1V-03

パケットスニフィングによるFree WiFiスポットのインターネット遮断の自動判定

瀬川　徳†，宮崎 敏明†
†会津大学コンピュータ理工学部

1. はじめに

日本は世界でも有数な災害大国である。2019年8月に非常に大きな勢力を持った台風が日本列島を直撃し、多くの地域で通信インフラに障害が発生して、お互いに連絡が取れない状況になった。筆者等は、電話やインターネットなどの通信インフラが使用できない状況でも、個人所有のスマートフォンを用いて、ローカル設置したWiFi無線通信環境を介し、災害現場の情報共有を可能とするRIMシステム(Resilient Information Management System)を提案している[1]。RIMシステムはNTTが開発した移動式ICTユニット[2]が災害現場で迅速に構築するWiFi無線通信環境を用いることを前提として開発した。しかし、移動式ICTユニットは数に限りがあり、広域災害発生時には、十分なWiFi通信エリアを確保できない。一方、スマートフォンの普及に伴い、近年、Free WiFiスポットが急速に整備され、屋外でWiFiを用いてインターネットにアクセスできる環境が整ってきている。筆者等は、Free WiFiスポットにRIMシステムのサーバを設置しておき、災害時に当該Free WiFiスポットからインターネットへの接続が出来なくなった状況でも、WiFi機能自体が正常動作していれば、インターネットへの回線をRIMサーバへ自動切替し、RIMシステムのサービスを開始する手法も提案している[1]。既提案手法においては、インターネット接続遮断の有無の確認には、RIMサーバが定期的にGoogleやAmazonなどの良く知られたインターネットサービスサイトにパケットを送信し、その反応の有無を確認することによって行っていた。しかし、既提案手法には、２つの大きな問題がある。第一の問題は、Pingパケットを送信するための送信システムがWiFiスポットに常時接続されている必要がある点である。公共のFree WiFiスポットは多くの場合、同時接続可能台数に制限がある。その限られた台数制限の一つをPingパケット送出のために占有してしまうことになる。第二の問題は、不要なPingパケットが大量にネットワーク上に放出される点である。セキュリティ機能が実装されたWiFiスポットでは、本動作がDOSアタックと誤認識されてしまう可能性がある。

本稿では、Free WiFiスポットにおいて、上記問題を解決し、インターネット接続遮断の有無を判断する新たな手法を提案する。具体的には、Free WiFiスポットを通過するパケットを監視するパケットスニフィングによる方法である。提案手法は、他のユーザがFree WiFiスポットを介してインターネットサービスを利用している状況で送受信されるパケットを監視するだけなので監視対象のFree WiFiスポットに一クライアントとして接続する必要もなければ、大量のPingパケットをネットワーク上に送出することもない。よって、Free WiFiスポット利用者に影響を与えることなく、当該Free WiFiスポットのインターネットの接続状況を確認できる。

Automatic Detection of Internet Disconnectivity at a Free WiFi Spot Using Packet Sniffing
Toku Segawa†, Toshiaki Miyazaki†
†Department of Computer Science and Engineering, the University of Aizu, Japan

2. 提案手法

提案手法の構成概要を図１に示す。システムは、Free WiFiスポットの無線ルータ、パケットキャプチャを行うPC、クライアントから構成されている。平時はクライアントがFree WiFiスポットを介してインターネットサービスを利用することができ、有事の際には、後述する手法によりインターネット遮断を検出し、インターネット回線をRIMサーバに切り替える。

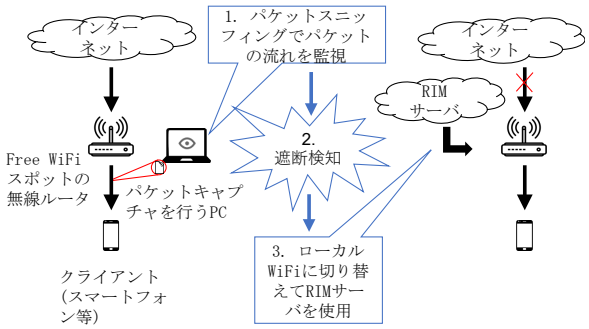

図1. システム概要

2.1. パケットスニフィング・モード

パケットスニフィングは、インターネットの接続状況を把握のための有効な手法である[3]。パケットスニフィングにより、サーバとクライアント間のパケットをロギング・解析することが可能になる。パケットをキャプチャする際には二つのモードが存在する。プロミスキャスモードとモニタモードである。プロミスキャスモードはキャプチャ対象のアクセスポイントに接続を認証されている必要がある。認証を済ませているためそのネットワーク上を流れる全てのパケットをロギング・解析できる。一方、モニタモードはターゲットとなるアクセスポイントに接続認証される必要はないが、キャプチャできるパケットに制約がある[4]。また、モニタモードを使用するには特定のNIC(Network Interface Card)が必要になる[4]。

ここでは、無線でのスニフィングを想定し、アクセスポイントに接続が不要なモニタモードを用いることとする。

2.2. ネットワーク遮断検出：ステップ１

本提案では、２つステップでインターネット遮断を検出する。ステップ1では、キャプチャされるパケット量で遮断の有無を判断する。インターネット遮断前後ではネットワークを流れるパケット量に大きな差が出るのが一般的である。図２に例を示す。本例は、以下の手順で、予備実験をし、得たデータをプロットしたものである。

キャプチャ時間を$(T_i|i = 1,6,10,20,30)$分とし、

1. パケットキャプチャ用のPCのNICをモニタモードに設定しパケットスニフィングを開始する。
2. $\frac{T_i}{2}$秒でアクセスポイントのインターネットを故意に遮断する。
3. X軸に経過時間、Y軸にキャプチャしたパケット量の累積をとり、キャプチャしたパケット量が急激に変化する時点を探索する。

図2は$(T_i|i = 1)$分のグラフであり、インターネット遮断前後でスニフィングしたパケット量が明らかに異なることが分かる。ただし、$(i = 6,10,20,30)$分の場合は、パケット量の急激な変化は見られなかった。特に、$(T_i|i = 20,30)$分の場合は、途中でキャプチャエラーが発生した。対象のWiFiスポットに接続しているクライアント数にも依存するが、１分程度のパケットスニフィングで、インターネットの遮断が検出できることが分かった。

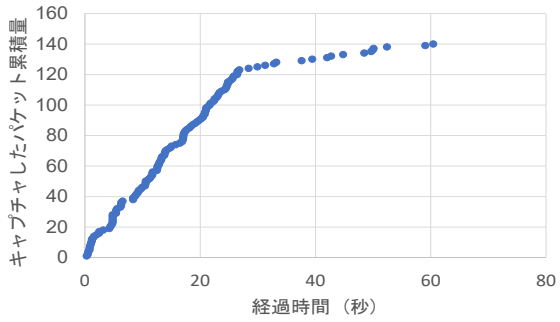

図２．１分間にキャプチャパケット量の変化

2.3. ネットワーク遮断検出：ステップ２

ステップ１のインターネット遮断検出は、WiFiスポットを利用しているクライアントの数や、それらが利用しているサービスの種類などにより、検出精度に揺らぎが生じる可能性がある。そこで、ステップ２として、ステップ1でパケット量の変化が急変した時刻の前後でスニフィングしたパケットの詳細を調べ、遮断検出の精度を上げる。具体的には、”Block Ack Bitmap”の値が全て０になるのに加え、”Missing Frame”というエラーが含まれるパケットの存在有無を確認する。図３は、Wireshark[5]を用いて当該パケットの内容をダンプした一例である。本パケットを検出した場合は、インターネットが遮断したと判断する。

前述したステップ1およびステップ2で共に遮断と判断した場合のみ、最終的にインターネットが遮断されたと判断する。以上が、今回提案するWiFiスポットのインターネット遮断検出法である。

```
Receiver address: 34:3d:c4:6b:91:48 (34:3d:c4:6b:91:
Transmitter address: fc:65:de:ed:4e:30 (fc:65:de:ed:
▾ Compressed BlockAck Response
  ▾ Block Ack Control: 0x0004
      .... .... .... ...0 = BA Ack Policy: Immediate A
      .... .... ...0 010. = BA Type: Compressed BlockA
      .... 0000 000. .... = Reserved: 0x00
      0000 .... .... .... = TID for which a Basic Bloc
  ▾ Block Ack Starting Sequence Control (SSC): 0x1d00
      .... .... .... 0000 = Fragment: 0
      0001 1101 0000 .... = Starting Sequence Number:
  ▾ Block Ack Bitmap: 0000000000000000
      Missing frame: 464
      Missing frame: 465
      Missing frame: 466
```

図 3. インターネット遮断後に観測されるパケットの内容例

3. 評価

Free WiFiスポットを模擬した環境を構築し、提案遮断検出法の評価を行った。キャプチャ途中で、故意にネットワークを遮断し、それを検出できるかを実験した。表１に評価結果を示す。同一条件で10回の試行を行い9回、すなわち90%の精度でネットワーク遮断を検出できた。また、通信量が少ない、すなわち判断するパケット量が少ないとネットワーク遮断の検出が困難になることもわかった。

表１．検証結果

試行	通信量	ステップ１	ステップ２	最終判断
1	52.2MB	OK	OK	OK
2	42.1MB	OK	OK	OK
3	10.9MB	OK	OK	OK
4	20.1MB	OK	OK	OK
5	1.2MB	NG	NA	NG
6	14.1MB	OK	OK	OK
7	21.4MB	OK	OK	OK
8	22.1MB	OK	OK	OK
9	30.3MB	OK	OK	OK
10	20.4MB	OK	OK	OK

4. おわりに

監視対象のFree WiFiスポットのアクセスポイントに接続することなく、さらに不要な検証パケット類をWiFiネットワーク内に送信することなく、当該WiFiスポットがインターネットから遮断されたか否かを判断する手法を提案した。評価実験により、提案手法はインターネットの遮断を高い精度で検出できることが分かった。今後は、WiFiスポット内のトラフィック量が少ない場合でも、インターネット接続遮断が精度良く検出できるように提案手法の改良を重ねていく。

参考文献

[1] T. Miyazaki, K. Anazawa, Y. Maruyama, S. Kobayashi, T. Segawa, P. Li, "Resilient Information Management for Information Sharing in Disaster-Affected Areas Lacking Internet Access," 18th ADHOC-NOW 2019, Luxembourg, Oct. 1-3, 2019, pp. 3-17, Springer LNCS 11803.

[2] 坂野寿和, 小田部悟士, 小向哲郎, “移動式ICTユニット方式の全体概要,” NTT技術ジャーナル, 2015.3, pp. 12-16. https://www.ntt.co.jp/journal/1503/files/jn201503012.pdf (Accessed 26 Dec. 2019)

[3] J. Yeo, M. Youssef, A. Agrawala, “A framework for wireless LAN monitoring and its applications,” Proceedings of the 2004 ACM Workshop on Wireless Security, pp.2-8, 2004.

[4] Marko. P, Ivan. C, Dragan. P, Sinisa. H, “Beacon Technology for real-time informing the traffic network users about the environment,” Faculty of Transport and Traffic Sciences, pp.2-9, 2017.

[5] “Wireshark,” https://www.wireshark.org/ (Accessed 24 May 2019)