Universal Peer-to-Peer Network Investigation Framework

Mark Scanlon (mark.scanlon@ucd.ie)
School of Computer Science and Informatics,
University College Dublin, Ireland.

amazon web services™
IRISH RESEARCH COUNCIL
An Chomhairle um Thaighde in Éirinn

ABSTRACT

Peer-to-Peer (P2P) networks are becoming widely used as a low-overhead, efficient, self-maintaining, distributed alternative to the traditional client/server model across a broad range of cybercrimes and cyberattacks. These cybercimes can take the form of distributed denial of service attacks, authentication cracking, phishing attacks, unauthorised distribution of copyright material, spamming, identity theft, cyberwarfare or malware distribution. These cyberattacks can also cross over into the physical world attacking critical infrastructure causing its disruption or destruction (power, communications, water, etc.). P2P technology lends itself well to being exploited for such malicious purposes due to the minimal setup, running and maintenance costs involved in executing a globally orchestrated attack, alongside the perceived additional layer of anonymity. In the ever-evolving space of botnet technology, reducing the time lag between discovering a newly developed or updated P2P botnet system and gaining the ability to mitigate against it is paramount. Often, numerous investigative bodies duplicate their efforts in creating bespoke tools to combat particular threats.

PREMISE FOR UNIVERSAL FRAMEWORK

Since P2P networking has become mainstream, the technology has been deployed across a broad range of systems and services. While the level of variation in topologies is significant, all P2P networks must share a number of common attributes [1]:

- **Ability to connect to the network (bootstrapping)**
  When a new node wishes to join the network, it must have the ability to contact at least one other active participant in the network.
- **Record Active Nodes**
  In a decentralized network the peers themselves must all contribute to the recording of active nodes on the network. In a centralized design, this duty falls on the controlling server(s). As each new node comes online, it announces its presence to the database maintainer and requests a list of other active peers to begin working.
- **Query/Order/File Propagation**
  In order for a P2P network to fulfil whatever the purpose it was designed for, intra-peer communication is requisite.
- **Software Maintenance**
  The P2P enabled binary can quickly become out-dated. The upgrade process must be simple to perform while maintaining node uptime. While newer versions of the application might have additional functionality, it must to ensure backwards compatibility otherwise the network as a whole may suffer.

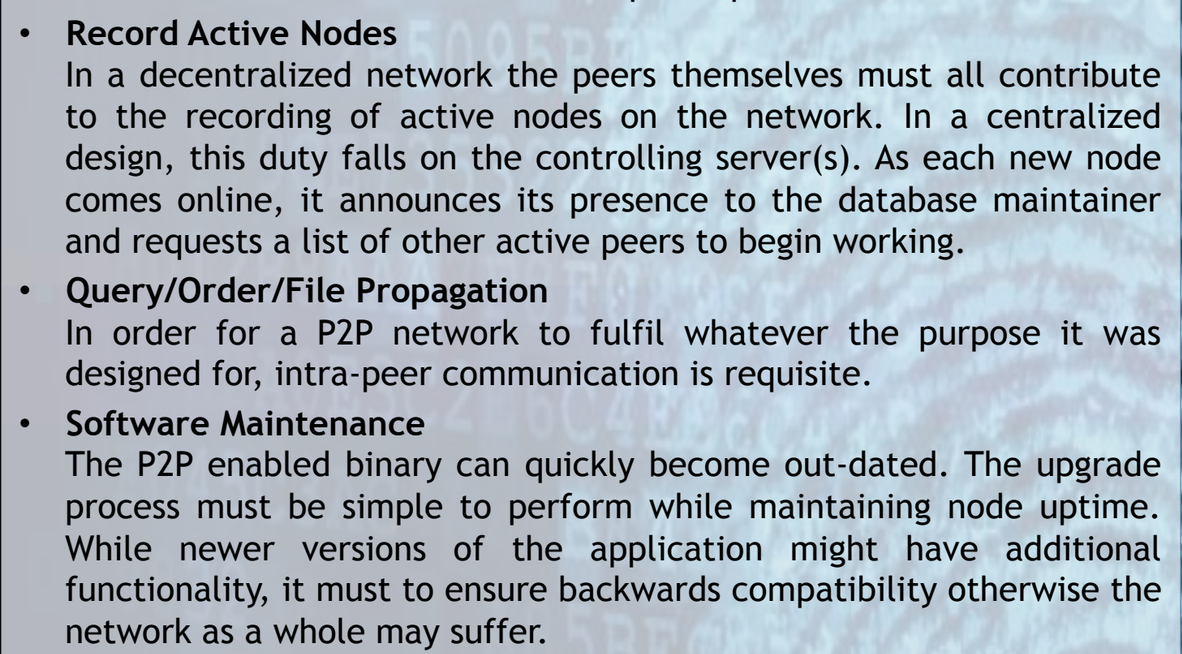

Fig 1. Overview of the UP2PNIF

PROGRESS TO DATE

A collaborative framework for the investigation of P2P based cybercrimes can greatly improve the time from network discovery to investigation. This has been designed and implemented for a select number of P2P networks. Reusing common investigative methodologies across different P2P networks can fast-track the development process. Standardised configuration, network characteristic specification and outputted digital evidence avoids the current practise of developing a bespoke tool per network to be investigated. Using common processing, gathered data can quickly be analysed and meaningful data can be extracted. For example, Figure 2 shows the results of a month long investigation on BitTorrent TV Show piracy at a global city level.

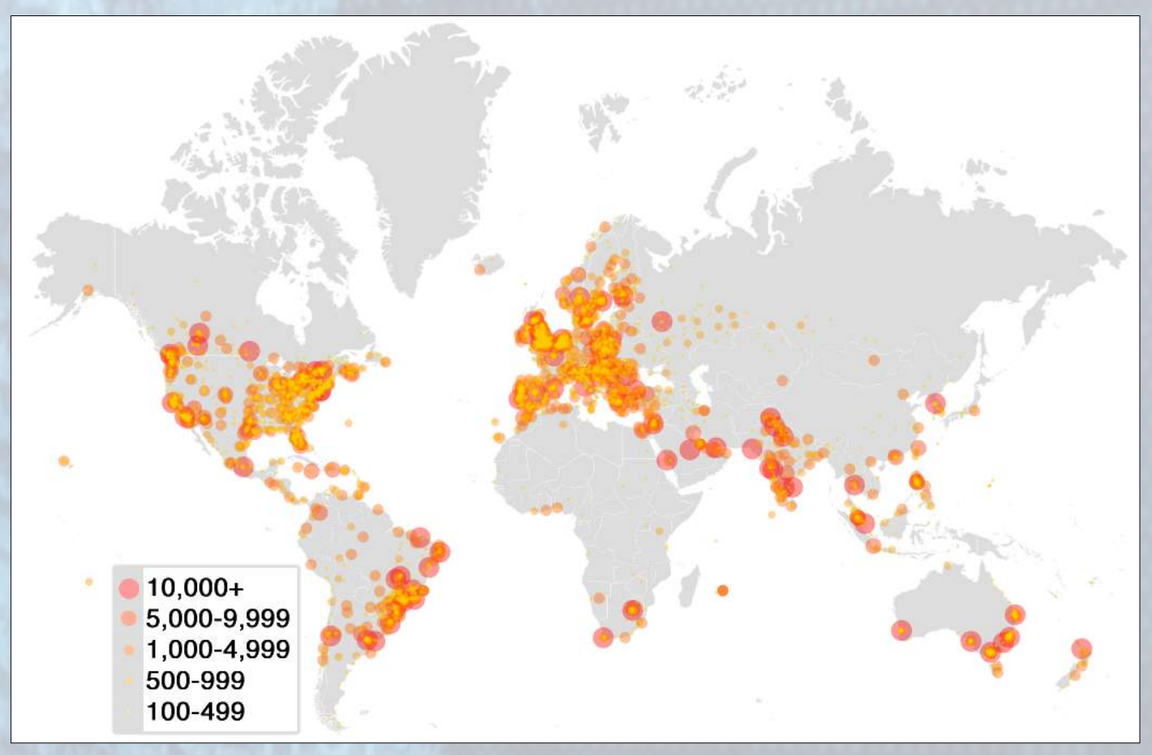

Fig 2. Geolocational Distribution of BitTorrent TV Show Piracy

P2P has recently been used to build a secure, cloudless alternative to popular file synchronisation tools, such as Dropbox and Google Drive. These tools are gaining significant popularity, with BitTorrent Sync gaining over two million active users in December 2013. The dissection of this tool's network protocol facilitated the quick development of an investigative tool capable of recording what peers are involved in the sharing of a particular piece of content [2]. This information might prove invaluable in the focusing of a forensic investigation resulting in the discovery of further suspects.

CONCLUSION

The design and results from initial testing for the UP2PNIF and its constituent parts has been published and peer reviewed [3]. The extensibility of the framework should facilitate the relatively easy addition of further P2P networks compared to current network investigation methods. Future work will include the building of further common network components to increase the range of P2P networks capable of being investigated. Releasing the framework open source should encourage collaboration in combatting this common issue.

REFERENCES

1. Scanlon, M., Kechadi, M-T., *Peer-to-Peer Botnet Investigation: A Review*, International Symposium on Digital forensics and Information Security (DFIS'12), September 2012.
2. Farina, J., Scanlon, M., Kechadi, M-T., *BitTorrent Sync: First Impressions and Forensic Implications*, Digital Forensics Research Workshop EU (DFRWS EU), Amsterdam, Netherlands. May 2014.
3. Scanlon, M., Kechadi, M-T., *The Case for a Universal Botnet Peer-to-Peer Network Investigation Framework*, International Conference on Emerging Cyberthreats and Countermeasures (ECTCM'13) Regensberg, Germany. September 2013.