EXTENDING DARKNETS VIA MOBILE AD HOC NETWORKS

Aaron Helton, St. Edward's University

ABSTRACT

The future of darknets, for good or ill, depends on their ability to adapt to new technologies designed both to defeat them and to facilitate them. One of the best ways to strengthen and extend darknets is through mobile ad hoc networks that can provide robustness, and anonymizing software that can provide a fair amount of anonymity to users of darknets. This paper explores some of the ways that mobile ad hoc networks can be secured against attacks aimed at reducing or eliminating the availability of darknet materials or discovering the identities of darknet participants that utilize such networks.

DARKNET OVERVIEW

The term "darknet" was coined in 2002 by four Microsoft employees. It is typically used to describe one of the many peer-to-peer file sharing networks in wide use today. As Biddle, England, Peinado and Willman [3] state, a "darknet is not a separate physical network but an application and protocol layer riding on existing networks." Ideologically, however, such networks are thought to exist on the fringes of the regular, "legitimate" Internet. Despite this, evidence suggests that usage is on the rise. For example, according to Nathan Anderson [1], writing for technology news site Ars Technica, users (called peers) of one of the most popular BitTorrent site on the Web, ThePirateBay, recently broke the twenty-two million mark. This represents only a fraction of total peer-to-peer file sharing, since this is only one site and one protocol. There are still numerous users on other file sharing networks such as Kazaa, GNUtella, and the like. The trend in peer-to-peer file sharing has been a steady increase in use over the past decade.

At the time of this writing, and despite significant legitimate uses for peer-to-peer networks, digital piracy of software, music, and movies remains the most prevalent use of darknet technologies. So far, the largest deterrents to such uses have been legal and technological. The media industries, largely comprised of Motion Picture Association (MPA) and Recording Industry Association (RIA) member organizations, have waged a nearly continuous war against file sharing networks since the days of Napster. Armed with existing copyright law, which was strengthened considerably by the Digital Millennium Copyright Act (DMCA) in 1998, the RIAA alone has "filed, settled, or threatened legal actions against at least 30,000 individuals" since 2003, according to a white paper published by the Electronic Freedom Foundation. [6] Even so, the impact on actual file sharing has been minimal, as the popularity of file sharing networks has grown nearly unabated in the last five years.

Technological deterrents for digital piracy, according to Biddle, et al [3], focus mainly on preventing or delaying "the injection of new objects into the darknet." Any litigation targeting circumvention of such technological protection measures, or TPMs, are explicitly covered under the DMCA itself. Other TPMs have been proposed by various internet service providers, namely Comcast's willingness to attempt deep packet inspection [2] and bandwidth throttling to curb file sharing (tactics it has since abandoned as unfeasible). Fred von Lohman [10], speaking specifically about the DMCA, surmises that "[t]rends in digital distribution technologies…indicate that any regulatory regime

focused on TPMs as a solution to this problem may be doomed to fail." Thus the technological impediments seem to have as little impact on the use of darknets as legal ones. Darknets simply refuse to die.

Both approaches have their drawbacks, aside from their relative inefficacy in stopping the unauthorized trade of copyrighted works. For one thing, as Von Lohman [10] points out, TPMs are easily circumvented, and their presence places undue burden on legitimate users. Second, extensive litigation has the potential to catch innocent parties in the dragnet, and the fact that very few of the file sharing cases have actually gone to court means that few precedents have been set for case law in those that are proceeding through trials. Third, in countries where the flow of information is tightly controlled, peer-to-peer networks offer capabilities of disseminating information that might otherwise have been restricted. Therefore it is beneficial to arm average Internet users with tools to prevent or circumvent these measures, regardless of how they are actually used.

To combat the overreaching powers of oppressive governments and organized media cartels, network technology must make provisions for the greatest amount of anonymity feasible and reasonable robustness against denial of service attacks, man-in-the-middle attacks, deep packet inspection (and resulting bandwidth throttling) and any other points of failure or discovery. This can be achieved with a combination of existing technologies, not the least of which is the mobile ad hoc network, or MANET.

MOBILE AD HOC NETWORKS

Mobile ad hoc networking is not a new concept. Its roots lie in the "packet radio" networks developed by DARPA in the early 1970s. Originally envisioned as the future of battlefield communication, mobile networking has taken a new direction. More appropriate terminology, according to the Internet Engineering Task Force's (IETF) charter on mobile networking, RFC2501 [4], is "Mobile, Multihop, Wireless Networking." Specifically, the applications that will be most useful, such as linking mobile networks to the physical Internet or transmitting revolutionary manifestos, require extensive use of the IP protocol. Thus, routing and data transmission will occur within a well-known framework. The largest constraint here is additional routing complexity, as mobile devices would also have to know about routes to the wired Internet. Advances in mobile network technologies, especially for mobile phones, has increased bandwidth available to wireless devices, and so ad hoc networking should be possible even now.

Regardless of the protocols used, all mobile networks share certain characteristics. The topology is dynamic, with the nodes changing location rapidly and often unexpectedly. In such networks, available bandwidth per device may be limited (although this is improving), often due as much to power constraints as the signal strength constraints. Also, security in such networks is only as good as existing wireless network security. Mobile wireless networks are susceptible to "eavesdropping, spoofing, and denial-of-service attacks" [4] to a greater extent than their wired counterparts.

Implementing mobile networks is not trivial, in part because of the above characteristics. In addition to these, probably the most significant challenge of implementation is routing itself. Because a mobile network would be useless without the ability to reconfigure routes on-demand, a number of approaches have been suggested. All approaches are similar in their basic methodologies, in that they rely on small

discovery packets to roam around the nodes on the mobile network to establish and maintain a list of current routes. The two discussed here, however, differ somewhat in their approach to securing against the types of attacks to which these networks are necessarily susceptible.

Mobile routing algorithms come in three basic flavors. Table-driven algorithms "try to maintain routes to all other nodes at all times." [5] This approach is the same approach taken by the Bellman-Ford equation, and differs greatly from the approach taken by demand-driven algorithms, which "gather routing information when a data session to a new destination starts, or when a route which is in use fails." [5] The third variety, a hybrid approach, combines the reactive nature of demand-driven algorithms with the reactive nature of table-driven algorithms. Two such routing schemes, discussed here, are AntHocNet and ANODR (ANonymous On-Demand Routing).

AntHocNet uses reactive measures to establish routes when such routes are requested, and proactive measures to attempt route improvement. Its basic methodology is based on the concept of Ant Colony Optimization (ACO), a natural phenomenon by which ants establish direct routes to food sources. While successful versions of such protocols exist already for wired networks, AntHocNet was developed to extend that functionality efficiently to wireless networks. To establish routes and to maintain paths, AntHocNet utilizes small control packets called ants, which adaptively estimate the quality of each local routing choice. [5] The result is a distributed route discovery and path maintenance that also has the desirable properties of being scalable, adaptive, and automatically load-balancing. These properties go a long way toward maintaining the reliability required for use as darknets, especially if requested information originates from within the mobile portion of the network and is to travel to any number of wired destinations on the Internet. However, this is but one facet of the overall security picture, and it provides no measure of anonymity.

ANODR is mechanically very similar to AntHocNet, in that it has both a reactive path establishment phase and a proactive path maintenance phase. It also relies on path discovery packets similar to AntHocNet's ants. The major difference, however, is that in addition to providing a multi-path routing environment, it also addresses privacy concerns. ANODR extends other protocols by providing an "untraceable and intrusion tolerant routing protocol for mobile ad hoc networks" (emphasis original). [7] This is achieved by adding some complexity to the algorithm such that actual node addresses are abstracted by a pseudonym, and the actual node-specific information is included inside a one way hash (so-called trapdoor). This requires a bit more overhead to process the routes, but has the effect of rendering the senders and receivers untraceable. Because of this approach, "an on-demand ANODR route is traceable only if all forwarding nodes en route are intruded." [7] Given the highly distributed nature of the networks likely to use this technology, this kind of intrusion is unlikely. While this technology has enormous and quite obvious benefits for military use, it adapts well for use with the purposes behind darknets by masking the sender.

COMPROMISING MOBILE AD HOC NETWORKS

Tactics that are likely to be used against mobile networks that host darknet content are the same ones used against wired networks, and include denial of service, eavesdropping, packet inspection, and spoofing. Further tactics, such as bandwidth

throttling and deep packet inspection can be employed by internet service providers to determine the nature of traffic passing through their networks and to attempt to throttle the speed at which such information might be transmitted. This is really only effective at the edges between wired and wireless networks. Each tactic has a specific goal, and the risk of each can be reduced or eliminated by very specific means.

A denial of service (DOS) attack attempts to render the source of objectionable content inaccessible to the rest of the network, either by saturating the network bandwidth available to the host node, by exhausting the resources of the target node (as happens with the so-called Slashdot effect, where a web site is brought down by too many simultaneous users), or by conducting similar attacks on nodes in the host's route. An effective attack requires a bit of information, and can take several forms, some unique to mobile wireless networks. The very basic requirement for such an attack to succeed is knowing where the target node is and being able to target it directly. In wired networks, simply picking apart packets passing through the network is sufficient to get the IP address of senders or receivers. This can work in one of two ways: by becoming a recognized node in that network, or by a man-in-the-middle attack. These attacks will be discussed in the following paragraphs, but it is important to mention them here, since they offer the best ways to get the IP address of an offending node. Once this information is known, it is trivial to initiate the denial-of-service attack.

In addition to the traditional forms of denial-of-service attacks, wireless networks are susceptible to radio jamming (signal saturation or network congestion) and battery exhaustion. With radio jamming, “an attacker can deny service to the nodes in a given area by jamming the radio frequencies they use.” [8] In terms of mobile wireless networks, especially those whose edges also touch some edge of the physical Internet, that means the threat is doubled. If the attacker is in range of the wireless device that is the target of the attack, then simply saturating the wireless bands available to such devices would be sufficient to reduce or eliminate that node’s availability. The drawback of this approach is that, unless it’s done by a government, government agency, or someone working in collusion with a government, it carries potential legal risk. Thus, as a tactic against file-sharing, it might only find sparing use. The other possible approach to deny a node’s availability is a network flood (like the aforementioned Slashdot effect), in which the attacker attempts to overwhelm the target with more packets than can be processed.

The far more likely scenarios for compromising wireless hosts are eavesdropping, packet inspection, and spoofing, especially if the goal is to discover the identities of peer to peer users or the contents of the files being exchanged. Eavesdropping allows the attacker to capture information passively to help identify the source or destination of any packets analyzed. This is similar to deep packet inspection, a tactic employed by some internet service providers, wherein the goal is to help shape traffic in a fair way or to discover the transfer of files that infringe on some copyright. While this is definitely problematic if the sender and receiver wish to maintain some confidentiality, it is far eclipsed by the threat of spoofing. Spoofing simply means that some other node has either fooled other nodes into believing it is a legitimate source or destination, or that it contains files that are marked as legitimate. This tactic has been used in the past by the RIAA and MPAA in their battle against file sharing networks. By creating files that look authentic, or by creating nodes that participate in file sharing, the attacker gains access to

the file sharing network. This seriously impacts the reliability of any darknet and is the most difficult to protect against.

SHORING UP THE MOBILE NETWORK

Mobile ad hoc networks must be resilient to node outages while providing for both the reliability of the files that are transferred and the security of the sharers' identities if they are to be used as darknets. Doing so is technically challenging and will require several steps. For wired networks, some of these challenges become easier to solve. For instance, there are secure routing protocols, IPSec, and other tunneling protocols that protect the information being sent over an otherwise unsecured network such as the Internet. However, because mobile and wireless devices are typically smaller than wired nodes, and their mobility is predicated on the use of battery power, both range and overall bandwidth are ultimately limited, if not in terms of actual speed and distance, then in terms of duration of presence. Secure routing and transport protocols consume greater resources, including processing and bandwidth, which makes them less suitable for mobile networks. Thus, from the standpoint of mobile ad hoc network security, an acceptable routing protocol should only provide for robust path maintenance to guard against denial of service and other node outages. Identity security and network purity should be addressed by other means.

Confidentiality or anonymity requires that a software solution be used on the sending and receiving nodes such that no intermediary node can be aware of what is being transmitted. One of the most mature of these software technologies is onion routing, specifically Tor. Developed by Roger Dingledine and Nick Mathewson of Free Haven and Paul Syverson of the Naval Research Laboratory [9], the Tor project "helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination." In this way, determining which machine is the actual sender is very difficult. Tor acts as a black box with a number of defined exit nodes. Traffic moving across the Tor network is encrypted, then routed through random Tor nodes and exits the network (thus re-entering the public Internet) from a similarly random exit node. This has several effects on such traffic. First, since no node inside the Tor network can be entirely certain of the origin of any Tor traffic, it cannot reveal that source. Second, since the data traveling around the Tor network is encrypted, the contents of the data stream are unknown to anyone except the requesting party. Third, since the exit nodes are used randomly, tracking a particular host's communications between a Tor network and the public Internet is almost impossible. Ideally, traffic would never need to leave such secure networks, but then their usefulness on the whole might be diminished. The reality is that there will always be some hosts that have defined exit nodes. Even if an eavesdropper is using a machine inside the Tor network, identifying the source host of any transaction is nearly impossible.

The only protection still lacking is preventing file spoofing and host intrusion into the trusted network. To date, this has scarcely even been addressed, despite the problem it poses. It should form the basis of continued research in this field, as peer to peer networks show no signs of disappearing and mobile ad hoc networks appear to be one of the next steps in networking innovation.

CONCLUSIONS

By combining a robust routing protocol with anonymizing software, mobile ad hoc networks can be used in the creation of mobile ad hoc darknets whereby information can pass freely and almost anonymously, operating well outside the direct control of oppressive governments and big media cartels. Combating such networks directly will be difficult even for governments, making this the likely choice for new iterations of networked societies.

REFERENCES

1. Anderson, N., Pirate pride in Sweden as Pirate Bay hits 22 million peers, 2008, http://arstechnica.com/news.ars/post/20081105-pirate-pride-in-sweden-as-pirate-bay-hits-22-million-peers.html, 2008.
2. Bangeman, E., FCC officially opens proceeding on Comcast's P2P throttling, 2008, http://arstechnica.com/news.ars/post/20080114-fcc-officially-opens-proceeding-on-comcasts-p2p-throttling.html, 2008.
3. Biddle, P., England, P., Peinado, M., & Willman, B., The darknet and the future of content distribution, *2002 ACM Workshop on Digital Rights Management*, 2002.
4. Corson, S., & Macker, J., Request for comments: 2501, mobile ad hoc networing (MANET): routing protocol performance issues and evaluation considerations, 1999 http://www.ietf.org/rfc/rfc2501.txt, 2008.
5. Ducatelle, F., Di Caro, G., & Gambardella, L. M., Using ant agents to combine reactive and proactive strategies for routing in mobile ad-hoc networks, *International Journal of Computational Intelligence and Applications*, 5, (2), 169-184, 2005.
6. Electronic Frontier Foundation, RIAA v. the people: five years later, 2008, http://www.eff.org/wp/riaa-v-people-years-later, 2008.
7. Kong, J., & Hong, X., ANODR: anonymous on demand routing with untraceable routes for mobile adhoc networks, *International Symposium on Mobile Ad Hoc Networking & Computing*, 2003.
8. Stajano, F., & Anderson, R., The resurrecting duckling: security issues for ad-hoc wireless networks, *Proceedings of the 7th International Workshop on Security Protocols*, 172-194, 1999.
9. Tor: overview, 2008, http://tor.eff.org/overview.html.en, 2008.
10. Von Lohman, F., Measuring the Digital Millennium Copyright Act against the darknet: implications for the regulation of technological protection measures, *24 Loyola of Los Angeles Entertainment Law Review*, 635, 2004.