L-021

不正 RA 対策のための IPv6 拡張ヘッダオプションの提案
IPv6 extension header option in defiance of rogue Router Advertisement

佐藤　尚也 †　　**今泉　貴史** ‡†
Naoya Sato　　Takashi Imaizumi

1. はじめに

IPv6 で新たに追加された機能の 1 つに近隣探索がある。近隣探索は同一リンク内の通信に必要な情報を提供し、アドレス解決や到達不能性検出などの機能を持つ。近隣探索メッセージの 1 つである RA(Router Advertisement) は、ルータがネットワーク情報を近隣ノードに通知する際に使用される。

現在、RA を悪用した攻撃である不正 RA が問題となっている。不正 RA とは、ルータを偽ったノードが RA を送信して不正な設定を強要する攻撃である。不正 RA は、中間者攻撃や DoS 攻撃などに使用されており、近い将来に主流となる IPv6 にとっては無視できない問題である。しかし、不正 RA の対策技術は問題を抱えておりセキュリティが万全ではない。現状の対策技術では近隣探索を安全に運用できないため、早急に問題を解決する必要がある。

そこで本研究では、通信経路上の L2 スイッチで不正 RA のフィルタリングを行う RA Guard の強化のために、RA の存在を通知する RA オプションを提案する。RA オプションの使用により、RA Guard のフィルタリング回避問題を解決する。

2. 不正 RA

2.1.IPv6 ステートレスアドレス自動設定

IPv6 は、DHCP サーバを使用せずにアドレスを設定するステートレスアドレス自動設定の機能を持つ。予めルータのみ設定することでホストが特別な設定をせずに通信することが可能となる。ステートレスアドレス自動設定はアドレスの管理者を必要としないため、アドレス数の多い IPv6 とは相性が良い。ルータからホストへ情報を送信する際に RA を用いる。ステートレスアドレス自動設定の手順を図 1 に示す。

2.2. 不正 RA を利用した攻撃

RA にはネットワークプレフィックス、ゲートウェイアドレスなどのネットワーク外部との通信に必要な情報が含まれているため、不正 RA をホストが受信し処理すると通信に大きな混乱が発生する。

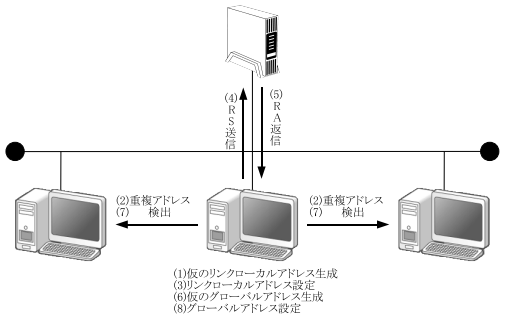

図 1: IPv6 ステートレスアドレス自動設定

2.2.1. 中間者攻撃

中間者攻撃とは、通信経路の途中でパケットを中継して誰にも気付かれずにメッセージを見る盗聴の方法である。不正 RA を利用した中間者攻撃を図 2 に示す。

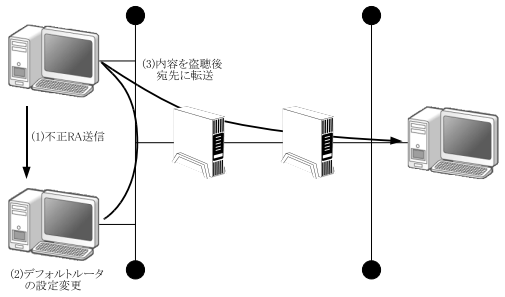

図 2: 不正 RA を使用した中間者攻撃

同一リンク内のノードが不正 RA を送信すると、受信したホストは攻撃者をデフォルトルータとして設定する。すると、ホストが外部のネットワークと通信する際には必ず攻撃者へパケットを送信してしまうため、攻撃者はパケットの内容を確認することが可能となる。

2.2.2.RA DoS

DoS 攻撃 (Denial of Service attack) とは、サービス提供を妨害する攻撃である。RA DoS では、攻撃者はホストに不正 RA を大量に送信する。ホストは RA を受信後に各設定を変更するため、不正 RA によって不正な設定を強要されると通信障害が発生する。また、ホストは大量の不正 RA の処理を行うため、リソースが占有されて応答不能となる。

†千葉大学融合科学研究科
‡千葉大学総合メディア基盤センター

2.3. 不正 RA の対策技術

不正 RA の対策技術は、RA の受信後にホストが検査する方法と通信経路上で検査する方法がある。受信後に処理する対策の例として SEND、通信経路上で処理する対策の例として RA Guard について説明する。

2.3.1.SEND

SEND(SEcure Neighbor Discovery) は、近隣探索を安全に使用するためのプロトコルである。SEND は近隣ノードの認証、近隣探索メッセージの改竄防止、リプレイ攻撃の防止などの機能を持つ。

不正 RA の対策には、承認委譲探索 (Authorization Delegation Discovery) を用いる。ホストとルータの間で予め信用点を登録しておき、ルータは信用点から証明書を発行してもらっておく必要がある。ホストが証明書パス要請を送信すると、ルータは証明書パス広告を返信する。証明書パス広告を受信したホストは、証明書を確認して信用点に登録されているルータであるか確かめることでノードの偽装を見抜くことが可能となる。

2.3.2.RA Guard

RA Guard とは、通信経路上の L2 スイッチで不正 RA をフィルタリングする機能である。RA Guard の構成を図 3 に示す。

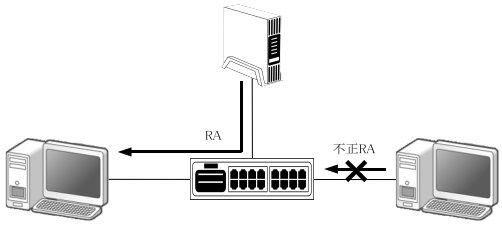

図 3: RA Guard

RA Guard は、受信した RA をメッセージの内容または L2 装置の構成に基づいた情報のみで通過させるかブロックするかを決定する。よく使用される情報は、送信元 MAC アドレス、送信元 IP アドレス、受信ポートである。前もって割り当てたルータに対してこれらの情報を当てはめると RA の送信元の判別を行えるため、不正 RA の対策が可能となる。

2.4. 対策技術の問題点

2.4.1.SEND

SEND は、証明書パスから RA の送信元を判別する対策であるが、事前にホスト・ルータ間で信用点を決めておいたり証明書を発行してもらうなどの複雑な設定が必要となるため、あまり普及していない。また、SEND は送受信者が相互にサポートしていないとメッセージの処理が行えない。すなわち、同一リンク上の全ノードが SEND をサポートしていない場合、効果を完全には発揮することができない。さらに、受け取った RA に対してノードは証明書パスを送受信して確認する必要があるため、負荷を増加させることが目的である RA DoS の対策としては不適切である。

2.4.2.RA Guard

RA Guard は、L2 スイッチで不正 RA のフィルタリングを行う対策であるが、IPv6 拡張ヘッダの仕様からフィルタリングを回避可能な方法が存在する。RA Guard のフィルタリング回避方法を図 4 に示す。

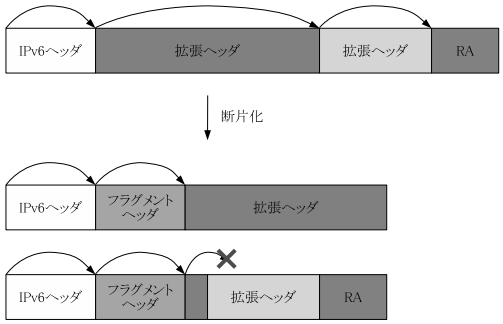

図 4: RA Guard のフィルタリング回避方法

IPv6 はヘッダの軽量化のため、いくつかの機能を拡張ヘッダで表現している。IPv6 拡張ヘッダは、直後のヘッダを識別する次ヘッダフィールドを持ち、このヘッダチェーンによって数珠繋ぎ状の構造をとる。IPv6 は断片化時にフラグメントヘッダより後の拡張ヘッダ及び上位層のデータをまとめて分割する。よって複数のパケットに分割する場合、拡張ヘッダの途中で分割される可能性がある。図 4 のような場合、ヘッダチェーンから RA の有無が確認できないため、RA Guard は不正 RA と認識できずに通過を許可してしまう。

現在、v6ops(IPv6 Operations Working Group) が回避対策として挙げている規則を以下に示す。

1. 送信元アドレスがリンクローカルアドレスでないなら通過
2. ホップリミットが 255 でないなら通過
3. 拡張ヘッダの最大数を制限
4. RA の有無を確認できなければ破棄 (非断片化またはフラグメントオフセットが 0 の時のみ)
5. RA と特定されたなら破棄
6. 他の全てのケースでは通過

規則 4 は、RA の有無が確認できない通常のパケットも破棄してしまうため有効とは言えない。他の規則は制限が緩いため、回避を軽減する程度の対策しか行えない。

3. 提案手法

3.1. 提案手法の概要

SEND は近隣の全ノードに複雑な設定を必要とし、また RA DoS の対策としては不適切であることから、複雑な設定をせずに不正 RA のフィルタリングする RA Guard の方が対策として現実的だと言える。

しかし、RA Guard は断片化による回避が可能である。そこで、IPv6 拡張ヘッダに新たなオプションである RA オプションを追加して RA Guard のフィルタリング回避を防止する方法を提案する。RA オプションは、RA の存在を知らせるためのオプションである。図 5 に提案手法の概要を示す。

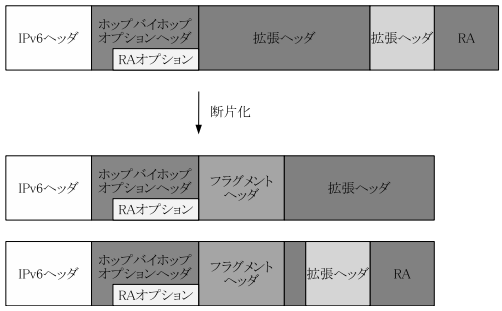

図 5: 提案手法の概要

拡張ヘッダには、処理の手順の関係から推奨される順番が存在する。IPv6 拡張ヘッダの推奨順を図 6 に示す。

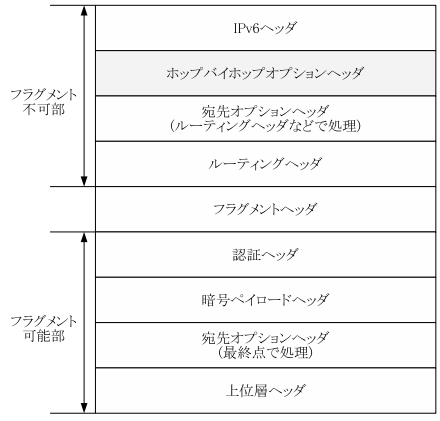

図 6: IPv6 拡張ヘッダの推奨順

フラグメントヘッダより前のヘッダは通信経路上で処理するためフラグメント不可部に属し、後のヘッダは宛先で処理するためフラグメント可能部に属している。RA の存在情報がフラグメント不可部に配置されていないと RA Guard は RA を発見できない。

そこで、RA オプションをフラグメント不可部に属するホップバイホップオプションヘッダ内のオプションフィールドの先頭に付加することで、RA の存在情報をフラグメント不可部に配置する。よってヘッダチェーンから RA の存在を知ることができるため、フィルタリング回避を防ぐことが可能となる。

3.2. 構成

提案する RA オプションの形式を図 7 に示す。

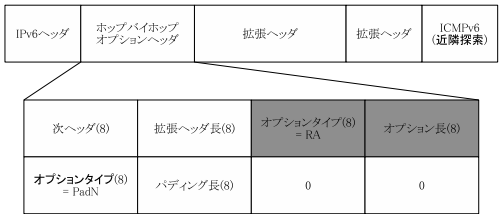

図 7: 提案する RA オプションの形式

各フィールドの内容は以下の通りである。

- オプションタイプフィールド
  オプションの種類を識別するための 8 ビット符号無し整数。RA オプションであることを表す数値を格納する。
- オプション長フィールド
  オプションのデータフィールドの長さを示す 8 ビット符号無し整数。データは必要ないため 0 が入る。

RA オプションは、RA 送信時に必ずホップバイホップオプションヘッダの先頭に配置しなければならない。L2 スイッチは、RA オプションを発見したら転送か破棄かを判別する。RA を受信したノードはホップバイホップオプションヘッダの先頭に RA オプションが無いならば破棄する。

3.3. 実際の使用例

例としてステートレスアドレス自動設定を挙げる。

1. リンクローカルアドレス生成
   ホストは、リンクローカルアドレス用のプレフィックス (FE80::/10) と MAC アドレスもしくは乱数を用いたインタフェース ID を合わせて仮のリンクローカルアドレスを生成する。その後ホストは重複アドレス検出を行い、返信が無ければ正式にリンクローカルアドレスとして設定する。
2. RS(Router Solicitation) 送信
   ホストは RS を用いてルータへネットワークプレ

フィックスを問い合わせる。このときホストはルータのアドレスを知らないため、RS はマルチキャストで送信される。

3. RA 返信
   RS を受信したルータは直ちにプレフィックス情報を格納した RA を RA オプションを付加して返信する。基本的にルータは、全ノードにマルチキャストで RA を送信する。

4. L2 スイッチのオプションチェック
   通信経路上の L2 スイッチは、通過する全パケットの IPv6 ヘッダの次ヘッダフィールドを読み取る。次ヘッダがホップバイホップオプションヘッダでない場合はパケットの通過を許可する。ホップバイホップオプションヘッダが存在する場合は、オプションフィールドの先頭に RA オプションが存在するか確認する。L2 スイッチは RA が含まれることを発見したならば、接続ポート、送信元 IP アドレス、送信元 MAC アドレスから送信元を確認し、ルータに偽装したノードであるならパケットを破棄する。L2 スイッチは、正規のルータによる RA と判断したならば宛先アドレスまで転送する。

5. ホストのオプションチェック
   ホストは、ホップバイホップオプションヘッダ内のオプションフィールドの先頭に RA オプションがあるか確認する。RA オプションを発見したら、正規のルータから受信した RA として処理する。それ以外の RA は不正 RA と判断して破棄する。

6. グローバルアドレス生成
   ホストは、RA に含まれるネットワークプレフィックスとインタフェース ID を合わせて仮のグローバルアドレスを生成する。その後ホストは重複アドレス検出を行い、返信が無ければ正式にグローバルアドレスとして設定する。

プレフィックス情報と送信元 MAC アドレスを付加した RA を使用するとパケットサイズが 96 バイトとなるが、提案手法を用いるとパケットサイズは 104 バイトとなる。パケットサイズが大きく変化しないことから、通信処理の影響は少ない。

表 1 に、対策手法である SEND、RA Guard 及び提案手法の処理の比較を示す。

4. 考察

4.1. v6ops が挙げる対策

送信元アドレスがリンクローカルアドレスでないなら通過させる場合、ルータはグローバルアドレスを用いる必要がある。しかし、攻撃者も同様にグローバルアドレスを使用して不正 RA を送信するとこの規則では防ぐことができない。

ホップリミットが 255 でないなら通過させる場合、ネットワーク外部からの不正 RA を抑制することができる。しかし、RA は同一リンク内で送信されるため、複数のルータを経由する必要が無い。よって、完全な破棄は行えない。

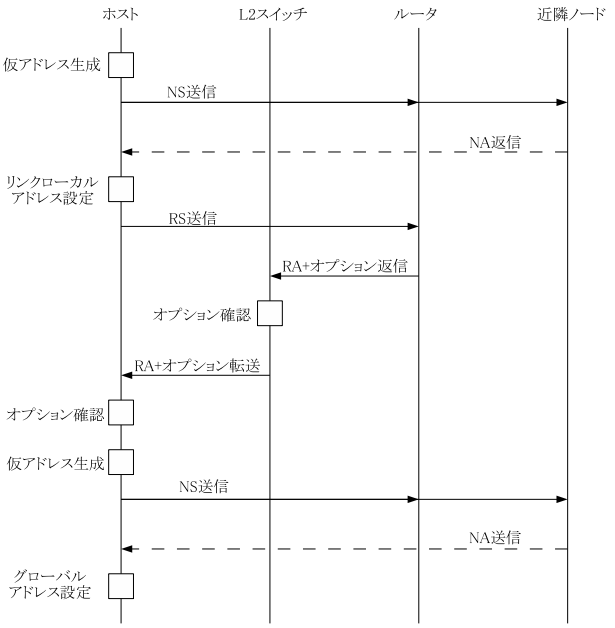

図 8: 提案手法を用いたステートレスアドレス自動設定

拡張ヘッダの最大数を制限する場合、使用する拡張ヘッダを減らして ICMPv6 を発見できるようにする。しかし、ヘッダチェーンの解析途中で制限数に達したら破棄するため、正常の非 RA パケットまで破棄する恐れがある。また、フラグメントヘッダ以外の拡張ヘッダは可変長であるため、使用する拡張ヘッダの数を減らしてもデータサイズが大きくなって断片化が必要となる場合がある。したがって、現状の IPv6 の仕様では、拡張ヘッダの使用数に制限を加えても RA Guard のフィルタリング回避は可能である。

RA の有無を確認できなければ破棄する場合、確認できない時点で疑わしいパケットと判断して破棄する。しかし、拡張ヘッダ使用数の多い非 RA パケットなども破棄してしまうため、現状では問題がある。

フラグメントヘッダの使用を禁止すると、次ヘッダフィールドとヘッダ長から ICMPv6 を発見できる。ただし、この方法では攻撃者が意図的にフラグメントヘッダを使用した場合、RA Guard は ICMPv6 を発見できないので不正 RA を通過させてしまう。よって、ホストは受信した全ての RA に対してフラグメントヘッダの有無を確認し、フラグメントヘッダがあるならば処理を行わず破棄しなければならないため負荷がかかる。

4.2. 近隣探索を拡張ヘッダで表現する方法

近隣探索のメッセージをフラグメント不可部に属する新しい拡張ヘッダで表現すると、フラグメントヘッダの有無にかかわらず RA を発見できる。よって、L2

表 1: SEND、RA Guard、提案手法の比較

	SEND	RA Guard	提案手法
処理方法	証明書で判別	L2 スイッチでフィルタリング	
処理するノード	ホスト & ルータ	L2 スイッチ	ホスト & L2 スイッチ
必要なもの	信用点	対応した L2 スイッチ	
設定	全ホスト & ルータ	L2 スイッチ	全ホスト & L2 スイッチ
不正 RA の対策	問題なし	脆弱性あり	問題なし
処理効率	証明書の通信が必要	問題なし	ホストはオプション確認必要
パケット長	変化なし		各パケット 8 バイト増加

表 2: RA Guard によるフィルタリング方法の比較

	処理ノード	フィルタリング	問題点
v6ops	L2 スイッチ	ICMPv6	回避可能及び偽陽性あり
拡張ヘッダで表現	L2 スイッチ	拡張ヘッダ	既存実装への影響が大きい
提案手法	L2 スイッチ & ホスト	オプション	RA DoS の対策必要

スイッチによる判別が可能なため、不正 RA のフィルタリングが可能である。

しかし IETF (Internet Engineering Task Force) は、拡張ヘッダに新しい機能を追加する場合に宛先オプションヘッダにあるオプションフィールドの使用を推奨している。これは、新しい拡張ヘッダの追加は既存実装への影響が大きいためである。既存の拡張ヘッダの順番には不確定な部分が多く、なるべく拡張ヘッダの増加は避けるべきである。よって新しい拡張ヘッダ定義の追加は推奨されておらず、既存の拡張ヘッダの枠組み内で新規機能の追加が勧められている。

4.2.1. 提案手法

ホップバイホップオプションヘッダは、拡張ヘッダの中で先頭に配置するため定位置となる。また、RA オプションはホップバイホップオプションヘッダにあるオプションフィールドの先頭に配置する制約を設けるため、ヘッダ内に複数のオプションを格納する場合でも RA オプションの配置は定位置となる。したがって、RA Guard による検査場所が定位置となるため、L2 スイッチの処理速度の向上が期待できる。

しかし、攻撃者が意図的に RA オプションを使用せず不正 RA を送信した場合、RA Guard はホップバイホップオプションヘッダのみ確認するので不正 RA を見逃してしまう。すると、ホストは受信した全ての RA に対して RA オプションの有無を確認し、RA オプションが無いならば処理を行わず破棄する必要がある。L2 スイッチのみで不正 RA の完全な破棄ができずにホストへ到達してしまうことから、大量の不正 RA による RA DoS に対して変わらず脆弱性を持つ。

5. おわりに

5.1. まとめ

本論文では、IPv6 の機能の 1 つである近隣探索を悪用した不正 RA による攻撃を防ぐために、既存の対策技術である RA Guard の欠点を補う方法として IPv6 拡張ヘッダの RA オプションを提案した。

RA オプションは RA の存在を通知し、フラグメント不可部に属するホップバイホップオプションヘッダのオプションフィールドの先頭に格納される。L2 スイッチとホストで RA オプションをチェックして RA Guard の欠点であった断片化によるフィルタリングの回避を防ぐことができる。

5.2. 今後の課題

本研究はまだ理論段階であるため、実装による評価が行えていない。実際の通信や処理の効率から、ホストと L2 スイッチの負荷の耐性について正確な評価を検討する必要がある。

提案手法では新たにホストがオプションのチェックを行う必要がある。L2 スイッチは RA オプションの有無しか確認しないため、攻撃者が意図的に RA オプションを使用せずに不正 RA を送信した場合、全てをホストが破棄しなくてはならない。場合によっては L2 スイッチの負荷軽減のためにホストと負荷を分散するなどの対策が必要になる。

また、提案手法によって RA Guard のフィルタリング回避問題を解決できるが、L2 スイッチのみで処理するという利点が失われるため、RA DoS の対策についても考慮する必要がある。

参考文献

[1] A. Conta, S. Deering, M. Gupta, Ed.
Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.

[2] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi.
IPv6 Router Advertisement Guard.

[3] F. Gont.
IPv6 Router Advertisement Guard (RA-Guard) Evasion.

[4] F. Gont.
Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard).

[5] J. Arkko, Ed, J. Kempf, B. Zill, P. Nikander.
SEcure Neighbor Discovery(SEND).

[6] P. Nikander, Ed., J. Kempf, E. Nordmark.
IPv6 Neighbor Discovery (ND) Trust Models and Threats.

[7] S. Deering, R. Hinden.
Internet Protocol, Version 6 (IPv6) Specifjcation.

[8] S. Krishnan, j h. woodyatt, E. Kline, J. Hoagland, M. Bhatia.
An uniform format for IPv6 extension headers.

[9] Mark A. Miller.
IPv6 入門. 株式会社翔泳社, 1999.

[10] 独立行政法人情報処理推進機構.
情報セキュリティ技術動向調査（2009 年下期）, 2009.

[11] T. Narten, E. Nordmark, W. Simpson, H. Soliman.
Neighbor Discovery for IP version 6 (IPv6).