications.

Specifically, network addresses on the Serval Mesh are public keys in the 256-bit Elliptic Curve Cryptography (ECC) Curve25519 cryptographic system [10], which allows all communications between nodes on a Serval Mesh to be encrypted, authenticated or signed as appropriate. Indeed, the default mode of communications at the protocol level is encrypted and authenticed, and sending unencrypted communications requires purposeful action on the part of the programmer.

D. Planned Capabilities

In addition to Ushahidi-like crowd-sourced information systems, there is also great utility in text-messaging systems, such as SMS and TwitterTM. The Serval Mesh software offers prototype of mesh-based equivalents to these services. Serval MeshMS allows the sending of encrypted text messages on the mesh. MeshMS also offers a primitive Twitter-like service in the form of broadcast unencrypted MeshMS messages. By supplementing that feature with hash-tag and sender filtering tools, it would be possible to create a distributed social networking platform that allows for local informal information sharing without dependence on any infrastructure. It would also be very simple to add a secure voice mail application. While this would be useful in and of itself, when considered in the context of the already pictorial user interface, it would be especially valuable for providing accessibility to people with poor literacy skills.

IV. AVAILABILITY & TESTING OF THE SERVAL MESH SOFTWARE

The current experimental version of the Serval Mesh software is available for free download from the Google Play store, and the source code is also available [11]. It implements the file distribution and secure text messaging functions, as well as the ability to share itself to other phones, and receive cryptographically signed software updates over the mesh network itself. We consider the software to be demonstration quality, and following a few minutes instruction, can be used relatively easily used even by school children. Several tests and trials of the software are summarised below.

A. Demonstration in the Australian Outback 2010

The initial version of the Serval Mesh software was demonstrated to the media in July 2010 in the Arkaroola Wilderness Sanctuary in the Australian Outback. Multi-hop unencrypted voice calls was the sole feature complete at that time. Phone calls were conducted in a remote village, in valleys and on hilltops as part of the media-oriented demonstration of the potential of mesh telephony. The most significant feature demonstrated was the ability to place mesh telephone calls using ordinary telephone numbers on a completely distributed network lacking a central number database.

B. Pilot in Nigeria 2010-2011

The Rhizome store-and-forward file distribution capability was added late 2010, including the ability to send delay-tolerant text messages. All communications in that version of the software were unencrypted. This software was then deployed to a number of residents in a Nigerian water-front community who were being threatened with eviction by their government, in order to assist them in organizing the defense of their right to retain their homes [12].

The independent report that was written following the trial that indicated that participants using the Serval Mesh software communicated more often, and spent less in the process. Two videos in support of their cause were also produced and uploaded to the Internet using video collected using the mesh software. The participants identified the limited range of Wi-Fi communications between the phones (which they found to be limited to around 60m in their urban environment) and the need for private communications as the aspects most needing attention. This trial proved that the technology was not merely academically interesting, but is also practically useful.

C. *Trials with New Zealand Red Cross 2012 & 2013*

Through 2011 and 2012 a comprehensive security framework was devised and implemented in the Serval Mesh that ensured that all communications would be end-to-end encrypted and authenticated by default, addressing one of the two outstanding issues raised by the Nigeria trial.

In addition the Rhizome store-and-forward functionality was thoroughly re-implemented, and the user interface overhauled to make it easy to install and use. These updates also included the ability to deliver updates to the Serval Mesh software via the Rhizome store-and-forward protocol. These improvements were tested with the New Zealand Red Cross IT and Telecommunications Emergency Response Unit on training exercises in 2012 [13] and 2013.

A number of such updates were delivered during the 2011 trial, as well as the sharing of maps, the collective generation and visualization of points-of-interest in the field using a prototype of the Serval Maps application.

The Serval SAM application was also used to facilitate field data collection using modified versions of New Zealand Red Cross field assessment forms demonstrating that capability.

Initial testing of Serval Mesh Extender prototypes was undertaken in the 2013 exercise, establishing that longer range communications was possible in open-country by using a UHF packet radio [14-16].

D. *Tests in Boston, USA and on the National Mall, Washington D.C. 2013*

The previous demonstrations left the limited range of Wi-Fi communications as the major identified limitation of the Serval Mesh technology, although some explorations had begin. Work in early 2013 began to address this by refining the Serval Mesh Extender concept into a hand-held and battery powered Serval Mesh router featuring both Wi-Fi and UHF packet radio (the RFD900 by RFDesign). The RFD900 radio operates in the ISM band adjacent to 915MHz, which is available for license-free operation in some form in Australia, New Zealand, the USA, Canada and several other countries.

The preliminary testing in New Zealand with New Zealand Red Cross had established that rural line-of-sight range of greater than 3km was easily achievable using Serval Mesh Extenders. Later tests proved communications proved possible over distances of greater than 1,300m on the National Mall [17] and across the Charles River in Boston [18], both open areas in urban centers. A Mesh Extender placed indoors in a hotel room in the challenging radio environment of urban Cambridge, MA, yet communications through multi-story buildings was possible to a distance of 200m – 300m [19]. Communications were also sustained in Washington D.C. subway trains, allowing text messaging from opposite ends of an approximately 200m long six railcar set [17].

Significantly, all these tests used un-aimed omnidirectional antennae and the Mesh Extender units were carried or placed in a realistic manner, such as on a cupboard in a hotel room, or carried in a backpack, supporting the notion that the distances reported here are likely to be representative of actual performance. We estimate that these range improvements allow a Mesh Extender to cover potentially hundreds of people in typical urban settings [20-21], compared with Wi-Fi mesh devices that typically cover fewer than ten people due to the short range of communications.

E. *Use by School Children during Australian National Science Week 2013*

Most recently as part of Australian National Science Week students from several regional and remote schools in the northern pastoral districts of South Australia were given the opportunity to use the Serval Mesh software. They were supplied with low-cost smart-phones preinstalled with the Serval Mesh software. Students ranged in age from approximately five to seventeen years of age. Students were able to make effective use of the technology almost immediately, and succeeded in sending encrypted text messages and making encrypted voice calls [22]. In this way the ease of use of the Serval Mesh software was demonstrated.

V. SUMMARY AND FUTURE DIRECTIONS

Overall, the Serval Project has demonstrated the technical feasibility of the Serval Mesh technology through various tests and demonstrations of functional prototypes of many required features of a useful crisis communications platform, addressing the major issues identified in the pilot undertaken in Nigeria in 2011.

While quite some refinement and extension work is still required, the technical risk for the remaining software development is low. We anticipate the focus over the next twelve months on consolidating the capabilities demonstrated to date ready for release as easy to use free and open-source software and low-cost hardware products for use by humanitarian organisations and the general public alike.

In the longer term we intend to focus on improving the scalability of the system, and improve the operation of the UHF radio in the Mesh Extenders to support multi-hop and point-to-multi-point operation to extend the effective range of the network to many times the native range of the UHF radio itself, just as is already possible with ad-hoc Wi-Fi.

REFERENCES

[1] Ushahidi. (2013 Aug 23) *Ushahidi* [Online]. Available: http://www.ushahidi.com

[2] P. Gardner-Stephen et al. (2013 Aug 23) *Serval Project Developer Wiki* [Online]. Available: http://developer.servalproject.org/wiki

[3] P. Gardner-Stephen and S. Palaniswamy, "Serval mesh software – WiFi multi model management", in *Proc. of the 1st International Conference on Wireless Technologies for Humanitarian Relief*, India, 2011, pp. 71-77.

[4] The Freedombox Foundation. (2013 Aug 23) *Freedombox* [Online]. Available: http://freedomboxfoundation.org

[5] The Open Technology Initiative. (2013 Aug 23) *Commotion Wireless* [Online]. Available: http://commotionwireless.net

[6] P. Gardner-Stephen and R. Challans et al. (2013 Aug 23) *The Serval Project* [Online]. Available: http://servalproject.org

[7] P. Gardner-Stephen, J. Lakeman, R. Challans, C. Wallis, A. Stulman, Y. Haddad. "MeshMS: Ad Hoc Data Transfer within Mesh Network". International J. of Communications, Network and System Sciences vol. 5, no. 8, pp. 496-504 Aug. 2012.

[8] M. Adeyeye and P. Gardner-Stephen. "The Village Telco Project: a reliable and practical wireless mesh telephony infrastructure". EURASIP J. on Wireless Communications and Networking, vol. 2011, no. 1, pp. 1-11, Aug. 2011.

[9] G. Borriello et al (2013 Aug 23) *Open Data Kit* [Online]. Available: http://OpenDataKit.org

[10] D. J. Bernstein, T. Lange, P. Schwabe, "The security impact of a new cryptographic library". in *Proc. of LatinCrypt 2012*, 2012, pp. 159–176

[11] P. Gardner-Stephen et al. (2013 Aug 23) *Serval Project Source Code Repository* [Online]. Available: http://github.com/servalproject

[12] A. Crandall and L. Mutuku. (2012 May) "Mesh-Casting News in the Port Harcourt Waterfronts", Internews Center for Innovation and Learning, [Online]. Available: http://developer.servalproject.org/dokuwiki/doku.php?id=content:publications:internews2010

[13] P. Gardner-Stephen. (2012 Mar 3) *KiwiEx 2012: Installing and Updating Software in a Simulated Disaster* [Online]. Available: http://servalpaul.blogspot.com.au/2012/03/kiwiex-2012-installing-and-updating.html

[14] P. Gardner-Stephen (2013 Feb 26) *Mesh link using our prototype Mesh Helper through ~200m of forest* [Online]. Available: http://servalpaul.blogspot.com.au/2013/02/mesh-link-using-our-prototype-mesh.html

[15] P. Gardner-Stephen (2013 Feb 26) *3KM Mesh link using Mesh Helper Prototypes* [Online]. Available: http://servalpaul.blogspot.com.au/2013_02_01_archive.html

[16] P. Gardner-Stephen (2013 Mar 6) *Testing Mesh Helper Prototypes in Moores Valley* [Online]. Available: http://servalpaul.blogspot.com.au/2013/03/testing-serval-mesh-helper-prototypes.html

[17] P. Gardner-Stephen et al (2013 May 30) *Range Testing Serval Mesh Extender on the National Mall in Washington with the New America Foundation* [Online]. Available: http://servalpaul.blogspot.com.au/2013/05/range-testing-serval-mesh-extender-on.html

[18] P. Gardner-Stephen (2013 May 31) *Crossing the Charles River by Mesh Extender* [Online]. Available: http://servalpaul.blogspot.com.au/2013/05/crossing-charles-river-by-mesh-extender.html

[19] P. Gardner-Stephen (2013 May 30) *Range Testing Mesh Extenders in Boston & at the MIT Media Lab* [Online]. Available: http://servalpaul.blogspot.com.au/2013/05/range-testing-mesh-extenders-in-boston.html

[20] P. Gardner-Stephen (2013 May 1) *Urban Testing of Mesh Extender (Part 1)* [Online]. Available: http://servalpaul.blogspot.com.au/2013/05/urban-testing-of-mesh-extender-part-1.html

[21] P. Gardner-Stephen (2013 May 4) *Urban Testing of Mesh Extender (Part 2)* [Online]. Available: http://servalpaul.blogspot.com.au/2013/05/urban-testing-of-mesh-extender-part-2.html

[22] P. Gardner-Stephen (2013 Aug 23) *Demoing the Serval Mesh and Mesh Extenders to School Children as part of Australian National Science Week 2013* [Online]. Available: http://servalpaul.blogspot.com.au/2013/08/demoing-serval-mesh-and-mesh-extenders.html