A Ubiquitous, Infrastructure-Free Network for Interpersonal Communication

Edoardo Biagioni
Department of Information and Computer Sciences, University of Hawaii at Mānoa
Email: esb@hawaii.edu

Abstract

Although cellphones are generally capable of communicating directly with each other, they are rarely used to do so. We describe a a low-bandwidth peer-to-peer ad-hoc network, AllNet, designed to provide direct connectivity among smart mobile devices. AllNet can be used for interpersonal communication in a number of situations: most notably in emergencies, but also for social networking, chatting, and other forms of interpersonal communication.

AllNet is based on established principles of wireless ad-hoc networking, and provides different forms of unicast and limited broadcast communication, secure communications, and a flexible priority scheme. The low resource requirement of AllNet encourages individuals to devote a small fraction of their devices' resources to supporting others' communication.

I. Ubiquitous Infrastructureless Network

Many people throughout the world carry cellphones, many of which not only provide multiple modes of communication, but also have substantial storage and computing power. Such devices range from laptops and tablets to smartphones and potentially even lower-powered devices.

The hardware of these units could be used to build an ad-hoc wireless network, where each device communicates directly with another device, where necessary forwarding data from other devices. In particular, in addition to the cellular radio, which could be used for ad-hoc communications should licensing and the manufacturer allow, most smartphones and tablets these days also have an 802.11 interface that is capable ad-hoc communication.

The benefits of such a network are obvious whenever the infrastructure fails to deliver communication to a mobile device. This may be due to absence of coverage in the area, or because the available coverage is too expensive for the user, as is often the case in airports. Within range of any given unconnected mobile device may be other devices able and willing forward data for this device, whether further within the ad-hoc network, or on to the wider Internet. Such a network, **Allnet**, can be particularly useful in cases of emergency. If users find AllNet useful on a daily basis, they will learn to use it and be able to employ the network when it is really needed, as in cases of emergency.

A companion paper [1] explores the many different motivations (summarized in Section VI), from selfish to altruistic, that may move people, perhaps strangers, to cooperate in forwarding each others' messages.

This paper describes the technical background of the design of AllNet.

Ubiquitous peer-to-peer networks have been proposed before, but generally not adopted widely enough to be considered a success. Some of the characteristics of AllNet that distinguish it from related proposals include:

- AllNet is designed primarily for local communication, avoiding the problems of scalability that impact larger P2P ad-hoc wireless networks.
- AllNet is designed for low-bandwidth communication, and does not substantially compete with regular Internet access providers. AllNet is specifically designed as a backup to infrastructure-based communications, and is mostly designed to support text-oriented communication among individuals and in small groups.
- AllNet can leverage other connections to the Internet where available for low-bandwidth activities such as checking email and reading the text of web pages.
- Allnet encrypts interpersonal communications by default, so devices forwarding messages do not have access to the contents of the message.

While technically these characteristics are independent, together they give a coherent network design that could feasibly see wide adoption. For example, the low-bandwidth nature of most AllNet communications is well-suited to encryption on energy-limited mobile devices because the computing demands to encrypt small amounts of data are less than what would be needed for larger amounts of data. The non-economic nature of AllNet and its potential use in emergencies make it easier for individuals and companies to choose to support it and build a community around it.

Ultimately, we envision AllNet supporting at least some sort of chat system and social network, but being flexible enough that, when the device's owner so chooses, it may be used for arbitrary communications among devices in range of each other, and for low-bandwidth exchanges in a range of situations and with a variety of applications.

II. Related Work: Secure Ad-Hoc Wireless Networks

AllNet brings together several related technologies, from ad-hoc networking to public-key encryption.

Building and designing ad-hoc multihop networks using 802.11 and Bluetooth has been explored quite thoroughly. For example, the goals of the AllNet project match the goals of the Networking for Communications Challenged Communities project [2], though AllNet is designed to work using existing rather than specialized equipment. Because of its greater communication range, we are focusing on 802.11 communications rather than Bluetooth for AllNet, but Bluetooth could be used as well.

Making practical use of existing research on wireless ad-hoc networks requires the selection of a routing algorithm or routing protocol, of which there is an amazing abundance. AllNet can be most useful if it supports different ways of routing. Among the most interesting for AllNet are limited broadcasts [3], which broadcast to an area limited by hop count or geographic coordinates, and delay tolerant networking (DTN or data mules) [2], where a device stores messages for delivery at a later time, when the destination is in range of that device. Also, replies may be forwarded along the reverse path of the original message, so a conversation may be unicast rather than broadcast.

While other algorithms have better performance in particular situations, both limited broadcast and DTN allow each device to apply its own priorities in forwarding traffic without necessarily disrupting the overall flow of information.

For security, AllNet can use standard algorithms such as RSA [4], [5], or the more elaborate and overall quicker mechanisms of SSL/TLS [6] and PGP/GPG. However, the more elaborate algorithms are only quicker if large amounts of data are exchanged. For small amounts of data, RSA is sufficient. For example, in 2009 on an Intel Core 2 1.83 GHz processor the time to perform RSA 2048-bit encryption, decryption, signing, and verification, which operate on 256 byte plaintexts, was about 12.5ms [7]. Even if mobile hardware is much slower than this, for interpersonal communication one packet every few seconds is sufficient, and such traffic would impose negligible overhead in CPU time and energy consumption.

To ensure that only few packets need to be decrypted and verified, AllNet needs a prioritization mechanism. This mechanism is described in Section IV.

Finally, public key encryption is only secure if the public keys are exchanged securely. This can be accomplished with Certificate Authorities, as in the most popular uses of SSL/TLS, or by interpersonal key exchange, as in PGP, or even by using an electronic "magic wand" as in Amy [8]. The last two techniques are independent of the infrastructure and have little or no cost, so may be popular for AllNet.

III. A Network for Interpersonal Communication

The resource and bandwidth demands for interpersonal text-based communications are slight. It is sufficient to note the success of SMS (text messages) and Twitter, both of which rely on exchanges of very short messages. Even a typist working at 100 words per minute only produces 10 bytes per second, and existing user interfaces on mobile devices are inadequate for most users to type at 100 words per minute. By comparison, a 4G cellular connection that is bandwidth limited to a very low 50MB/month can carry almost 20 bytes per second for the entire month, and considerably more if only used in short bursts, as most users would.

Such low-bandwidth communication requires relatively few resources. This is important on mobile devices that often are more limited than other computers in bandwidth, energy, storage, and computing power. In addition, sometimes communications are charged based on usage. For all these reasons, it is better for AllNet by default to consume a negligible amount of resources, particularly bandwidth. The goal is for AllNet to consume at most 1% of any particular resource on a device.

This default behavior of AllNet can be modified to support special cases. For example, high-bandwidth multimedia communications might be supported when the units are within direct range of each other, or when the owners of all intermediate units explicitly agree to support such communication. For another example, if a message is being broadcast to all units in the local area in hopes of attracting somebody's attention, especially in a localized emergency, then there is no point in encrypting the communication. However, in the default communication mode, AllNet carefully limits its resource usage and encrypts communications.

In order to effectively use scarce resources, AllNet must prioritize traffic, as discussed in the next Section.

IV. Packet Priority

Allnet uses features of each packet to reasonably assign a priority to each packet, such that higher priority packets are more likely to be forwarded or to be displayed to the user. We also distinguish cooperative nodes, which follow the overall rules of AllNet to minimize traffic and maximize the value of the traffic carried. As long as most devices are cooperative nodes, AllNet should be effective even in the presence of non-cooperative or malicious nodes.

Many networking technology provide mechanisms to control the amount of resources used in transmitting a packet. Most notably this includes the Time-to-Live (TTL) field of the IPv4 header. Technologies such as limited broadcast and DTN necessarily also need a mechanism to control the spread of the information.

For AllNet, we expect that this information, as well as information about the encryption of the packet, can be used to prioritize traffic. Higher values of a hop count or time to live, for example, mean the network is likely to spread a packet further afield. This makes the packet more expensive for the network as a whole, and therefore gives the packet a lower priority. On the other hand, once a packet has reached its next-to-last hop, its TTL will be minimal and devices can give this packet a higher priority. This favors packets that the network has already spent resources to forward, as well as packets that travel shorter distances, both of which are desirable goals. While the distributed and free nature of AllNet lets each node determine its own policy on packet priority, cooperative nodes will generally favor packets that can be predicted to use the fewest network resources. This includes favoring smaller packets, and neighbors that send or forward less data.

The device resources include the CPU time to decrypt and verify incoming packets. With limited broadcast as well as DTN transmission, nodes that are forwarding packets need not decrypt or verify such packets – encryption in AllNet is end-to-end. Each packet can carry in the clear a subset of the bits of the public key of the recipient. Then, every node that has a public key matching these bits must decrypt the packet just to see if they are the intended recipient. So, the more bits are given, the fewer nodes must decrypt the packet. Assuming that public keys are uniformly distributed, the probability of a node having to decrypt a packet showing n bits of the key is simply 2^{-n}. Therefore, cooperative nodes will prioritize packets showing more bits of the destination key.

Each AllNet device typically will have a limit both on the rate at which it will forward packets and the rate at which messages from strangers are presented to the user. This limit can be configured by the user, or set to a reasonable default value. Either way, such a limit encourages the transmission and communication of high-priority, infrequent data and discourages the transmission of low-priority data and spam.

V. Friends, Family, and Community

The previous section described limitations on forwarding anonymous packets, that is, packets whose sender and destination is not known, to limit the amount of resources devoted to supporting such communication.

This changes when AllNet is being used to forward packets on behalf of the owner of the device. In such cases, the owner (or a default) may decide to devote considerably more resources to AllNet traffic. For example, when the destination is directly reachable by the sender, there need not be any limit on bandwidth or energy consumption, because the communication is on behalf of the owner of the device. Similarly, when delay tolerant networking (DTN)

is used, a device will store messages for other devices that it has seen in the past few days, on the assumption that further contact is likely. As long as storage is abundant, large amounts of data could be transferred.

To support this DTN design, it is sufficient to keep a small Bloom filter [9] recording the public keys of the devices encountered within the past week (and keep each filter for two weeks or longer), and another Bloom filter for the keys that the device has sent data to or received data from. These filters quickly allow the device to determine whether to store a message for possible later delivery. These mechanisms could be effective even if only a few of the bits of the key are visible.

VI. Motivation to Participate

.

In any distributed, autonomous peer-to-peer network, each potential participant evaluates the perceived benefits and costs of participation before deciding whether to join the network.

Human motivations can be described as ranging from selfish to altruistic [1]. Individuals may be motivated to help build an online community or simply want to talk with their friends. Extending the notion of a social network, anyone for whose friends I have previously carried data, may be more willing to carry my data. Bloom filters can again be used to suggest keys that both sides might share, and possession of those keys can then prove the relationship. Possession of a key can be demonstrated by providing a hash of the key concatenated with a nonce provided by the requester.

By design, AllNet communication is pseudonymous and encrypted. This will encourage its use by people who value privacy and lack of centralized control, and discourage its use by people who dislike secrecy and anonymity, and value a more regulated system. Similar considerations apply to the TOR network [10], which can be used for illegitimate as well as legitimate purposes, and ultimately, to any peer-to-peer technology including BitTorrent.

It is useful to remember that congestion in today's Internet is avoided largely due to the cooperative behavior of millions of TCP senders, each of which slows down when it detects congestion. The cost to carry AllNet traffic should be much less than the cost of TCP congestion control. It is therefore reasonable to believe that, if AllNet is found to be useful, many people and devices will support it.

VII. Future Work and Considerations

AllNet is still entirely in the future. Here and in [11] and [1] we have just begun to sketch the design of the network. This design is likely to succeed because many of the necessary technologies already exist, and the only major effort is the design of the networking protocols and the system integration.

One question is, why hasn't something like AllNet been done before?

The first answer is that it has been done before, but in much more limited contexts, including the Networking for Communications Challenged Communities project [2]. These projects tend to focus on solving specific tasks for restricted uses. This has the advantage that the problem is better defined and solutions can more clearly be determined to be effective. In contrast, AllNet, as a backup mechanism, can be (like any backup) invaluable in

situations where it is really needed, but these are situations that everyone hopes do not happen very often. Our insight is that there are some situations, e.g. during travel or in the wilderness, that do not qualify as emergencies, but where AllNet might be sufficiently useful that individuals decide to support it.

There may be other reasons why something like AllNet has not yet become popular.

AllNet is decidedly noncommercial, and it is hard to envision anybody making money off a peer-to-peer free network technology that runs on existing hardware and does not require new Intellectual Property. In the absence of such profit motives, commercial developers would only be willing to provide such a service if it was in high demand, and such demand cannot be shown unless the product already exists. We hope to get around this chicken-and-egg dilemma by developing free software that individual users can download, until commercial providers find it in their own best interest to include AllNet with their products.

AllNet is also, by its very peer-to-peer nature and very much like PGP [12], independent of the infrastructure, free, and hard to control or manage. Individuals and their devices are each responsible for managing their own resources. However, unlike so many other peer-to-peer technologies, AllNet is designed for the average individual rather than for technically sophisticated individuals, and is not designed for exchanging large amounts of data.

The ultimate proof is in the pudding. We plan to build AllNet and deploy it as widely as possible. If this succeeds, obviously the technology is good and valuable, but until then, success cannot easily be predicted.

REFERENCES

[1] C. Desiato and E. Biagioni, "Sharing networking resources to create a pervasive infrastructure," University of Hawaii at Manoa, Department of Information and Computer Sciences, Tech. Rep., 2012. [Online]. Available: http://www2.hawaii.edu/ esb/allnet/desiato.pdf

[2] "Networking for communications challenged communities: Architecture, test beds and innovative alliances," 2008-2011. [Online]. Available: http://www.n4c.eu/

[3] A. El Fawal, J.-Y. Le Boudec, and K. Salamatian, "Multi-hop Broadcast from Theory to Reality: Practical Design for Ad Hoc Networks," in *First International Conference on Autonomic Computing and Communication Systems*, Rome - Italy, 2007. [Online]. Available: http://www.autonomics-conference.eu/

[4] R. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, February 1978.

[5] RSA Laboratories, "PCKS #1 v2.1: Rsa cryptography standard," 2002.

[6] T. Dierks and E. Rescorla, "The transport layer security (tls) protocol version 1.2," Network Working Group, IETF, Tech. Rep. RFC 5246, August 2008.

[7] W. Dai, "Speed comparison of popular crypto algorithms: Crypto++ 5.6.0 benchmarks," 2009. [Online]. Available: http://www.cryptopp.com/benchmarks.html

[8] W. Shin, K. Fukushima, S. Kiyomoto, and Y. Miyake, "Amy: Use your cell phone to create a protected personal network over de vices," *Consumer Electronics, IEEE Transactions on*, vol. 57, no. 1, pp. 99–104, 2011.

[9] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, Jul. 1970. [Online]. Available: http://doi.acm.org/10.1145/362686.362692

[10] N. M. Roger Dingledine and P. Syverson, "Tor: The second-generation onion router," in *13th USENIX Security Symposium*, San Diego, CA, August 9-13 2004. [Online]. Available: http://www.usenix.org/events/sec04/tech/dingledine.html

[11] E. Biagioni, "TWC SBES: Small: Allnet: trustworthy ubiquitous connectivity," Proposal to the National Science Foundation. Project description available at http://www2.hawaii.edu/ esb/allnet/proposal.pdf, Jan. 2012.

[12] P. Zimmermann, "Why i wrote PGP," Part of the Original 1991 PGP User's Guide (updated in 1999), 1991. [Online]. Available: http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html