# 無線端末による ARP を用いた セグメント内の通信妨害攻撃とその対策

松藤 央[1] 落合 秀也[1] 江崎 浩[1]

**概要**：現代において無線で繋がるデバイスはますます多くなり、社会の各地に浸透している。その一方で、悪意ある第三者からのネットワーク攻撃が問題となっていることもまた事実である。そのような実情を踏まえ、今回は無線端末からのネットワーク攻撃に注目した。その中でも本論文においては ARP プロトコルを用いた攻撃について考える。まず現在までに講じられている ARP 攻撃への対策法を挙げ、それを踏まえて本研究では ARP パケット検出機能を用いた対策法を提案した。具体的には、パケット中の二箇所の送信元 MAC アドレスが等しいかどうかを検査して、それが等しければ通過、等しくなければ破棄する。提案手法をモデリング化したものとして、検出器となるマシンを通信経路の間にブリッジ接続し、そのマシン上で ARP パケットを見てパケット中の二箇所の送信元 MAC アドレスが等しいかを検査する実験を行った。その結果、検出器を接続することで被害者が攻撃を受けず通信を続けられていることが確認できた。また遅延の計測により、検出器をつけることで攻撃前と攻撃後の回線速度がほぼ等しくなったことがわかり、この機能が実用的なものであることが確認できた。

## 1. はじめに

コンピュータ技術が発展し情報化社会と呼ばれるようになって久しい昨今、あらゆるものがデータとして管理され、物理的距離にとらわれず大量の情報を一瞬でやり取りすることが可能になった。そのような現代社会において情報を正しくまた安全にやり取りするということは、コンピュータ上に関わらず実生活においても重要な役割を占めていると言っても過言ではない。しかし、様々な技術の進歩によって、悪意ある第三者からの攻撃もまたより強力なものとなり、我々の安全な生活を脅かしうるものとなっている。このようなサイバー攻撃からどのように身を守り、立ち向かっていくかという問題は、情報社会を生きていく上で我々が考えずにはいられない問題と言える。

そのような実情を踏まえ、今回は無線端末からのネットワーク攻撃に注目した。その中でも本研究においては、ARP プロトコルを用いた攻撃について考える。

そもそも ARP(Address Resolution Protocol) は、宛先の IP アドレスから Ethernet の MAC アドレスを知るためのプロトコルである。セグメント内の通信においては正しい MAC アドレスと IP アドレスが対応付けされていなければ、正常な通信は行えない。しかし、その対応を記録する ARP テーブルの更新に関して、認証や暗号化は一切行われない。そのため別端末の振りをして全く関係ない IP アドレスと MAC アドレスを使って ARP リクエストを送ることが可能となっている。従って別端末からセグメント内の ARP テーブルを改竄できるため、通信の盗聴・妨害が可能であることが知られている。

ARP の脆弱性を利用し通信の傍受を行おうとする攻撃に ARP スプーフィングがある。図 1 に一連の流れを示す。

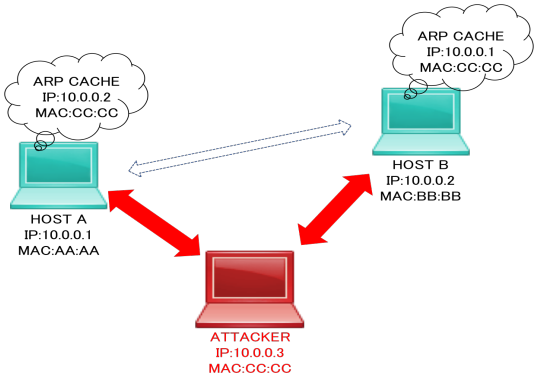


**図 1** ARP スプーフィング

正常な状態では点線のような通信が行われる HostA と HostB に対し、同じセグメントにある攻撃者が攻撃を仕掛ける。まず攻撃者は HostB になりすまし、A の持つ B に関する MAC アドレス情報を攻撃者のものに書き換える。その結果、HostA は本来攻撃者の MAC アドレスであるは

[1] 東京大学大学院情報理工学系研究科

ずの番号を B のものであると認識する。同様に B に対しても攻撃を行い、B の持つ A に関する MAC アドレス情報を攻撃者のものに書き換える。この 2 つの作業により、通信の流れが赤線のように変化し、AB 間の通信がすべて攻撃者を介して行われるようになり、攻撃者による通信の傍受が成立する。

このように ARP スプーフィングによる攻撃は、被害者に攻撃を悟られることなく通信を乗っ取ることのできる強力なものである。さらにこの攻撃はウイルスとして実装し攻撃したいセグメント内のコンピュータに仕込むことが可能であり、重大な被害を生じさせうるものとして問題となっている。

前述の通り、現状の通信には ARP という脆弱性のあるプロトコルが存在する。さらに現状の無線通信の危険性として、多くの Wi-Fi はパスワードがわかれば誰でも (悪意ある者でも) 通信ができてしまうことがあげられる。その上、Wi-Fi を用いた通信を確立する前にその端末が悪意のあるものであると判別するのは難しいという問題もある。そのような実情から、攻撃者が一般の使用者に紛れて Wi-Fi に侵入し、そこから ARP 攻撃を仕掛ける可能性が考えられる。そのため本研究では、無線端末からの ARP 攻撃への対策法の提案と実装を行った。

本論文の構成は次のようになっている。まず第 2 章において、これまで ARP に関する攻撃に関してどのような対策法を講じられてきたのかについて述べる。次に第 3 章において、無線端末からの ARP を用いた通信妨害攻撃への対策についての提案手法を論じる。さらに第 4 章においてその提案手法をモデリングした上で実装し、その実用性を確認する。そして第 5 章で実装における遅延の計測を元に考察を行い、第 6 章でまとめとする。

## 2. 関連研究

ARP スプーフィング攻撃に関して、現在いくつかの対策法が講じられている。その例を以下に示す。

- ARP に暗号化を施し、信頼性のある通信を約束するためのプロトコルである TARP(Ticket-based Address Resolution Protocol)
- ARP テーブルの上書きを検出する Arpwatch
- スイッチそのものに ARP パケットを検査する機能を施した動的 ARP 検査 (DAI)

以下、順にその概略を述べる。

### 2.1 TARP

TARP は、ARP に暗号化を施すことで、信頼性のある通信を行うプロトコルである。これにより通信は安全に行われ、ARP テーブルが攻撃される危険性も大幅に低くなるが、暗号化を行ったことで本来の ARP の機能であるアドレス解決に必要な時間が大幅に伸びてしまい本末転倒ではないかという指摘を受けている。

### 2.2 Arpwatch

ARP テーブルの上書きを検出することのできるツールとして Arpwatch が挙げられる。このツールは特に ARP スプーフィングを受けた際の攻撃検出として用いられる。しかしながらこのツールはあくまで攻撃を検出するためのものであり、攻撃を予防または防御するためのツールではない。すなわち攻撃を検知した時には既に攻撃が完了していたというリスクを避けられないため、本質的な解決策であるとは言えない。

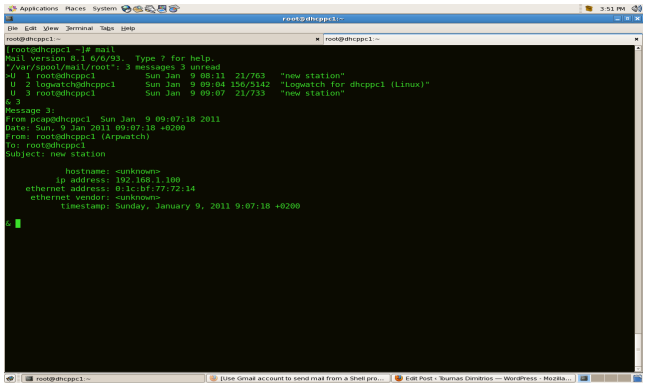

図 2 Arpwatch(図の出典 [3])

### 2.3 動的 ARP 検査 (DAI)

動的 ARP 検査 (Dynamic ARP Inspection) は ARP パケットを検査するセキュリティ機能であり、Cisco 社のスイッチに備わっている。これを用いることで無効な IP アドレスと MAC アドレスで組み合わされた ARP パケットを破棄し、有効な ARP リクエスト及び ARP リプライのみを中継できる。

この機能はスイッチ上の設定であるため、ネットワークホストの機能に手を加える必要がない。また、暗号化によるアプローチとは異なり、ARP 本来の機能のパフォーマンスを低下させることもない。ただし、先に述べたとおりこの機能は Cisco 社のスイッチ独自の機能であり、すべてのネットワークに通用する方法であるとは言えないのが難点である。

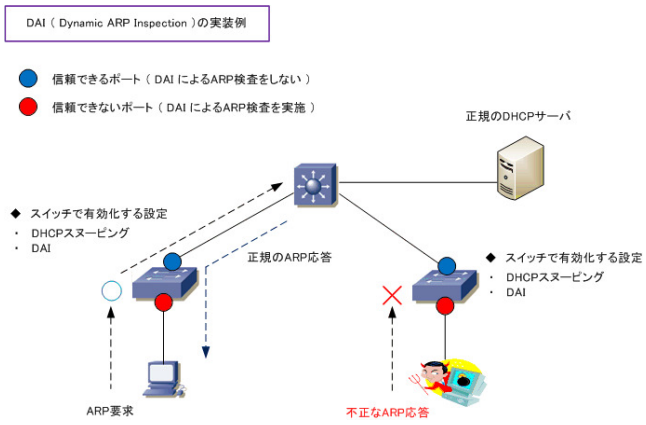


図 3 DAI(図の出典 [4])

### 2.4 ARP スプーフィング対策の現状

以上のように、既存の ARP スプーフィング攻撃への対抗策にはいずれもデメリットが存在し、本質的な解決策は現状開発されているとは言いがたい。更には、ARP はプロトコルそのものに問題があるため、スプーフィングに対する根本的な解決策は存在しないのではないかという見解すらある。ARP 攻撃は、ネットワーク研究の大きな課題の一つであると言える。

## 3. 提案手法

無線からの ARP 攻撃の対策法として、ARP パケット検出機能を用いた対策法を提案する。

ARP リクエストのフォーマットを図 4 に示す。

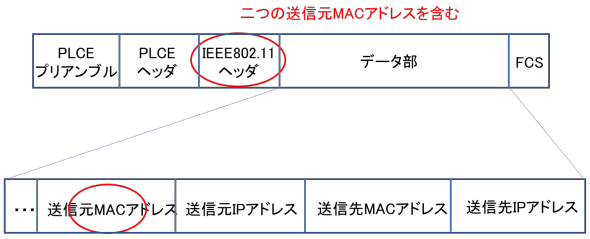


図 4 ARP リクエストのフォーマット

図 4 に示す通り、ARP リクエストには IEEE802.11 ヘッダ部とデータ部とに計二箇所の送信元 MAC アドレスを含んでいる。このうち IEEE802.11 ヘッダ部中のアドレスは無線端末からアクセスポイントへの通信の確立のために使われるアドレスであり、ここを偽装するとアクセスポイントによって不正なパケットであるとみなされ無線からのパケットは届かない。一方データ部中のアドレスはこのパケットを受け取った際にその端末中の ARP テーブルに記録されるアドレスであり、ARP を用いた攻撃の際に不正な値に改ざんされ、かつ改ざんされてもアクセスポイントによるチェックの対象とならないアドレスである。

本研究においては、無線からの ARP 攻撃の対策法として先に挙げた二つのアドレスが等しいかどうかを検査する機能を提案する。正常なパケットであれば本来上記の二つのアドレスは等しいはずであり、それらのアドレスが等しくないものは攻撃用の不正なアドレスとしてエンドノードで破棄すれば、パケット受信側の ARP テーブルは変更されず種々の攻撃を防御することができると考えられる。

## 4. 実験

### 4.1 実験手順

本研究では前述の提案手法をモデリングしたものとして端末に検出器を付属させ、そこでパケットを検査する実験を行った。実験の流れは以下の通りである。

(1) 攻撃を受けることが予想される端末とそれが所属するネットワークとの間に、検知用の別のコンピュータをブリッジ接続する。

(2) 検知用のコンピュータは、流れてくる ARP パケットの中身を見て、IEEE801.11 ヘッダ部の送信元 MAC アドレスとデータ部の送信元 MAC アドレスが等しいかどうかをチェックする。

(3) チェックした両者が等しければそのままそのパケットを通し、等しくなければ攻撃パケットであるとして破棄する。

以上の攻撃を図で表したものが図 5 である。

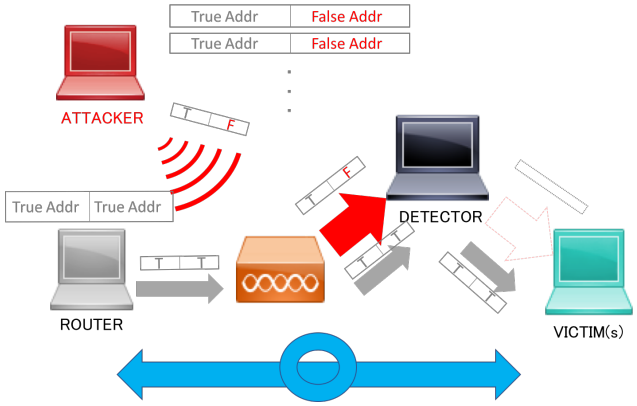


図 5 検出器を用いた ARP パケットの取捨選択

図 5 において、攻撃者からの ARP パケット及びルータからの正しい ARP パケットはともに検出器に入るが、検出器によって「入ってきた ARP パケットの IEEE802.11 ヘッダ部の送信元 MAC アドレスとデータ部の送信元 MAC アドレスが等しいか」というチェックが入る。通常の ARP パケットでは両者のアドレスは等しいはずであり、実際両者が等しいルータからのパケットは通過し、異なる攻撃者からのパケットは破棄される。これにより、攻撃を受けた際も ARP テーブルに間違った MAC アドレスが記録されることなく外部との通信を継続できると考えられる。

### 4.2 実験結果

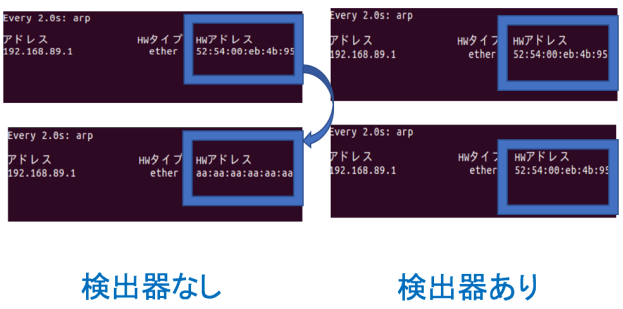


図 6 実験結果

図 6 は検出器を接続しなかった時と接続した時の被害者の ARP テーブルの変化を示したものである。図 6 より、検出器を接続することで被害者が攻撃を受けず通信を続けられていることがわかる (外部への ping も通ることが確認できた)。

## 5. 考察

### 5.1 検出器設置による遅延評価

実験結果より、検出器を用いることで無線からの攻撃を受けている時も通信が行えていることがわかった。ここで攻撃を受けたことによる遅延、さらには検出器そのものを設置したことによる遅延の影響について考える。表 1 は、検出器を設置した場合としなかった場合における ARP 攻撃前後の 8.8.8.8 への ping に要する時間 100 回の平均である。

**表 1** 8.8.8.8 への ping に要する Vc の平均時間 [ms]

| | 検出器なし | 検出器あり |
|---|---|---|
| 攻撃前 | 1.26 | 4.28 |
| 攻撃中 | (通信不可能) | 4.43 |

表 1 から、検出器なしでは攻撃を受けた際に全く通信を行えなかったが、検出器ありの状態では攻撃前と攻撃後の回線速度にはほとんど差がないことが見て取れる。このことから、検出器の設置による防御は成功したと言える。

一方検出器を設置したことにより、検出器なしの時と比べて約 3.4 倍の遅延が発生していることが確認できる。これを改善することは今後の課題のひとつであると言える。

### 5.2 Proxy ARP について

本研究で触れるべき懸念事項として、Proxy ARP(代理 ARP) というプロトコルの存在が挙げられる。Proxy ARP とは他のデバイス宛の ARP リクエストに対し、本来の宛先に代わって ARP リクエストを返す機能であり、ルータなどの L3 デバイスで実装されることがある。これを用いると、攻撃目的でない正しいパケットであるにもかかわらず、パケット中の IEEE802.11 ヘッダ部の送信元 MAC アドレスとデータ部の送信元 MAC アドレスが異なるという現象が起こりうる。本研究では両者の値が一致するか否かで攻撃パケットかそうでないかを判断しているため、Proxy ARP を利用して送られてきた正しいパケットをも破棄してしまうことが考えられる。

しかし、Proxy ARP というプロトコルはサブネットマスクを認識できない端末がある場合に限り必要とされるプロトコルであり、2018 年現在サブネットマスクを認識できない端末を考慮する必要は薄いと考えられる。さらに仮にそのような端末が存在する場合は、その端末に関してのみ例外的に両者のアドレスが異なるパケットを承認するという実装をすることが可能であり、結果として今回の検出機能を設置したことによる影響は薄いと考えられる。

## 6. 終わりに

本論文においては、ARP を用いた無線からの攻撃問題を取り上げた。まず現在までに講じられている ARP 攻撃への対策法を関連研究として挙げた。そしてそれを踏まえて本研究では ARP パケット検出機能を用いた対策法を提案した。具体的には、パケット中の IEEE802.11 ヘッダ部とデータ部の二つの送信元 MAC アドレスが等しいかどうかを検査して、それが等しければ通過、等しくなければ破棄するというものである。

さらに提案手法をモデリング化したものとして、検出器となるマシンを通信経路の間にブリッジ接続し、そのマシン上で ARP パケットを見てパケット中の二箇所の送信元 MAC アドレスが等しいかを検査する実験を行った。その結果、検出器を接続することで被害者が攻撃を受けず通信を続けられていることが確認できた。また遅延の計測により、検出器をつけることで攻撃前と攻撃後の回線速度がほぼ等しくなったことがわかり、この機能が実用的なものであることが確認できた。

今後の課題は、検出器を設置したことによる遅延の改善と、エンドノードに攻撃パケット検出機能を実装することである。

### 参考文献


[1] C. L. Abad and R. I. Bonilla, ”An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks,” Distributed Computing Systems Workshops, 2007. ICDCSW ’07. 27th International Conference on, Toronto, Ont., 2007, pp. 60-60.

[2] Man in the middle - VOER 入手先 ⟨https://voer.edu.vn/m/man-in-the-middle/a674d643⟩ (参照 2018-5-12)

[3] How to: Detect ARP Spoofing with “arp-watch” under Linux — Tournas Dimitrios 入手先 ⟨https://tournasdimitrios1.wordpress.com/2011/01/09/how-to-detect-arp-spoofing-under-unix-or-linux/⟩ (参照 2018-5-12)

[4] DAI(Dynamic ARP Inspection) とは 入手先 ⟨http://www.infraexpert.com/study/dhcpz7.html⟩ (参照 2018-05-12)

[5] Justin Seitz(2015)『サイバーセキュリティプログラミング–Python で学ぶハッカーの思考』(青木一史ほか訳) 株式会社オライリー・ジャパン