

閉じたWi-Fiネットワークを利用した ファイル共有システムの構築

地域の情報伝達をデジタル回覧板で

東京都立立川高等学校 平家 和志

研究動機/先行研究

研究動機

- 近所で自治会を抜けていくお年寄りが多いと感じ、回覧板が回らない家庭にも簡単かつ比較的速く情報を伝達できないかと考えたため



先行研究

- 「Wi-Fi Direct を用いた複数デバイス間ファイル共有転送最適化の検討」の論文を読み、Wi-Fiを用いることで、Bluetoothでは電波が届きにくく難しい「建物間でのファイル転送」を行うことができそうだと考えた

開発時の必須要件

- 画像・PDF・Wordファイルなど、テキスト以外のファイルの送受信⇒回覧板の代替手段
- 建物に対して工事が不要なこと⇒無線転送
- ファイルの到達範囲が広いこと⇒断続的なネットワーク
- サイバー攻撃を受ける機会の低減⇒閉じたネットワーク
- システムが安定していること⇒迂回可能なネットワーク
- 消費電力が比較的小さいこと⇒タブレットPC/一定時間ごとの実行

なぜ閉じたネットワークなのか

システムを使い続けられるようにするため

- もちろんいつかはシステムを更新しなければならない
- インターネットに繋がらないということは、送りたい情報を閉じたネットワークに取り次ぐ必要がある
- しかし、インターネットに繋がるのはリスクでもある
- 脆弱性/バグは潰しきれない。また、定期的な保守を行うのにも費用がかかる
- 安定したシステム:古い技術/変わらない環境
- 現在でも発車案内をWindows 2000で動かしている駅や、Windows XPで動いているデジタルサイネージもある
- 閉じたネットワークはこれらを実現できる

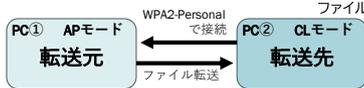
実験1

目的

- 実際にWi-Fiを用いたファイル転送が可能か検証するため
- WPA2などの暗号化を利用できるか検証するため

方法

- Fujitsu Arrows Tab Q5010/CE を2台用意
- OS:Ubuntu Desktop 22.04.2 LTS
- NetworkManagerを用いて1台でWPA2-PersonalのWi-Fiアクセスポイントを立てて(APモード)、もう1台をクライアントとして接続(CLモード)する。CLモードの端末からscpコマンドを用いてファイル転送を行う



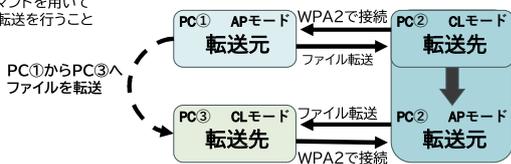
実験2

結果

- PC2からPC1に対してSSIDとPSK(パスワード)で接続。認証に成功した
- PC2にIPアドレスが振られ、scpコマンドを用いてファイルの転送を行うことが出来た

考察

- Network Managerを用いてWi-Fiのネットワークを作成し、ファイルの転送を行うことが出来た
- このファイル転送を繰り返すことで、ネットワークを形成できると考える



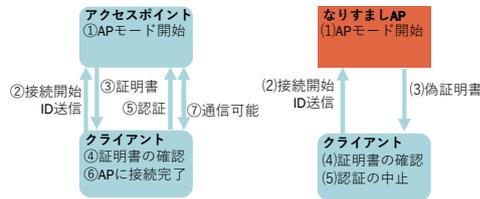
WPA2-Personalの限界

WPA2-Personalとは WPA2-Enterprise(WPA2-EAP)の利用

- クライアント端末がSSID(アクセスポイント名)とPSK(パスワード)で接続する方法
- 個人向けのWi-Fiの認証において今でも使われている方式
- SSIDが同じ「なりすまし」のアクセスポイントを立てられた場合に判別する方法がなく、攻撃を受ける可能性がある
- クライアント端末がSSIDに対してIDとパスワードで接続する方法
- 企業や学校などに設置されているWi-Fiの認証において使われている方式
- アクセスポイント(サーバー)が正規のものであるか確認する方法(証明書の確認)があり、「なりすまし」のアクセスポイントが立てられた場合でも安全
- ここからはeduroamや都立高校のBYODでも使われている **WPA2-EAP PEAP-MS-CHAP v2** を実験に利用していく



WPA2-EAP(PEAP)での接続手順



実験2

目的

- 実際にWPA2-EAP PEAP-MS-CHAP v2を利用可能なアクセスポイントを作成し、ファイル転送が可能か検証するため
- APモードとCLモードを1台の端末上で同時に実行できるか確認するため

方法

- Fujitsu Arrows Tab Q5010/CE を2台用意
- OS:Ubuntu Desktop 22.04.2 LTS
- APモード用に仮想NIC(ネットワークアダプター)を作成し、AP構築ソフトウェア(hostapd)とDHCPサーバー(isc-dhcp-server)を導入、認証サーバー(radius・Samba・Active Directory)を構築しWPA2-EAP PEAP-MS-CHAP v2なAPを作成
- CLモードでは実験1同様Network Managerを使用し、APモードの端末に対してscpコマンドを用いてファイル転送を行う



実験2

結果

- WPA2-EAP PEAP-MS-CHAP v2での接続に成功し、クライアント側にIPアドレスが振られた
- scpコマンドを用いて、CLモードの端末からAPモードの端末へファイルの転送を行うことが出来た
- APモードで実行する際、仮想NICには固定IPアドレスを割り当てるようにしていたため、CLモードの端末は固定のアドレスに対して接続すれば問題がなかった
- 仮想NICを作成することで、1つの端末内でAPモードとCLモードを両立できることが分かった
- hostapd-isc-dhcp-server-radius-samba-Active Directoryを用いることで、WPA2-EAP PEAP-MS-CHAP v2で接続可能なAPを立てられることが分かった
- WPA2-EAP PEAP-MS-CHAP v2なAPIに有効な証明書を配置することによって、接続する機器(CLモードの端末)が不正なAPIにアクセスしてしまうことを防ぐことができると考えられる
- ESP32やRaspberry Pi Pico WなどのWi-Fi搭載のマイコンボードをこのネットワークに加える場合は、内部で認証サーバーを動かすことが難しいため、CLモードの役割のみを与えるべきと考えられる
- Linuxが動作し、Wi-Fiを利用可能な安価な端末といえば、Raspberry PiやChrome Bookである。これらの端末はこの実験に適していると考えられる

考察

まとめ・今後の展望

まとめ

- 仮想NICを作成することで、1つの端末内でアクセスポイントとクライアントの機能を同時に使用できる
- hostapd-isc-dhcp-server-radius-samba-Active Directoryを用いることで、WPA2-EAP PEAP-MS-CHAP v2で接続可能なアクセスポイントを立てることができる
- APモードとして動く端末が自身に固定IPアドレスを割り当てた上でWi-Fiアクセスポイントを立て、IPアドレスを配布するようにし、CLモードの端末は固定のアドレスに接続することで、DHCP環境においてもAPモードの端末がCLモードの端末(同時に複数台接続される可能性がある)のIPアドレスを管理せずにファイル転送を行うことが出来る

今後の展望

- 更新日時が古いファイルをいつまで管理すれば良いのか実験したい
- ネットワークの規模、つまりコンピューターの台数を変更しながらファイルが全ての端末に伝わるまでの時間を計測し、最適な同期のタイミングを検討したい
- 通信強度を変えながら通信速度を計測し、どのくらいの通信強度があれば実用的なファイル転送を行えるか、その数値を検討したい
- scpコマンドはssh接続の仕組みに依存しているため、FTP(S)等のファイル転送プロトコルを使用することを検討したい
- GIGAスクール構想などで導入されている一人一台端末(例:Windows OS搭載タブレットPC/Chrome Book)は、スベックの面ではファイル共有システムに十分利用でき、特に更新される場合は余剰となるものが同時かつ大量に発生するため、今回の実験を大規模に、地域レベルで行う際には有用であると考えられる

参考文献

水村 直人 金岡 諒 齊藤 裕樹 高橋 淳二 戸辺 義人
「Wi-Fi Direct を用いた複数デバイス間ファイル共有転送最適化の検討」2016年
<https://zenn.dev/yuyakato/articles/b21541666a41a8>
@minosys (Qiita)
「RP4 に NetworkManager を導入し、wlan0 を ap にしたら良かった」2020年
<https://qiita.com/minosys/items/6571ab963b6c93a05e60>
@8mamo10 (Qiita)
「Ubuntu を無線 LAN ルーターとして稼働させる」2014年
<https://qiita.com/8mamo10/items/59adae2c9f286e041792>
Yuya Kayo (Zenn)
「Raspberry Pi 4, Samba 4, FreeRADIUS, hostapdを使ってWPA2 Enterprise対応APを構築する」2022年
「Raspberry Pi 4, Ubuntu 22.04 LTS, Samba 4を使ってActive Directory/ODCを構築する」2022年
<https://zenn.dev/yuyakato/articles/1186de8f2d675d>
富士通株式会社 無線LANのセキュリティ(設定マニュアル 第3版 2006年
<https://www.fmworld.net/biz/fmw/product/hard/network/manual/security/manual/chap100010.html>
みかんのゆるふわ技術ブログ
「Raspberry Pi WiFiアクセスポイント+クライアント同時使用」2022年
<https://www.mikan-tech.net/entry/raspi-wifi-ap-sta>
「Raspberry PiをWiFiアクセスポイントとしてスタンドアロン運用」2022年
<https://www.mikan-tech.net/entry/raspi-wifi-ap>
サイテックス・テクノロジー株式会社
Wirelessのあと EAPのななし(2) 2013年
<https://www.silex.jp/blog/wireless/2013/10/eap2.html>