家庭内無線LAN環境における不正端末の検知・遮断システムの開発

衛藤 雄平[1]　神屋 郁子[2]　下川 俊彦[2]

概要：近年家庭内無線 LAN が普及してきている．しかし, 家庭内無線 LAN はセキュリティ対策が不十分な場合が多く, 攻撃対象となりやすい．そこで本研究では, 家庭内無線 LAN 環境における不正端末検知・遮断システムを開発した．このシステムは家庭内無線 LAN AP に接続しようとする不正端末を検知し, 遮断するシステムである．本研究では, 不正端末の検知に偽装が困難な Association Request フレームで判断し, 不正端末の遮断にフレームインジェクションを利用し無線 LAN AP と不正端末の接続を遮断する手法を提案する．提案手法を実装し有効性を評価した．

Development of Rogue Device Detection and Blocking System for Home Wireless LAN

Yuhei ETO[1]　Yuko KAMIYA[2]　Toshihiko SHIMOKAWA[2]

Abstract: Home wireless LAN has become popular. However security of home wireless LAN is not enough. Thus it will become an attack target. In this research, we developed rogue device detection and blocking system for home wireless LAN. We proposed detection and blocking method using IEEE802.11 frame. It is difficult to spoof. In addition, our blocking method uses frame injection. It blocks connection between wireless LAN AP and rogue devices. We implemented the proposed method and evaluated the effectiveness.

1. はじめに

近年, 企業, 大学, 一般家庭など様々な場所において無線 LAN が広く使われている．無線 LAN は, 導入コストが低く, 電波の届く範囲であれば場所を選ばずインターネットに接続できるなどの利点を持っている．また, 現在の無線 LAN は, 通信速度の高速化が進んでおり有線のギガビットイーサネットに匹敵するほどの通信速度を持っている．タブレット端末やスマートフォンなどの普及や様々なものがインターネットに接続していく中で, 無線 LAN はなくてはならないものとなっている．

一方で, 無線 LAN には克服すべき問題がいくつかある．そのうちの一つとしてセキュリティにおける問題がある．どのようなネットワークでもセキュリティは重要である．しかし, その中でも無線 LAN のセキュリティは重要視されている．無線 LAN は適切なアンテナと送受信機があれば誰でも利用可能なため攻撃対象となりやすい．企業や大学内の無線 LAN であれば, IT やセキュリティに詳しい人が管理し, 十分なセキュリティ対策が施されている場合が多い．しかし, 家庭内の無線 LAN は IT やセキュリティに詳しい人が管理しているとは限らず, セキュリティ対策が不十分な場合が少なくない．そのため, 企業・大学内の無線 LAN に比べ, 家庭内の無線 LAN は攻撃対象となりやすい．

本研究では, 家庭内環境における無線 LAN のセキュリティの向上及び対策を目的としている．家庭内無線 LAN を対象とした攻撃のうち, 本研究では不正アクセスを扱う．

2. 無線 LAN への不正アクセス

適切なセキュリティ対策が施されていない無線 LAN では, 無断で第三者の端末から接続される恐れがある．これ

[1] 九州産業大学大学院 情報科学研究科
Graduate School of Information Science, Kyushu Sangyo University
[2] 九州産業大学 情報科学部
Faculty of Information Science, Kyushu Sangyo University

を本研究では不正アクセスと呼ぶ. 不正アクセスされることで, インターネットを勝手に利用されたり, 情報機器に侵入されデータの改竄や漏洩に繋がったりする恐れがある.

家庭内無線 LAN で不正アクセス対策をするためには, 無線 LAN AP に備わっているセキュリティ対策機能を用いることがほとんどである. 現在の無線 LAN AP に機能として備わっている主要なセキュリティ対策として, 暗号化, SSID ステルス, ANY 接続拒否, MAC アドレスフィルタリングの 4 つがある. しかし, これらはセキュリティ対策として効果的でない場合が多い. 暗号化は WEP や WPA で暗号化している場合, 暗号解析される恐れがある. SSID ステルスは SSID の通知をしないだけで, 無線 LAN への接続を阻止できない. ANY 接続拒否は端末から無線 LAN AP を自動検出できなくするだけで, 無線 LAN への接続を阻止できない. MAC アドレスフィルタリングは接続許可されている端末の MAC アドレスに偽装することで無線 LAN に接続可能である.

3. 家庭内無線 LAN 不正端末検知・遮断システム

本研究では家庭内無線 LAN 不正端末検知・遮断システム “Rogue Device Sniper” を開発する. 以降 Rogue Device Sniper を RDS と呼ぶ.

本研究では, 各家庭内における無線 LAN AP の管理者および管理者が許可した利用者が持っている端末を正規端末と呼ぶ. それ以外の端末を全て不正端末と呼ぶ. また, 正規端末, 不正端末の両方を合わせて端末と呼ぶ.

3.1 システム概要

RDS は家庭内無線 LAN AP に接続しようとする不正端末を検知し, 遮断するシステムである. 検知手法については 3.3, 遮断手法については 3.4 で説明する.

本システムは, 家庭内無線 LAN AP の既存のセキュリティ対策との併用が可能でセキュリティ強度を向上することができる. そのため WEP や WPA を利用している環境でも, 安心して家庭内無線 LAN AP を利用することができる. システムの利用者はセキュリティに関する知識は必要とせず, Web UI から簡単な設定でシステムを利用することができる.

3.2 システム構成

RDS のシステム構成を図 1 に示す. RDS は端末から家庭内無線 LAN AP 向けて送られる電波を常時監視する. 監視して得られた情報から不正端末を検知する. 不正端末を検知すると, RDS は不正端末と無線 LAN AP との無線 LAN 接続を遮断する.

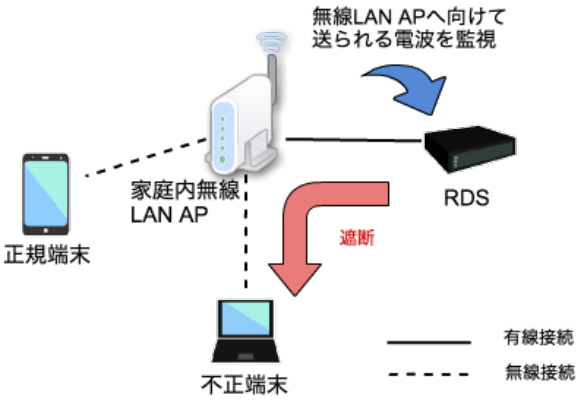

図 1 システム構成
Fig. 1 System architecture

3.3 不正端末検知手法

本研究では IEEE802.11 フレームの Association Request フレームを用いて不正端末を判別する検知手法を提案する.

Association Request フレームを利用した不正端末検知手順は以下の通りである.

(1) あらかじめ正規端末の Association Request フレームを RDS に登録
(2) 端末から家庭内無線 LAN AP に向けて送られる電波を常時監視し, Association Request フレームを取得
(3) 取得した Association Request フレームが正規端末であるか判別
(4) 正規端末と判別されなかった端末を全て不正端末とみなす

3.3.1 Association Request フレーム

Association Request フレームとは, 端末と無線 LAN AP が無線 LAN 接続するためにやりとりを行うフレームの一つである. このフレームでは, 端末側がサポートしている通信規格, チャンネル幅, 電波強度, 暗号化情報, ベンダー情報などの情報が送信される. このフレームで, 端末が持っている無線 LAN アダプタのハードウェア情報を無線 LAN AP に送信する. そのため, 端末ごとに Association Request フレームは異なる場合が多い. 端末の判別に使う情報は, Association Request フレームヘッダの中の BSSID, Source MAC アドレスと Association Request フレームボディ全体である.

Association Request フレームを用いる利点として以下の 2 つがある.

- MAC アドレス偽装に対して有効
- Association Request フレームの偽装が困難

1 つ目の MAC アドレス偽装に対する有効性については, 端末の判別に Association Request フレームを用いるため, MAC アドレス偽装していたとしても不正端末の検知ができる.

2 つ目の Association Request フレームの偽装の困難さ

図 2 無線 LAN AP 選択画面
Fig. 2 Wireless LAN AP choice page

については, Association Request フレームを偽装した場合, 不正端末のハードウェアではサポートされていないものをサポートしていることと偽ることになるため, 不正端末と無線 LAN AP との通信の確立に問題が生じ, 正常な通信を行うことができなくなるのではないかと考える. そのため偽装が困難であると言える.

3.4 不正端末遮断手法

本研究では不正端末の遮断にフレームインジェクションを用いる. IEEE802.11 では無線 LAN AP から端末に向けて Disassociation フレームもしくは Deauthentication フレームを送ることで接続を切断することができる. 本研究ではこの二つのフレームを合わせて遮断フレームと呼ぶ. 不正端末を遮断するためには, 無線 LAN AP から不正端末へ向けて遮断フレームを送信する必要がある. 無線 LAN AP から不正端末へ向けて遮断フレームを送信する命令を, RDS から無線 LAN AP に対して出すことは困難である. そのため, 本研究では無線 LAN AP から不正端末へ向けて遮断フレームを送信した時と同じフレームを RDS から不正端末へ送り, 無線 LAN 接続を遮断させる手法を提案する.

3.5 RDS の機能

RDS の機能について以下に記述する.

3.5.1 無線 LAN AP 選択機能

無線 LAN AP 選択機能は, RDS の保護対象とする家庭内無線 LAN AP を SSID で選択する機能である. RDS 周辺の無線 LAN AP の SSID を取得し一覧表示する. 利用者は一覧の中から RDS の保護対象とする家庭内無線 LAN AP を SSID で選択する. SSID を選択すると同時に, 端末の検知・遮断に必要な AP の BSSID, チャンネルの情報も取得される.

この機能は無線 LAN 選択画面 (図 2) から操作可能である.

3.5.2 チャンネル自動更新機能

チャンネル自動更新機能は, RDS が不正端末の検知・遮断に用いるチャンネルを, 現在選択されている無線 LAN

図 3 正規端末管理画面
Fig. 3 Device management page

AP のチャンネルに自動的に合わせる機能である. 無線 LAN AP はチャンネルを選択することで, 電波の送受信に使用する周波数を決定する. RDS は不正端末の検知・遮断を行うために, 無線 LAN AP と同じチャンネルを監視する必要がある. 一般的に無線 LAN AP のチャンネルは頻繁に変わるものではない. しかし, 無線 LAN AP に備わっている機能でチャンネルの Auto 設定がされている場合, チャンネルが変化することがある. 本機能はそのような場合でも, 自動的に無線 LAN AP のチャンネルを検出し, 監視するチャンネルを自動的に変更する.

3.5.3 検知機能

検知機能は, 家庭内無線 LAN AP に接続しようとする端末の Association Request フレームを取得し, 正規端末か不正端末かを判別する機能である.

3.5.4 遮断機能

遮断機能は, 家庭内無線 LAN AP に接続しようとする不正端末を遮断する機能である. この機能では, 検知機能により判別された不正端末に対し, 遮断フレームを送信する.

3.5.5 正規端末自動登録機能

正規端末自動登録機能は, 家庭内無線 LAN AP に接続する端末全てを正規端末とみなし, システムに端末の Association Request フレームを自動登録する機能である.

この機能を持たせる理由は, 端末の判別に Association Request フレーム利用しているからである. システム利用者による Association Request フレームの取得は困難である. また, 手動で登録するには登録量が多すぎる. そのため自動で Association Request フレームをシステムに登録する機能を持たせた.

登録された正規端末は正規端末管理画面 (図 3) から確認できる. 正規端末管理画面には正規端末の端末名, MAC アドレス, 登録日時の一覧と検知された不正端末の端末名, MAC アドレス, 最終検知日時が表示される. 端末名の初期値はベンダー名が登録される.

3.5.6 モード切替え機能

本システムは遮断モードと登録モードの二つの動作モー

図 4 設定管理画面
Fig. 4 System management page

図 5 メールアドレス管理画面
Fig. 5 Mail address management page

ドを持つ．モード切替え機能は，この二つの動作モードを切替える機能である．遮断モードでは，遮断機能 (3.5.4) が動作する．登録モードでは，正規端末自動登録機能 (3.5.5) が動作する．

システム初回起動時に家庭内無線 LAN 管理者までもが無線 LAN AP に接続できない問題を防ぐため，システム初回起動時や正規端末が一台もシステムに登録されていない場合は，登録モードとなる．

この機能は設定管理画面 (図 4) から操作可能である．

3.5.7 通知機能

通知機能はシステム利用者に不正アクセスがあったことを通知する機能である．この機能を利用するには，あらかじめ通知先のメールアドレスを設定しておく必要がある．不正アクセスがあった日時，不正端末の MAC アドレス，ベンダー名を登録されたメールアドレス宛に送信する．

この機能はメールアドレス管理画面 (図 5) から操作可能である．

4. RDS の実装

RDS の実装について以下に記述する．

4.1 実装環境

実装環境は以下のとおりである．

- Kali Linux
- Raspberry Pi 3 MODEL B
- Java 1.8.0
- Java Servlet 3.1
- JSP 2.3
- MySQL 5.6.30

4.2 検知機能の実装

検知機能の実装する際 Association Request フレームを取得するだけでなく，Reassociation Request フレームも取得するように仕様変更している．Reassociation Request フレームは端末が再接続する際に送信するフレームである．遮断後，端末によっては再接続時に Association Request フレームではなく，Reassociation Request フレームを送信する端末があることがわかったため，このフレームを含めたフレームを取得する．今回の実装では Reassociation Request フレーム取得時に端末判別せず，全て不正端末として扱うように実装した．

4.3 RDS の導入

RDS を導入する際に考慮しなければならない点について述べる．

4.3.1 RDS を導入する計算機

RDS を導入するためには以下の条件を満たす計算機が必要である．

(1) モニターモード可能な無線 LAN インタフェースを持つ
(2) 上記とは別のネットワークインタフェースを持つ

1 つ目のモニターモードとは，無線 LAN 上を流れるパケットを監視する無線 LAN アダプタのモードである．これは端末から送られる電波の監視と不正端末の遮断に必要である．

2 つ目は RDS の設定にネットワーク通信を必要とするためである．この際に用いるネットワークインタフェースは有線・無線どちらでも良い．しかし無線 LAN で接続している場合，RDS が遮断攻撃を受けて RDS の設定ができなくなる恐れがある．そのため，有線 LAN で接続したほうが安全度は高く確実に設定できる．

4.3.2 RDS を設置する位置

RDS は家庭内無線 LAN AP に物理的に近い場所に設置する必要がある．なぜなら，不正端末から無線 LAN AP への電波を RDS にも届かせる必要があるからである．電波が RDS に届かない場合，不正端末を検知できない問題が出てくる．また，不正端末からの電波が届いて検知できたとしても，RDS から不正端末へ送られる遮断フレームが届かず，不正端末を遮断できない問題も出てくる．RDS を家庭内無線 LAN AP に物理的に近い場所に設置することで，これらの問題が起きる可能性を減らす．

5. 不正端末検知・遮断手法の評価

本研究で提案したの検知・遮断手法の評価について述

べる.

5.1 評価内容

本評価では, 提案した不正端末検知・遮断手法がセキュリティ対策として有効であるかを評価する. そのために, 検知・遮断手法を用いたセキュリティ対策システムである RDS の性能評価を行う. RDS が正しく不正端末として判別し, 無線 LAN 接続を遮断できれば, 提案手法はセキュリティ対策として有効であると言える.

評価では, 無線 LAN AP から送られる電波の受信強度が強い場所と受信強度が弱い場所の両方から端末を接続させた場合の, RDS の動作および端末側の無線 LAN AP との接続状態を確認した. 場所を分ける理由は, Association Request フレームを取得しやすい環境と取得しにくい環境で RDS の検知・遮断性能がどれほど変わるかを比べるためである. 電波の受信強度は, RSSI(Received Signal Strength Indicator) によって示され, 無線 LAN 端末で測定できる. RSSI は 0 に近い値ほど受信強度が強い. 本評価では, RSSI の値が-40〜0 の場合は受信強度が強い場所とする. また, RSSI の値が-70 以下の場合は受信強度が弱い場所とする.

正しい検知・遮断ができているかの評価指標に, 偽陰性 (不正端末なのに正規端末と判別), 偽陽性 (正規端末なのに不正端末と判別) の確率を用いる. 確率が低いほど, RDS は安全度が高いセキュリティ対策と言える. また, 偽陰性, 偽陽性がある場合, 検知・遮断のどちらの原因があるかを調査する.

5.2 評価環境

無線 LAN AP に PLANEX MZK-750DHP を用いる. また, 無線 LAN 端末に様々な種類のタブレット, スマートフォン, PC など全 30 台用いる. この 30 台の中には同一仕様の端末も含まれている. 評価に用いた端末を表 1 に示す.

5.3 評価方法

電波受信強度が強い場所と弱い場所の両方から不正端末と正規端末を接続させ, RDS が正常に動作するかを確認する. 不正端末接続時における評価方法について 5.3.1 で説明する. 正規端末接続時における評価方法について 5.3.2 で説明する.

5.3.1 不正端末接続時における性能評価方法

この評価では, 全 30 台の端末を全て不正端末として接続した. これらの端末が無線 LAN AP に接続した場合, 全て正常に遮断されるか確認する. この評価における「正常な遮断」は, 不正端末からの無線 LAN 接続がタイムアウトになるか, 再接続と遮断の繰り返しが 1 分以上続くこととする. この理由は, 遮断フレームを受けた不正端末は一度遮断されるが, またすぐに再接続を試みるためである. RDS は, この接続を再び検知して遮断するという動作を繰り返す. 端末によってこの繰り返しの動作が延々と続くため, 単に不正端末を検知して遮断フレームを送ることは「正常な遮断」とは言えない. 不正端末の接続は 1 台ずつ行い, 電波受信強度が強い場所と弱い場所の両方において, 正常な遮断がされるかの確認を 4 回繰り返す. もし, 一度でも RDS から検知もしくは正常な遮断できずに接続された場合は偽陰性の端末と数える.

表 1 評価に利用した端末
Table 1 Evaluated device

No.	メーカー	機種	モデル	OS
1	Apple	MacBook Pro	13-inch, Early 2011	OS X Yosemite
2	Apple	MacBook Pro	Retina, 15-inch,Mid 2014	OS X EL Capitan
3	Apple	MacBook Pro	Retina, 13-inch, Early 2015	MacOS Sierra
4	Apple	MacBook Air	13-inch, Early 2014	OS X EL Capitan
5	Apple	MacBook Air	11-inch, Mid 2011	OS X Yosemite
6	Apple	MacBook Air	13-inch, Early 2014	OS X Yosemite
7	Apple	iPhone5s	NE339J/A	iOS 10.2
8	Apple	iPhone5	ME043J/A	iOS 9.3.2
9	Apple	iPhone4s	MD261J/A	iOS 9.3.5
10	Apple	iPod Touch	MD057J/A	iOS 6.1.6
11	Apple	iPad3	MD330J/A	iOS 9.3.5
12	Apple	iPadmini	MK6l2J/A	iOS 10.2
13	DELL	Inspiron	15R-5537	Windows8.1
14	DELL	Inspiron	15R-5537	Windows8.1
15	DELL	Inspiron	15R-5537	Windows8.1
16	Fujitsu	LIFEBOOK	S560/B	Windows10
17	Fujitsu	LIFEBOOK	S560/B	Windows10
18	Microsoft	Surface Pro 4		Windows10
19	Acer	Chromebook	CB3-111	Google Chrome OS
20	HTC	Nexus9	T810	Android7.0
21	ASUS	Nexus7	K008	Android5.1.1
22	ASUS	Nexus7	K008	Android6.0.0
23	ASUS	Nexus7	K008	Android6.0.1
24	ASUS	MemoPad 7	ME171C	Android5.0
25	HP	Slate7 Extreme	4405RA	Android6.0
26	HUAWEI	Kardon	M2-802L	Android5.1.1
27	SONY	Xperia Z3	401SO	Android5.0.2
28	LG エレクトロニクス	isai vivid	LGV32	Android6.0
29	SHARP	Disney Mobile	DM015K	Android4.2.2
30	Nintendo	ニンテンドー 3DS	CTR-S-JPN-C0	

5.3.2 正規端末接続時における性能評価方法

この評価では, 全 30 台の端末を全て正規端末として接続した. これらの端末が無線 LAN AP に接続した場合, 全て正常に無線 LAN 接続されるか確認する. この評価における「正常な無線 LAN 接続」は, 正規端末を検知して接続許可することである. 正規端末の接続は 1 台ずつ行い, 電波受信強度が強い場所と弱い場所の両方において, 正常な無線 LAN 接続がされるかの確認を 4 回繰り返す. もし, 一度でも正常な無線 LAN 接続できずに遮断された場合は偽陽性の端末と数える.

5.4 評価結果

まず, 電波受信強度が強い場所においての端末検知・遮断評価結果を表 2 に示す. 電波受信強度が強い場所においての偽陰性の確率は 10.0%, 偽陽性の確率は 6.7%という端末検知・遮断結果が得られた. 次に, 電波受信強度が弱い場所においての端末検知・遮断評価結果を表 3 に示す. 電波受信強度が弱い場所においての偽陰性の確率は 53.3%, 偽陽性の確率は 13.3%という結果が得られた. ここから電波強度が弱くなるにつれて偽陰性・偽陽性の確率も上がることがわかった.

表 2 電波受信強度が強い場所においての端末検知・遮断評価結果
Table 2 Result : strong RSSI

	遮断	接続
不正端末	90.0%	10.0%
正規端末	6.7%	93.3%

表 3 電波受信強度が弱い場所においての端末検知・遮断評価結果
Table 3 Result : weak RSSI

	遮断	接続
不正端末	46.7%	53.3%
正規端末	13.3%	86.7%

表 4 不正端末・正規端末検出率
Table 4 Device detection rate

	受信強度が強い	受信強度が弱い
不正端末	90.0%	53.3%
正規端末	93.3%	56.7%

これらの結果と不正端末・正規端末検出率 (表 4) を比較してみると, 受信強度が強い場所では偽陰性の確率と偽陽性の確率に伴った検出率がでている. しかし, 受信強度が弱い場所では偽陽性の確率が 13.3%に対し, 正規端末の検出率が 56.7%である. これは正規端末の検知時に Association Request フレームを取得できなかったことが原因で正規端末の検出率が下がっていることがわかった.

5.4.1 偽陰性・偽陽性の端末調査

偽陰性・偽陽性と判別された端末について, 検知・遮断のどちらの原因があるかを調査した.

調査結果として, 偽陰性と判別された全ての端末において無線 LAN AP に接続または再接続する際の Association Request フレームを RDS が取得できず取りこぼしていたことが原因であるとわかった. しかし, 取得できていた Association Request フレームに関しては全て端末判別ができており不正端末の検出率は 100%という結果が得られた. これらのことから本研究で提案した検知・遮断手法はセキュリティ対策として有望であることが言える.

次に偽陽性と判別された端末では, Reassociation Request フレームが原因で遮断されていることがわかった. 評価で使用した端末のうち MacBook Pro, MacBook Air の端末は再接続時に Reassociation Request フレームを送信することがわかっている. 今回の実装では, Reassociation Request フレームを取得した場合, 端末判別せず不正端末とみなす方法をとっている. そのため, MacBook Pro, MacBook Air と無線 LAN AP が接続する際に Reassociation Request フレーム送信された時, RDS が正規端末にも関わらず遮断フレームを送信してしまうという結果が得られた.

5.5 考察

5.4.1 より, Association Request フレームが取得できなかったことが原因で, 不正端末を検知・遮断性能に問題が生じることがわかった. しかし, これは提案手法のアルゴリズムではなく, 使用している無線 LAN アダプタ側に問題があると言える. この問題は, RDS で使用する無線 LAN アダプタの電波の送受信性能を上げることで解決できるのではないかと考えている. また, 無線 LAN アダプタの性能をあげることができない場合, 無線 LAN AP が送る電波の出力強度を RDS に合わせて下げることでも問題解決できるのではないかと考える.

また, MacBook Pro, MacBook Air といった Reassociation Request フレームを無線 LAN 再接続時に送信する端末においては, フレーム取得時の動作について考える必要がある. RDS に Association Request フレームだけでなく Reassociation Request フレームの情報も登録しておくことで偽陽性の確率を減らすことができると考える.

今回の評価で行った, 端末 1 台ずつの接続に関して Association Request フレームによる端末の誤判別はない. しかし, 同時に複数台の無線 LAN 端末が接続されることも大いに考えられる. 様々な家庭内環境においての無線 LAN 利用に合わせるためにも, 更なる検証が必要である.

6. 関連研究

関連研究として以下の 2 つの研究を挙げる.

6.1 A new MAC address spoofing detection algorithm using PLCP header

[1] は IEEE802.11 フレームの PLCP ヘッダを利用した MAC アドレス偽装検出アルゴリズムの提案研究である. IEEE802.11 フレームの PLCP ヘッダはフレーム毎に変更される. これは信号強度によって変わってくる. 正規端末と MAC アドレス偽装している不正端末が無線 LAN AP の周りに設置されている場合, 無線 LAN AP から両方の端末に向けて Data フレームを送信する. 端末はその時, 無線 LAN AP に向けて ACK フレームを返信する. この時, 2 つの端末の ACK フレームを監視し, その PLCP ヘッダを比べると高い確率で大きく異なってくる. これにより, MAC アドレス偽装している端末を見つけることができるという研究である. 正規端末と不正端末のそれぞれを近くに監視端末を設置しておくことで, MAC アドレス偽装検出率が 100%である.

本研究との相違点として, MAC アドレス偽装の検出方法である. [1] は, 無線 LAN AP の電波が届く範囲に, 正規端末と MAC アドレス偽装している不正端末の両方が存在する必要がある. しかし RDS では Association Request フレームを利用し端末毎に判別しているため, 正規端末と不正端末が無線 LAN AP の電波が届く範囲に存在しなくても, MAC アドレス偽装を検出できる. また, [1] は MAC アドレス偽装した不正端末の検知することしかできない. しかし RDS は不正端末を検知後, 遮断までの動作をするため不正アクセスがあったとしても対処できる.

6.2 家庭内無線 LAN における「無線 LAN ただ乗りおよび不正アクセスポイント」対策システムの開発

家庭内無線 LAN におけるただ乗り対策システム “DefRer”[2] は, 家庭内無線 LAN AP に接続している不正端末を検知し, ネットワーク通信を遮断するシステムである. 家庭内無線 LAN AP と同一セグメント上に DefRer を配置しておくだけでシステムの利用が可能である.

本研究との相違点として, 一つ目は不正端末検知手法である. DefRer では無線 LAN AP に接続している不正端末を監視し, MAC アドレスを用いた不正端末検知をしている. この検知手法は MAC アドレスを用いているため MAC アドレス偽装に対応できない. RDS は無線 LAN AP に接続しようとする不正端末を監視し, Association Request フレームを用いた不正端末検知をしている. この検知手法は偽装が難しい Association Request フレームを用いているため MAC アドレス偽装されたとしても対応できる.

二つ目は, 不正端末遮断手法である. DefRer では不正端末の通信を DefRer に誘導し, パケットフィルタリングを用いることで, ネットワーク通信を遮断する. しかし, これは無線 LAN AP に接続している状態が続くということである. RDS では, 不正端末に対して, 無線 LAN AP とのアソシエーション自体を遮断させる方法をとっている. そのため, 家庭内のネットワークに接続される恐れがない.

7. おわりに

7.1 まとめ

本研究では攻撃対象となりやすい家庭内無線 LAN におけるセキュリティ対策として, 家庭内無線 LAN 不正端末検知・遮断システム “Rogue Device Sniper”(RDS) を開発した. RDS は家庭内無線 LAN AP に接続しようとする不正端末を検知し, 遮断するシステムである. 不正端末の検知に, 偽装が困難な Association Request フレームを用いた. また, 不正端末の遮断にフレームインジェクションを利用し無線 LAN AP と不正端末の接続を遮断する.

RDS は, 家庭内無線 LAN AP の既存のセキュリティ対策との併用が可能でセキュリティ強度を向上することができる. そのため WEP や WPA を利用している環境でも, 安心して家庭内無線 LAN AP を利用することができる. システムの利用者はセキュリティに関する知識は必要とせず, 簡単な設定でシステムを利用することができる.

評価では Association Request フレームを用いた端末検知・遮断が有効であるかの評価をした. その結果, 受信強度が強い場所において 90%の確立で不正端末の検知・遮断が可能であることがわかった. しかし 10%の確立で Association Request フレームを取得できず不正端末に接続されることがわかった. Association Request フレームを取得できた場合においての端末判別の誤りはなく, 不正端末の検出率は 100%であった. そのため提案した検知・遮断手法はセキュリティ対策として有望であると言える.

7.2 今後の課題

今後の課題は, まず AssociationRequest フレームの取りこぼし問題の改善である. RDS は Association Request フレームを取得できなければ, 不正端末に接続されてしまう. 単純に電波の受信性能の問題であれば, RDS の無線 LAN アダプタの性能を上げることで対処できる. しかし, 電波干渉により電波が衰退し検出できなかったり, 取得される Association Request フレームに誤りがあったりすることも考えられる. 各家庭によって様々な環境が考えられるため, 更なる状況下においての技術検証が必要である.

次に Reassociation Request フレームが送信された場合の RDS の動作である. 今回の実装では, Reassociation Request フレームが送信された場合全て不正端末として判別した. しかし, これでは偽陽性の確率が上がる恐れがあることがわかった. Reassociation Request フレームが送られた際の動作について今後考えていく必要がある.

最後に RDS の設定方法の改善である. RDS を利用するために Web ブラウザから RDS の設定をする必要がある. 現在の設定方法は PC から設定する際においてスムーズに設定可能だが, スマートフォンやタブレットから設定する場合にボタンが小さく押しづらい. そのためスマートフォンやタブレットからもスムーズに設定可能な Web デザインに改善する必要がある. また, ユーザビリティの評価をして, 利用者に使い易いシステムにしていく必要がある.

参考文献

[1] Prawit Chumchu, Tanatat Saelim, Chunyamon Sriklauy, “A new MAC address spoofing detection algorithm using PLCP header”, IEEE Xplore, (January 2011).
[2] 桧室和馬, 神屋郁子, 下川俊彦, “家庭内無線 LAN における「無線 LAN ただ乗りおよび不正アクセスポイント」対策システムの開発”, 情報処理学会 第 78 回全国大会講演論文集, 3-599 - 3-560, (Mar. 2016).