The First International Conference on Digital Forensics and Investigation (ICDFI) (2012)

Enhanced monitoring rule through direct node query for Foxy Peer-to-Peer Network

Ricci S. C. leong, K. P. Chow Computer Forensics Research Group Center for Information Security and Cryptography The University of Hong Kong



## Typical P2P Clients

| Web 😭 My Ka<br>Kew search 🛝 D | ois Accions Telp   |   |  |  |  |  |   |   |                         |   |         |
|-------------------------------|--|---|--|--|--|--|---|---|-------------------------|---|---------|
| 🔁 🙀 🦂 🕅                       | azaa 🚺 Theater 🔍 Search 😤  | Traffic 🔗 Shop 😤 T                              | Fell A Friend Revealed Free CD's           |  | Competence and an and                                    | -  |   |   |                         |   |         |
|                               | Download   | O Search Field                                  |  |  | D µTorrent 1.8   | B  |   |   |                         |   | -       |
| arch                          | Title  | Artist  | Size User                                  | ETA Band Album   | Ere giptions i   | Reib   |   |   |                         |   |         |
|                               | alia 👘 Julia   | Beatles   | 2,720KB ilsa3@KaZaA                        | 0:00:42 511 The Beatle   | es 👩 🌑 🔝   | 🭸 🗙 🕨 🖩 🕷  | A Y @   |   |                         |   | 1       |
| Search to                     | or audio files   | ife Beatles<br>nw Never Knows The Beatles       | 2,305KB 2 Users<br>3.466KB dkdc@KaZaA      | 0:00:36 511 Rubber So<br>7:42:08 1 Revolver  | Nante  | A 500  | Done Status   | Seeds Peers D   | Nown Speed Up Speed ET  | TA Uploaded Rate  | Aval.   |
| Search for:                   | Piggies  | The Beatles                                     | 4,860KB rwphilli@KaZ                       | 0:06:45 96 White Albu  | un O Obbe.wafer,   | 1 1.16-08  | 0.0% Downloadin   | g 1 (1) 11 (30)   | 0.618/6 5%              | 6d 0.8 0.000  | 1,243   |
| beatles                       | Junk   | The Beatles                                     | 2,325KB mcq@KaZaA                          | 0:00:36 511 Anthology  | (3 0   |  |   |   |                         |   |         |
| Found 122 files. Click        | k Search More to get mor   | n't Do That The Beatles                         | 2,387KB kornkid1@K                         | 0:01:08 279 Unknown  |  |  |   |   |                         |   |         |
| O All : O Title : (           | Artist     Helter  | ikelter The Beatles                             | 10,540KB rwphill@KaZ                       | 0:14:38 96 White Albu  | un 🦉 🚺 General   | W Trackers IP Peers C Ple  | ces 🗄 Pies 🎐 Sc   | seed (1) Logger   |                         |   |         |
| Search More                   | Stop Search Come   | ine in through t The Beatles<br>ogether Beatles | 1,839KB rwphili@KaZ<br>4.046KB defaultuser | 0:02:33 96 Unknown<br>0:08:42 62 Abbey Roa   | ac P   |  | Clent   | Flags Ni - Dov  | in Sp., Up Speed   Recs | Uploaded Downloaded   | Peer    |
| Back                          | I Want   | to Tell You The Beatles                         | 3,936KB dkdc@KaZaA                         | 8:44:49 1 Revolver   |  | 99.22  | BitConet/0.0.6.2  | DS X 500.0  | 0.6kB/w 110             |   | 1111111 |
| iore search options ?         | What's What's Amore Amore<br>Amore Amore A | The New Mary The Beatles                        | 5,880KB mcq@KaZaA                          | 0:01:32 511 Anthology  | /3 🔝 💻   | 218.broad.().(x.dynamic.163data.c.   | BitComet/0.0.7.0  | 05 20.6   | 110                     |   | 29.5 kt |
| <u>arch filter</u>            | If I Fel   | In Love With Y Beatles                          | 2,222KB TeenageRic                         | 0:01:43 172 Unknown  | us.  | 14, 211  | Reference of Linda  | 07 5.4  | 216                     |   | 72.210  |
| voe in what you ar            | re looking for, If you are   | The Beatles                                     | 6,806KB rwphilli@KaZ                       | 0:09:27 96 White Albu  | u 📄  | 0.58 broad sz.gd dynamic. 163data  | BtComet/0.0.9.7   | dH 2.8  |                         |   |         |
| ireus                         |  |   | 0.40000 J 121000                           |  |  | 185.51   | Xunlei/0.0.1.2  | DSH 1.9   | 3   0                   | 16:0 kB   | 4.28    |
| ransfers Vi                   | iew Tools Plugins Help   |   |  |  | -  | 79.124.broed.xw.sh.dynamic.163da   | uTorrent 1.8.1  | dH 0.5  |                         |   | 12.7 k  |
| Comproved Th                  | John Topp Dagup Top  |   |  |  |  | 145.105  | Xunle/0.0.1.2   | DSH 0.3   | 110                     |   |         |
| 📄 🔊 I                         | 🖻 🔄   😣 🛆 '  | ▽ \∀   😒 🛈                                      | ) 😔 🖯 🔜 🕅                                  | 🗧 🔁 eMule  | e vû.48a VeryED Build                                    | 080627   |   |   |                         |   |         |
|                               |  |   |  |  |  | etical And Ale   | FOXY  |   |                         |   |         |
| file                          | (F) edit (E) Show ('   | /) commonly used                                | d settings (_R) min                        | efields (C) tool (T  | ) componen »   | etical And Ak<br>Igative Data<br>d Scorecard.<br>s An Intro<br>dar Science                                   | FOXY<br>國克牛行<br>Q 建克牛仔  |   |                         | -   | ×       |
| file                          | (F) edit(E) Show()<br><u> </u> 5 3   | /) commonly used                                | d settings (.R) min                        | efields (C) tool (T  | Componen <sup>»</sup>                                    | etical And Al<br>Igative Data<br>d Scorecard.<br>der Science   | FOXY<br>地支井行<br>Q 建支井行  | adam i Majar dat M  |                         | -   | ×       |
| file                          | (F) edit (E) Show ()<br>5 迅雷5<br>Thundor 5   | /) commonly used                                | d settings (_R) min                        | efields (C) tool (T,   | componen <sup>»</sup>                                    | etical And Al<br>lightive Data<br>d Scorecard,<br>ar - An Introv<br>dar Science                              | FOXY<br>独克牛仔<br>又雄克牛仔<br>丁化 新来  | ?金郡?:扶政196 午結果  |                         | -   | × 0     |
| file                          | (F) edit (E) Show ()<br>5 江雷5<br>Thunder 5   | /) commonly used                                | d settings (.R) min                        | efields (C) tool (T)   | componen <sup>»</sup>                                    | rtical And Al<br>Igathem Data<br>8 Sconsearch<br>dar Science   | 建筑牛仔           建筑牛仔           丁素: 重素           文件名称: 3) 建文牛仔 東点十世日  | ?金雷?;获到196 个结果<br>[1]属来 out]  | <u>.</u> Q2# <u>.</u>   |   | ×       |
| file                          | (F) edit (E) Show (1   | /) commonly used                                | d settings (R) min<br>movies to dog<br>ame | efields (C) tool (T<br><b>克祥</b><br>⊻ 资源搜  | Componen <sup>w</sup><br>Componen <sup>w</sup><br>条 网页搜索 | rtical And AA<br>lightmen Data<br>di Sconsente<br>ar Science<br>dar Science<br>EXT<br>EXT<br>Consente<br>Tit |   | ?金額?: 鉄道196 个結果<br>f5(重先 np3<br>た町3)<br>た町3 月(油気中行の級病子<br>指一 np3<br>素別の紹子3 np3<br>以和一 m約月光 np3<br>以和一 m約月水 np3<br>以和一 m約月水 np3<br>(第33人 np3<br>np3<br>点を全型10(重先 np3)  | _ Q ±≇ _                | 大小 安皇<br>大小 安皇<br>大山 68 HS Format Sourd<br>5,902 ED HS Format Sourd<br>5,902 ED HS Format Sourd<br>5,904 ED HS Format Sourd<br>5,907 ED HS Format Sourd<br>5,907 ED HS Format Sourd<br>5,907 ED HS Format Sourd<br>5,907 ED HS Format Sourd<br>5,908 ED HS Format Sourd<br>4,200 ED HS Format Sourd<br>4,200 ED HS Format Sourd<br>4,207 ED HS Format Sourd   | × *     |
| equi                          | (F) edit (E) Show (1   | /) commonly used                                | d settings (R) min<br>movies to dog<br>ame | efields (C) tool (T<br>文祥<br>受源搜<br>资源搜<br>の<br>の<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>し<br>の<br>の<br>の<br>し<br>の<br>し<br>の<br>の<br>し<br>の<br>し<br>の<br>の<br>の<br>の<br>の<br>し<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>し<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の<br>の | □ ■ ×<br>componen <sup>≫</sup><br>下載, 征<br>案 网页搜索<br>♪   | rical And Al<br>hydren Data<br>discovered<br>- An hitro<br>dar Scence  | FOXY           速度中行           「素」 激素           支持名数           2 建立中行手指表の意味           2 建立中行手指表の意味           2 建立中行手指表の意味           2 量子構築の単行する           2 量子構築の単行する           2 量子構築の単行する           2 量子構築の単行する           2 量子構築の重要に行うる           2 量素が構築の進発中行の結子           2 量素が構築の進発中行の結子           2 量素が目的通子者等           2 量素が相互の進力が差           2 量素の単行の進力が差           2 量素の単行の進力が差           2 量素の単行の進力が差           2 量素の単行の進力があり           2 量素の目的であり           2 量素の単行の進力があり           2 量素の単行の進力があり           2 量素の単行の進力があり           2 量素の単行の進力があり           2 量素の単行の進力があり           1 量素の単行の進力があり           1 量素の単行の進力があり           1 量素の単行の進力があり | *金額7: 鉄道146 千藤栗<br>f5.重キ-np3<br>約mp3<br>大明岁月(油気中行る級病子<br>約mp3<br>本第50代子3mp3<br>小四3<br>中約3月大-mp3<br>mp3<br>中35<br>本多生型(1)重単、np3<br>高5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>用5<br>大明3<br>円5<br>大明3<br>大明3<br>大明3<br>大明3<br>大明3<br>大明3<br>大明3<br>大明3 | _ Q ±≇ _                | TA         Stat           1,610 EB MPS Promit Sound         5,972 EB MPS Promit Sound           5,972 EB MPS Promit Sound         6,976 EB MPS Promit Sound           6,976 EB MPS Promit Sound         5,997 EB MPS Promit Sound           5,997 EB MPS Promit Sound         5,997 EB MPS Promit Sound           5,997 EB MPS Promit Sound         5,997 EB MPS Promit Sound           5,997 EB MPS Promit Sound         5,997 EB MPS Promit Sound           5,974 EB MPS Promit Sound         5,974 EB MPS Promit Sound           4,577 EB MPS Promit Sound         5,974 EB MPS Promit Sound           5,974 EB MPS Promit Sound         5,974 EB MPS Promit Sound           6,576 EB MPS Promit Sound         5,974 EB MPS Promit Sound           6,576 EB MPS Promit Sound         5,974 EB MPS Promit Sound           6,210 EB MPS Promit Sound         5,997 EB MPS Promit Sound           6,210 EB MPS Promit Sound         5,997 EB MPS Promit Sound           6,998 EB MPS Promit Sound         5,997 EB MPS Promit Sound           6,998 EB MPS Promit Sound         5,997 EB MPS Promit Sound           6,998 EB MPS Promit Sound         5,997 EB MPS Promit Sound           6,998 EB MPS Promit Sound         5,997 EB MPS Promit Sound           6,998 EB MPS Promit Sound         5,997 EB MPS Promit Sound | × ×     |

## Case 02/2008 : Edison Chen's scandal photos leakage

- On Feb 2008, Internet users use FOXY to share Edison's scandal photos:
  - Whenever new photos surface on the internet, they pass on the messages using the code: "hurry on bit the fox" and using the keyword "新閃卡"
  - Users share the files with names 新閃卡 by putting those files in their share folder
  - The photos spread rapidly on the Foxy network



 Law enforcement has tried to trace users who share the photos on the Foxy network





## Foxy P2P related incident

- 2008年1月至2月,陳冠希裸照事件時,大量網友以Foxy作為傳播裸照的工具。刑事警察局偵九隊表示,Kuro、ezPeer與BitTorrent等P2P軟 體必須指定欲分享的資料夾,其他使用者只能在指定的資料夾內搜尋檔案,但是Foxy的分享資料夾設定方式容易讓使用者誤設為「全機分 享」。組合國際電腦股份有限公司技術顧問林宏嘉建議:在Foxy的安全疑慮被排除之前,Foxy使用者應立刻徹底移除Foxy,並刪除電腦中的 相關資料夾。
- 2008年4月,香港亦發生Foxy洩露政府機密事件,涉及政府部門包括民航處、警務處及入境處。<sup>[2][3]</sup>
- 2008年9月,香港發生吉野家員工懷疑強姦少女事件,一段用手機拍攝的疑似香港吉野家員工強姦 少女的短片在網上流傳並透過Foxy散播。最後警方根據有關短片,拘捕了三名青年協助調
- 查。<sup>[4]</sup>富強姦短片首次在網上傳播的翌日,有關短片已在Foxy上快速傳播,來源多達約1200多個,並且出現雙重搜尋效應,可見Foxy的傳播速度比起手機、BitTorrent及普通網絡都快得多。



- 2009年4月15日,登記地址位於台北縣永和市環河東路的景昌資訊科技總部鐵捲門深鎖,原因是臺灣板橋地方法院檢察署於該日認定Foxy涉及 侵權,可讓人非法下載音樂、影片,侵權金額高達新台幣58.42億元,將設計推出該軟體的景昌資訊科技及其負責人李憲明依違反《著作權 法》起訴。<sup>[5]</sup>
- 2010年3月20日,Foxy因為分享未授權的電影和音樂而被眾多的電影商和唱片公司提告,景昌資訊科技負責人李憲明違反《著作權法》「擅自公開傳輸罪」而被法官判處1年半的徒刑,景昌資訊科技也被判處罰金新台幣70萬元;而這也是《著作權法》增訂「擅自公開傳輸罪」以來的第一起有罪判決。<sup>[6]</sup>
- 2010年11月,彰化縣員林鎮一名三十歲的林姓男子從Foxy下載了二十件中華民國國軍作戰防禦計畫檔案,被<mark>臺灣高等法院高雄分院檢察署</mark>依 「外患罪」起訴,求處八個月徒刑<sup>[7]</sup>。
- 2011年3月,一名33歲彭姓男子在新竹市東區中正路租間套房,利用FOXY軟體下載持卡人的消费紀錄,取得信用卡卡號、授權碼等個資,冒名 盜刷購買3C產品後立即拍賣掉,作為生活费及購毒品解癮。同年4月10日,基隆市政府警察局第一分局趁彭男取貨物時將他逮捕,彭男坦稱以 此手法盜刷18筆、得款新台幣71951元,訊後被警方依詐欺、偽造文書及妨害電腦使用罪嫌移送臺灣新竹地方法院檢察署偵辦。<sup>[8]</sup>



## Foxy P2P in 2012

- Foxy (P2P client) has been used for sharing files with traditional Chinese character keywords or file names in a search based network.
- Taiwan government took down the publisher of Foxy client application in 2009, but Foxy network is still operating for P2P file sharing.
- With the presence of the Foxy specific GWebCaches server (Gnutella 2 web caches server for Foxy network), Foxy clients can still connect to the existing Foxy network



# Case 05/09/2012 : Police confidential information leakage [New]



【本報訊】警方靠害,販募案的「金手指」敏感資料網上任睇!近日有市民經 Foxy軟件搜尋到警隊210份文件,包括一宗販募案污點證人的個人資料;負責撰 寫該文件的警官對此也感驚訝,擔心該名「金手指」資料曝光後性命受威脅。關 注警權組織則批評警隊無做好把關工作,再三洩露機密資料。

警方發言人稱,非常關注有警隊內部文件再流傳,會深入調查,以確定是否涉及 人為過失,如證實有人違規,會嚴肅處理,亦會知會受事件影響的人士。

210份文件輕易下載

■有市民前晚起一連兩晚,透過一度「沉寂」的Foxy軟件,輸入「Foxy天王」曾用 於搜索警隊機密文件的熱門關鍵字,「pol」及「memo」,輕易下載到210份相信 是警隊文件,部份更註明是「secret」(機密)。



## Keyword search in Foxy Client



## Sample download





## HOW TO FIND FIRST SEEDER(S)?

## Connection to Foxy Network

Is first seeder inside?

吉

○ 吉

檔案名稱

ഉി

•

٤ĩ 吉

**B** 吉

「「古」

🔊 吉

🔊 吉



## File distribution period in the Seeder's curve







## PREVIOUS MONITORING RULES

## The investigation rule to be analyzed



**Rule R1**: From  $T_1$  to  $T_s$ , the first observed seeder is the initial seeder, where  $T_s = min(T_R, T_e)$ .



## Simulation Experiments performed

- More than 100 simulation experiments were performed using FoxyNS3.
- File size 13MB, file packet size 512KB, simultaneous downloader connections as 3
- Four different sets of simulation experiments performed based on the following criteria
  - (i) average inter-arrival of search query time (T<sub>arr-s</sub>);
  - (ii) Number of downloaders interested in the target file during the simulation period (N<sub>p</sub>);
  - (iii) Number of hub nodes within the foxy network swarm (N<sub>h</sub>);
  - (iv) Data transfer rate (both upload and download rates) of all peers.



Mean and standard deviation results calculated from simulations of Set 2(a) & 2(b)





## Validation and analysis

- Step 1: if at T<sub>s</sub>, a single seeder is observed and the seeder is the first seeder, then the finding is considered to be correct.
- Step 2: if at T<sub>s</sub>, more than one seeder is found, then we will classify that as Type I error.
- Step 3: if at T<sub>s</sub>, the seeder is found to be rejected, then we will classify that as Type II error.



# Findings using previous monitoring rule

| Experiment(s) | Correct<br>identify a<br>seeder | Type I error | Type II error |
|---------------|---------------------------------|--------------|---------------|
| Set 1(a)      | 100%                            | 0%           | 100%          |
| Set 1(b)      | 100%                            | 0%           | 0%            |
| Set 1(c)      | 100%                            | 100%         | 0%            |
| Set 1(d)      | 100%                            | 80%          | 0%            |
| Set 2(a)      | 100%                            | 100%         | 0%            |
| Set 2(b)      | 100%                            | 100%         | 0%            |
| Set 2(c)      | 100%                            | 100%         | 0%            |
| Set 2(d)      | 100%                            | 100%         | 0%            |
| Set 3(a)      | 30%                             | 100%         | 0%            |
| Set 3(b)      | 30%                             | 100%         | 0%            |
| Set 4(a)      | 100%                            | 100%         | 0%            |
| Set 4(b)      | 100%                            | 100%         | 0%            |







## **REVISIT OF THE FOXY P2P FEATURES**

## Foxy Architecture

- 1. Connecting to the Foxy network
- 2. Search for files on the Foxy network
  - Based on Gnutella 2 protocol
- 3. Download file from a peer
  - Based on http download



## Search and response in Foxy P2P Network

- When query packets (Q2) with identical query pattern are found to be initiated from many different IP addresses, Q2 query value should be forward to all neighboring ultrapeers to speed up the spreading.
- All the Query Hit packets (QH2) are collected and the source IP addresses of the QH2 with the matched file name are identified.





## Key observations from supplementary set of Foxy Experiments

#### File packets range is initiated by client



Reconstructed packet captured of Foxy download initiation using Wireshark



## Key observations from supplementary

## set of Foxy Experiments

- Returned potential uploader may not be full seeder
- File packets download is controlled by uploader
  - Normal downloader can initiate no more than 3 connections
  - Uploader can permit 1 concurrent connection from each downloader
  - Download request tends to continue in stream
  - Downloader can requests for packets, but uploader will determine if slots are available for download







## Enhancement of monitoring rules

#### M-Rule1:

Search the network for the available upload source.  $U_t = (U_1, ..., U_n)$  where  $U_1$  to  $U_n$  are the identified available upload source at time t

#### M-Rule2:

Submit request to check their possession of individual file packet.  $F = (F_p \dots F_m)$  where a file consists of m packets.

EF(Fi) = 1, if packet is found,

EF(Fi) = 0, if packet cannot be found.

$$MRule(U) = \sum_{j=1}^{m} EF(Fj)$$

- MRule( $U_i$ ) = m, if full source uploader;
- MRule(U<sub>i</sub>) < m, if partial source uploader.</li>



## Enhancement of monitoring rules (2)

#### M-Rule3:

#### When more than one seeder found,

- the first seeder is uploader with the search time of U<sub>i</sub> initiated first and
- search duration time is longer than normal file download time.



# Explanation of the download and seeder monitoring (1)







# Explanation of the download and seeder monitoring (2)









### NS-3 Network Simulator

#### NS-3 is

- discrete-event network simulator for research and educational use
- C++ library which provided a set of network simulation models implemented as C++ objects wrapped through Python
- Capable of simulating network protocol at network

level



## Experiment Setup in NS-3

- Performed on two Ubuntu Linux machines using NS3.13 version
- File search portion
  - Simulate Gnutella 2 protocol
    - the bootstrap server communication protocol
    - Q2 and QH2 protocol
- File sharing portion
  - Simulate HTTP partial download protocol (using content range)
  - Communicate with CSMA network topology with Internet Stack and backbone network to 1Gbps



## Experiment Setup in NS-3



### Simulation in action





## Effect of Inter-arrival $(T_{arr-s})$



## Effect of Inter-arrival $(T_{arr-s})$

- Outline of the settings
  - Fixed data rate at 1024kbps
  - □ With variation of  $T_{arr-s}$  used (1a  $T_{arr-s}$  = 100s, 1b  $T_{arr-s}$  = 50s, 1c  $T_{arr-s}$  = 10s, 1d  $T_{arr-s}$  = 10s, 100s, random at 1000s)
- Findings
  - When file is less popular, first seeder is more likely to be rejected in previous rule
  - With the new rule, first seeder can be confirmed if the search has been initiated at early stage.

| Experiment(s) | Correct | Туре І | Type II | Correct (N) | Type I (N) | Type II (N) |
|---------------|---------|--------|---------|-------------|------------|-------------|
| Set 1(a) - L  | 0%      | 0%     | 100%    | 100%        | 0%         | 0%          |
| Set 1(b) - M  | 100%    | 0%     | 0%      | 100%        | 0%         | 0%          |
| Set 1(c) - H  | 100%    | 100%   | 0%      | 100%        | 0%         | 0%          |
| Set 1(d) - R  | 100%    | 80%    | 0%      | 100%        | 0%         | 0%          |
|               |         |        |         | ISC         |            |             |

### Effect of data rate with random Inter-

## arrival $(T_{arr-s})$

- Outline of the settings
  - Random T<sub>arr-s</sub> employed
  - With variation of data rate (2a 100kbps, 2b with some 1Mbps, 2c random between 0 100 kbps, 2d all 1Mbps)
- Findings
  - When random T<sub>arr-s</sub> and varying data rate, more downloader started the search and download time, thus more completed downloader would be identified when rapid-rising period reached (using previous rule)
  - When the uploader is requested by a lot of downloaders at initial stage, monitoring node may not be able to get sufficient packets for confirmation (using new rule)

| Experiment(s) | Correct | Type I error | Type II error | Correct (N) | Type I (N) | Type II (N) |
|---------------|---------|--------------|---------------|-------------|------------|-------------|
| Set 2(a)      | 100%    | 100%         | 0%            | 100%        | 0          | 0           |
| Set 2(b)      | 100%    | 100%         | 0%            | 20%         | 0          | 80%         |
| Set 2(c)      | 100%    | 100%         | 0%            | 100%        | 0          | 0           |
| Set 2(d)      | 100%    | 100%         | 0%            | 100%        | 0          | 0           |
|               |         |              |               |             |            |             |











## Effect of number of hubs

- Outline of the settings
  - Random T<sub>arr-s</sub> employed, 10 hubs
  - □ With variation of data rate (2a & 3a 100kbps, 2b & 3b with some 1Mbps)
  - Set 2 (overall view), Set 3 (individual hub view)
- Findings
  - When more hubs were involved, the shape of the seeder curve deviated more from the single hub seeder curve (using previous rule)
  - With the new rule, the search does not depends on the number of hubs. (using new rule)

| Experiment(s) | Correct | Type I error | Type II error | Correct (N)  | Type I (N) | Type II (N) |
|---------------|---------|--------------|---------------|--------------|------------|-------------|
| Set 2(a)      | 100%    | 100%         | 0%            | 100%         | 0%         | 0%          |
| Set 2(b)      | 100%    | 100%         | 0%            | 20%          | 0%         | 80%         |
| Set 3(a)      | 30%     | 100%         | 0%            | Same as 2(a) |            |             |
| Set 3(b)      | 30%     | 100%         | 0%            | Same as 2(b) |            |             |
|               |         | RG           | EE            |              |            |             |

ŝ

## Effect of transfer rate and leaf

### departure

- Outline of the settings
  - Random T<sub>arr-s</sub> employed, 10 hubs
  - 500 nodes, 200 downloaders
  - Mean data rate of 100kbps
  - Set 4(a) no leaf departure; Set 4(b) leaf departure between 2100 2500s

#### Findings

- Identification of first seeder not affected much by the departure of leaf nodes (using previous rule)
- With new rule, when the first seeder leave earlier than the search, the Type I error will increase (using new rule)

| Experiment(s) | Correct | Type I error | Type II error | Correct (N) | Type I (N) | Type II (N) |
|---------------|---------|--------------|---------------|-------------|------------|-------------|
| Set 4(a)      | 100%    | 100%         | 0%            | 100%        | 0%         | 0%          |
| Set 4(b)      | 100%    | 100%         | 0%            | 80%         | 20%        | 0%          |
|               |         | The form     |               |             |            |             |



## Results analyzed using new monitoring

## rule

- Effect of search initiation time
  - Direct query search must be initiated before appearance of second full uploader
  - The smaller the file, the shorter the earlier the search initiation time required
- Effect of downloader populations
  - At equilibrium stage of file sharing (during rapid rising period), download requests will be evenly distributed to various uploaders.
  - At initial stage, requests will be sent to early announced uploader.
  - Due to stickiness of the download process, requests will be concentrated to the same uploader.
- Reverse file packet existence check is faster for Foxy network
  - Because download requests for download packets will be submitted in sequential order (in real foxy P2P file sharing client), last packet of a file will be downloaded latest.
  - Thus, for Foxy P2P file sharing network, if last file packet is request first, then the time used for existence check could be shortened.





## Conclusions

#### From our experiments

- New findings about actual Foxy P2P network has been collected
- New monitoring rules (M-Rules) have been derived and compared with previous rule
  - Higher accuracy
  - Susceptible to the effect of hubs in the testing
  - Non-first uploader responded much faster than first uploader



## Next Steps

- Our future research
  - Determine the effective download initiation period
  - Extend our monitoring rules to other P2P environment

