Spontaneous Wireless Networking to Counter Pervasive Monitoring

Emmanuel Baccelli, Oliver Hahm, Matthias Wählisch

Spontaneous Wireless Networking to Counter Pervasive Monitoring

E. Baccelli, O. Hahm, M. Wählisch *

February 11, 2014

1 Pervasive Monitoring is a Myth

Pervasive monitoring does not exist for one good reason: if monitoring does happen, as revealed by recent whistleblowing that highlighted the scale of NSA surveillance activities [1], it happens in very few key central locations in the network. Monitoring, as we know it so far, is thus by no means pervasive in the geographical or topological sense. One might further speculate that such monitoring will probably never become pervasive because it would simply be too expensive to put in place.

This observation leads to a fundamental question: how could NSA surveillance reach such an incredibly large scope, to the point where it *seems* pervasive, while in fact, they only monitor the network from a few select locations? The answer to this question is simple: the NSA's monitoring could scale because *we* are addicted to centralization.

From the physical point of view, we made ourselves absolutely dependent on the deployed, fixed infrastructure. Whenever we communicate, the quasi totality of the traffic relies upon going through a central access point of some sort. This approach to networking certainly offers substantial advantages (a good performance/cost compromise for starters), but on the other hand it offers cheap and efficient vantage points for whoever seeks large scale monitoring opportunities. It does not have to be so.

Similarly, from the logical point of view, we make ourselves more and more dependent on cloud services. Whenever we store, or access our data, we rely on a centralized architecture that concentrates everything in data centers. Again, this approach offers great advantages (e.g. easier access from anywhere, lower

*Emmanuel Baccelli is affiliated with INRIA and Freie Universität Berlin. Oliver Hahm is affiliated with INRIA. Matthias Wählisch is affiliated with Freie Universität Berlin.

cost reliability and efficiency), but on the other hand it offers more cheap and efficient vantage points for would-be spies. It does not have to be so either.

2 Making Massive Surveillance Harder

At this point, it becomes apparent that there are essentially three ways to make large scale systematic surveillance a much harder task.

The first type of solution is to significantly increase the physical security of potential vantage points. While this type of solution is obviously necessary, history shows that there are always cracks to infiltrate if the will to break in is there. And it will be there. So this type of solution is by no means sufficient.

The second type of solution is to significantly increase the default levels of encryption used over the network. For starters, the default behavior should be to encrypt "door-to-door" and don't let communication be decrypted by intermediate devices. Furthermore the default cryptographic mechanisms should be significantly harder to decipher. Note that to ensure this actually happens consistently, the use of open source software should be mandatory concerning such cryptographic mechanisms. On one hand, as highlighted in [21], open-source bundled with automatic updates can slow down or stop obsolescence altogether, and on the other hand, open source is best known guarantee against malware and potential backdoors. However, if one of the physical end points of the communication is a vantage point of potentially high interest (say a data center), we quickly come back to the problems of the first type of solution, i.e. there are always cracks to infiltrate if the will to break in is there. And it will be there, with an extremely intense focus, because this is a potential vantage point – and with an intense focus one can do wonders.

The third type of solution is of an entirely different nature, which is the main purpose of this document. Instead of hardening the current architecture and increasing the security of high profile targets, another category of approach could be to aim for *target dispersal*, as suggested recently by B. Schneier in [2]. Target dispersal would eliminate "default" vantage points and thus naturally disable systematic mass surveillance. De facto, surveillance efforts would be forced to be more specific and personalized, and thus more directly accountable for.

To that end, *stateless* networking approaches should be developed and employed, i.e. approaches that do not rely on central entities (infrastructure-based), but rather on spontaneous interaction between autonomous peer entities, as locally as possible (topologically and/or geographically). The network architecture should evolve towards a mode of operation where all possible stateless solutions are tried first, before considering any infrastructure-based approach – again, the goal being to increase target dispersal. In fact, several examples of stateless approaches have appeared over the last decade, at different layers. These include

for instance peer-to-peer (P2P) networks or WebRTC [22] at the application layer, and multi-hop spontaneous wireless networks at the network layer [4], such as mobile ad hoc networks [3], wireless sensor networks, vehicular networks, or wireless mesh networks.

While P2P networks have been massively deployed and adopted (WebRTC will likely enjoy the same fate) spontaneous wireless networks have not yet been widely adopted. There has however been quite some work in the research community over the past decade on this topic, which has identified issues that must (still) be tackled in order to efficiently adapt IP protocols for these new networks. Actually, the community has already produced a number of new protocol specifications dedicated to spontaneous wireless networking operation, such as [5] [6] [9], [13] among others. Some of these protocols have even been deployed in specific contexts. Several european and american military applications have deployed using mobile ad hoc routing to power spontaneous, on-the-move local communications between elements on-site. In another context, several cities in Europe and in the USA have deployed wireless community mesh networks (e.g. [18] [19]), which use these protocols. Last, but not least, the highly anticipated Internet of Things (IoT) is heavily based on spontaneous wireless networking and the outcome of efforts such as 6LoWPAN [14] or ROLL [15].

Indeed, merging spontaneous wireless networks with traditional, operated networks presents a number of advantages, aside of target dispersal to counter massive surveillance. First, it could offer operator infrastructure offloading [20]. Second, the resulting network would systematically maximize connectivity at marginal cost. Third, it offers natural coverage extension for the network access infrastructure already deployed. And last, it offers increased resilience of the network in face of infrastructure outage.

There are of course lingering issues that do not allow off-the-shelf, spontaneous wireless networking at large scale. Among others, such issues include (i) the absence of efficient standard router auto-configuration schemes in this context [12], which has profound implications, (ii) the lack of dedicated, optimized link layer technology (which has focused on infrastructure based networking for decades), (iii) no standard key exchange protocol or alternatives for efficient authentication method to date, and (iv) some fundamental differences in terms of characteristics compared to traditional networks, such as throughput capacity *vs* number of nodes in the network.

However, in light of the recent events revealing massive and systematic surveillance [1], there is a strong argument to decentralize our networking paradigms, and in this realm, spontaneous wireless networking at the networks layer is an asset that should not be overlooked. Contrary to infrastructure-based approaches, which are prone to monitoring, spontaneous wireless networking uses communication links that are local and volatile, i.e. unless one is physically present at the time and location of the communication, one must abandon all hope of

monitoring anything. While the wireless nature of the communication may on the other hand facilitate eavesdropping, the fact that one has to be there at the time/place of the communication significantly hampers mass surveillance, and cryptographic techniques can provide a privacy equivalent to what is achieved on wire. The honest, technical question that we should ask ourselves at this point is: are the lingering issues of spontaneous wireless networking integration in the IP stack worth solving/improving or not, taking into account our goal to maximize surveillance target dispersal?

3 Position: More Spontaneity Please

The position highlighted in this paper is that in order to maximize target dispersal to counter systematic massive surveillance, we should not overlook the full potential of decentralized network paradigms. This full potential includes not only mantras such as "*think hard before you use the cloud*", or "*let's bypass the service provider*" but also alternative techniques at the network layer, such as multi-hop spontaneous wireless networking, which could significantly reduce our dependence on the infrastructure – which will remain, whether we want it or not, a desirable vantage point for mass monitoring. There are a number of issues that need to be resolved or alleviated towards native and massive integration of spontaneous wireless networks in the currently deployed IP architecture and infrastructure-based networks (massive IPv6 adoption could already help somewhat). However, the gains obtained in terms of target dispersal alone could be worth this cost – and there are other gains too.

References

[1] G. Greenwald, E. MacAskill, L. Poitras, "Edward Snowden: the whistleblower behind the NSA surveillance revelations", The Guardian, June 2013.

[2] B. Schneier, "What we know and what we do not know", IETF88 Technical Plenary on Internet Hardening, Vancouver, November 2013.

[3] M. Corson, J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, January 1999.

[4] J.A. Cordero, J. Yi, T. Clausen, E. Baccelli, "Enabling Multihop Communication in Spontaneous Wireless Networks", in ACM SIGCOMM eBook on "Recent Advances in Networking", Hamed Haddadi and Olivier Bonaventure (Ed.), Volume 1, Chapter 9, pp. 413-457, August 2013.

[5] T. Clausen, P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[6] C. Perkins, E. Belding-Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[7] R. Ogier, F. Templin, M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", RFC 3684, February 2004.

[8] D. Thaler, "Multi-Link Subnet Issues", RFC 4903, June 2007.

[9] E. Baccelli, P. Jacquet, D. Nguyen, T. Clausen, "OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks", RFC 5449, February 2009.

[10] D. Johnson, Y. Hu, D. Maltz, "The Dynamic SourceRouting Protocol (DSR) for Mobile Ad Hoc Networks forIPv4", RFC 4728, February 2007.

[11] D. Thaler, "Evolution of the IP Model", RFC 6250, May 2011.

[12] E. Baccelli, M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

[13] T. Winter, P. Thubert, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," IETF Request For Comments, RFC 6550, March 2012.

[14] IPv6 over Low power WPAN (6lowpan) IETF Working Group, https://datatracker.ietf.org/wg/6lowpan/

[15] Routing Over Low power and Lossy networks (roll) IETF Working Group, https://datatracker.ietf.org/wg/roll/

[16] Kotz, D., Newport, C., and C. Elliott, "The Mistaken Axioms of Wireless-Network Research", Dartmouth College Computer Science Technical Report TR2003-467, 2003.

[17] E. Baccelli, C. Perkins, "Multi-hop Ad Hoc Wireless Communication", IETF Internet Draft draft-baccelli-manet-multihop-communication, 2013.

[18] Freifunk Wireless Community Networks, online at http://www.freifunk.net, 2014.

[19] Austria Wireless Community Network, online at http://www.funkfeuer.at, 2014.

[20] E.Baccelli, F. Juraschek, O. Hahm, T. C. Schmidt, H. Will, M. Wählisch, Proceedings of the 3rd MANIAC Challenge, published on ARXIV, http://arxiv.org/abs/1401.1163v2, January 2014.

[21] B. Schneier, "Security Risks of Embedded Systems", published online (Blog) http://www.schneier.com/blog/archives/2014/01/security_risks_9.html, 2014.

[22] Real-Time Communication in WEB-browsers IETF Working Group, http://tools.ietf.org/wg/rtcweb/