

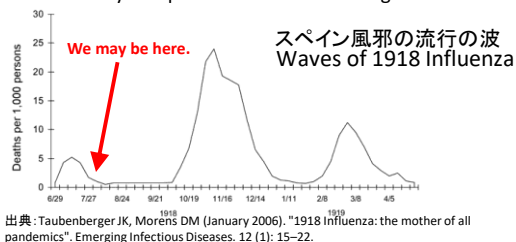
東京大学 人口密度観測プロジェクト (セグメント単位) の実施について

UTokyo Crowd Monitoring Project (Network Segment WG)

1. プロジェクトの目的 (Project Goal)

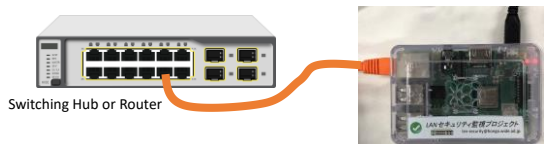
新型コロナウイルス第2波、第3波の到来に備え、人の密集度に気を付けながらキャンパスライフを送る必要があります。人手で通学・出勤簿を作って密集度を気にする方法もありますが、本プロジェクトで用いるネットワーク接続端末数を自動的にカウントする方法を用いれば、楽に密集度を推定することが可能になり、より効果的に感染症に対抗できるようになります。

We must be aware of crowded situation in campus lives due to the expected second/third epidemic waves of COVID-19. Automatic counting of connected hosts on a network will allow estimation of crowd-ness more easily compared to manual handling of commuters.



2. 概要 (System Overview)

- ① お使いのスイッチング・ハブやルータのLANの空きポートに観測モニタを接続します。
Connect your 'Monitoring Device' to a LAN port of your switch hub or router.



- ② 観測モニタの電源を入れます。
Power on your 'Monitoring Device'.

Then, it automatically starts monitoring.

1. IP address assignment by DHCP
2. Clock synchronization by NTP
3. To fetch the opt-out list from the database
4. To count up the detected hosts
5. Upload the number to the visualization server

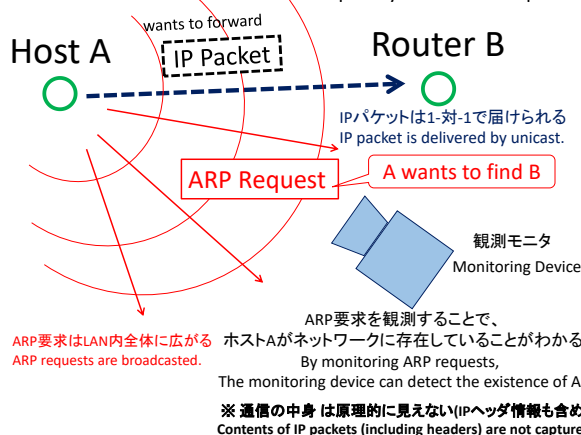
- ③ 可視化サーバを見ます
Check the visualization server

ネットワークのセグメントは、「研究室単位」、「建物単位」、「部局単位」といった区分になっています。観測モニタを用いると、その区分単位で端末数を数え上げ、増減傾向を可視化できます。「研究室単位」の可視化は匿名化され、建物名や部局名と関連付けられて示されるデータは広く集約されたものに限ります。Network segments are separated and managed by laboratory, building, department, etc. The monitoring device allows the visualization of increase or decrease of connected hosts by such a segment. Laboratory-based visualization is anonymized. The data associated with building names or department names are widely aggregated.

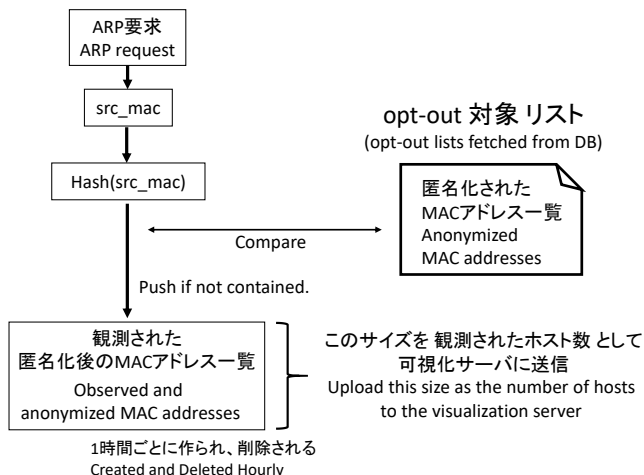
3. ホスト存在検知の原理 (How to Detect a Host)

本プロジェクトで用いる手法では、パソコンやスマホが行う個々のインターネット通信を見ることなく、サイドエフェクトとして発生するブロードキャストARP要求を観測することでホストの存在を検知します。

This project detects a host by observing the ARP requests broadcasted over the entire network segment, which is performed without capturing individual Internet communications developed by PCs and smartphones.



4. ホスト数カウントの方法 (How to Count Hosts)



観測モニタが取得するMACアドレスには、位置情報に相当するものが含まれますが、匿名化されるうえ、1時間ごとに消去されます。可視化サーバに送信されるデータは、(観測モニタID、時刻、ホスト数)のみであるので、個人に紐づく位置情報は保存されません。The MAC addresses observed by the monitoring device contains location information. However, they are anonymized and deleted every hour. Only (Monitoring device ID, timestamp, number of hosts) are sent to the visualization server, and location information associated to persons are not saved.

5. 対象となるネットワーク (Target Networks)

この周囲では下記ネットワークにて接続端末数の観測を行っています。The following networks monitors the number of hosts around here.



6. opt-out申請の方法 (Opt-out Application)

<https://www.crowd-monitor.net/opt-out/>

上記URLにアクセスし、ネットワーク接続ホスト数のカウント処理から除外してほしい端末のMACアドレスを登録してください。代表的な端末のMACアドレス確認方法は上記サイトに書かれています。登録するMACアドレスはお使いのブラウザ内で十分に匿名化してから送信されるため、生のMACアドレスが記録されることはありません。

Please access the URL above, and register the MAC addresses of the hosts which want to be exclude from the counting process of connected hosts. How to find your MAC address is shown in the URL above. The MAC addresses going to be registered will be transmitted after the anonymization within your web browser.

7. お問い合わせ (Contact)

東京大学 大学院 情報理工学系研究科 准教授 落合秀也
Associate Professor, Hideya Ochiai, Ph.D.,
Graduate School of Information Science and Technology,
The University of Tokyo
E-mail: ochiai@elab.ic.i.u-tokyo.ac.jp
TEL: 03-5841-6748