Vol.2019-GN-106 No.36
Vol.2019-CDS-24 No.36
Vol.2019-DCC-21 No.36
2019/1/25

# 無線 LAN 中継機のグループ鍵更新問題に関する解決手法の提案

濱本望絵[†1†2]　土屋薫子[†1]　石川博一[†1]　村上隆史[†1]
杉村博[†2]　森信一郎[†2]　一色正男[†2]

**概要**：無線対応端末がルータや中継機に無線接続する際，暗号化・復号化に必要な鍵を 2 つ取得する．1 つはユニキャスト通信する際に使用する PTK(Pairwise Transient Key)，もう 1 つはブロードキャストおよびマルチキャスト通信する際に使用する GTK(Group Temporal Key)である．家庭用ルータ・中継機の中には，一定時間ごとに GTK を更新し，1 つの GTK を長い期間共有しないことで通信の安全性を高める設定が可能なものもある．しかし，中継機の GTK 更新の実装仕様により，無線 LAN ネットワーク上の端末間で GTK の不一致が発生する場合がある．その結果古い GTK を持つ端末と，新しい GTK を持つ端末との間でブロードキャストやマルチキャスト通信が不能になり，相互接続ができない問題が発生する．本論文では，中継機の GTK 更新に関する実装状況を調査し，その問題が発生する条件を明らかにする．またその問題に対して，端末側の実装で相互接続性を確保するための手法の提案を行うと共に提案手法の評価と考察を述べる．

**キーワード**：無線 LAN，暗号，グループ鍵，GTK，マルチキャスト，ブロードキャスト，中継機

# Proposal of a solution method on the problem for updating group temporal key of wireless range extender

MOE HAMAMOTO[†1†2]　KAORUKO TSUCHIYA[†1]　HIROKAZU ISHIKAWA[†1]
TAKASHI MURAKAMI[†1]　HIROSHI SUGIMURA[†2]　SHINICHIRO MORI[†2]
MASAO ISSHIKI[†2]

***Abstract***:
When a wireless terminal connects to a router or wireless range extender, the terminal obtains two keys necessary for encryption or decryption. One is PTK (Pairwise Transient Key) used for unicast communication, and the other is GTK (Group Temporal Key) used for broadcast and multicast communication. Some home routers and wireless range extenders can update the GTK at regular time intervals and set up to enhance communication safety by not sharing one GTK for a long period. However, due to the implementation specification of GTK update of the wireless range extender, GTK inconsistency occurs between the terminals on the wireless LAN network. As a result, broadcast or multicast communication between the terminal having the old GTK and the terminal having the new GTK becomes impossible, and there arises a problem that interconnection is impossible. In this paper, we investigate the characteristics related to updating GTK of wireless range extenders that hamper the interconnectivity of the devices and clarify the problem. In addition, we propose a method to improve interconnectivity in the implementation on the device side against the problem of wireless range extender. Furthermore, evaluation and consideration of the proposed method are described.

***Keywords***: Wireless LAN, encryption, group temporal key, GTK, multicast, broadcast, wireless range extender

## 1. はじめに

近年 IoT の急速な普及を背景に，家庭では各端末の接続は無線が主流となってきたが，例えばリビングに設置された家庭用無線ルータ（以降ルータと呼ぶ）の電波が弱い場所や届かない場所も少なからずあり，家中どこにいても端末からインターネットにアクセスしたいというユーザの要望を満たせないケースもある．こういった問題を解決するため無線 LAN 中継機（以降中継機と呼ぶ）を導入する家庭が増加してきている．ここで，ルータや中継機は通常 Wi-Fi Alliance の WPA(Wi-Fi Protected Access)および WPA2 の認証プログラムを取得している[1]．WPA2 は IEEE802.11i[2]で規格化された無線 LAN セキュリティ仕様であり，無線ネットワーク上の通信においては TKIP(Temporal Key Integrity Protocol)や AES(Advanced Encryption Standard)で暗号化される．

図 1 に示すように家庭内のネットワークに中継機を設置した場合，ルータ配下のネットワークと中継機配下のネットワークに切り分けられる．各端末は，それぞれが接続するルータ・中継機から配布される暗号鍵を用いて通信の暗号化／復号化を行う．ルータと中継機間の通信においてはルータが配布する鍵を使用して通信を行う．端末がルータや中継機に無線接続する際，ユニキャスト通信する際に

†1 パナソニック株式会社
Panasonic Corporation, Kadoma, Osaka 570-8501, Japan
†2 神奈川工科大学
Kanagawa Institute of Technology, Atsugi, Kanagawa 243-0292,Japan

Vol.2019-GN-106 No.36
Vol.2019-CDS-24 No.36
Vol.2019-DCC-21 No.36
2019/1/25

使用する PTK(Pairwise Transient Key)と，ブロードキャストおよびマルチキャスト通信する際に使用する GTK(Group Temporal Key)の 2 つの鍵を取得する．

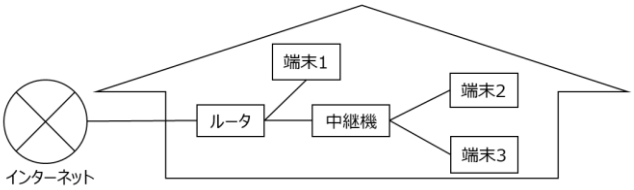


図 1　無線 LAN ネットワークの例
Figure 1　Example of wireless network.

ルータ・中継機の中には，一定時間ごとに GTK を更新し通信の安全性を高める設定が可能なものもある．しかし，GTK 更新における中継機の実装仕様により，無線 LAN ネットワーク上で古い GTK を持つ端末と，新しい GTK を持つ端末が混在する状況が発生するケースがあり，その場合ブロードキャストやマルチキャスト通信が不能になり，相互接続ができない問題が発生する．本論文では，中継機の GTK 更新に関する実装状況を調査し，相互接続性を確保するための手法の提案を行うと共に提案手法の評価と考察を述べる．

## 2. 無線中継の仕組みと GTK 更新の課題

本章ではまず, WPA2(IEEE802.11i)の無線接続および鍵交換シーケンスの概要と中継機による無線中継の仕組みを説明し，中継機の GTK 更新に関する実装仕様により発生する課題を示す．

### 2.1 無線接続および鍵交換シーケンスの概要

端末がルータや中継機に無線接続する際，端末は Probe Request 送信によりルータ・中継機を検索し，ルータ・中継機からの Probe Response により暗号化情報を得る．続いて 802.11 オープン認証(Authentication)を行い，Association Request/Response によりアソシエーションが成功し，無線接続が完了する（図 2 の①）．ルータ・中継機の暗号化が設定されている場合，4-way handshake と呼ばれる鍵交換シーケンスを行い，この間に PTK が計算され，ルータ・中継機が GTK を生成して端末に渡す（図 2 の②）．無線接続～4-way handshake の詳細は本論文とは直接関係ないため説明は割愛する．この 4-way handshake 中あるいは完了後,「選択した暗号スイート, 端末の MAC アドレス, 鍵情報, SSID」などのセキュリティパラメータを対にしたエントリを作成し管理テーブルに追加する（図 2 の③）．その後，ルータ・中継機の GTK が更新された場合，ルータ・中継機は自身に接続されたすべての端末に対して Group key handshake と呼ばれる EAPOL-Key メッセージの 2 パケット交換により各端末に対して GTK 更新通知を行い（図 2 の④），管理テーブルを更新する（図 2 の⑤）．ここで，IEEE802.11i などの標準規格では GTK 更新のプロトコルは規定されているが，GTK の更新条件に関しては，特に規定はされていないため，実際には各ルータ・中継機の実装依存となる．PTK や GTK などの一時的な鍵は，端末がルータ・中継機に無線接続している間は保持され，無線切断（Disassociate や Deauthentication の送信）により認証やアソシエーションを失うと関連する一時的な鍵はすべて削除される．

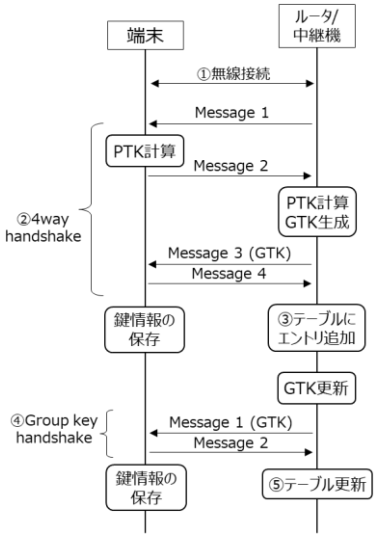


図 2　無線接続および鍵交換シーケンス
Figure 2　Association and Key exchange.

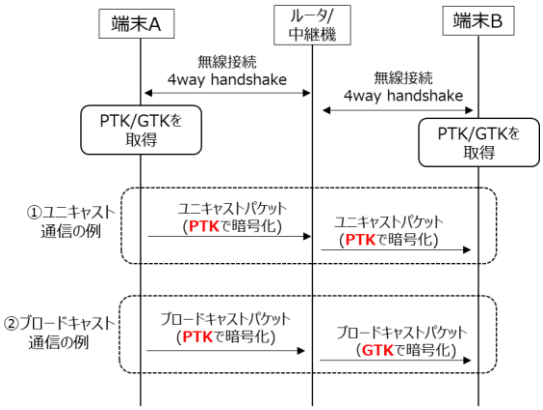


図 3　ユニキャストとブロードキャストの例
Figure 3　Example of unicast and broadcast

インフラストラクチャモードの接続形態においては，無線端末同士の通信は全てルータや中継機を経由して行われる．端末 A から端末 B にユニキャスト通信する場合，パケットは PTK で暗号化されてルータ・中継機に送信される．ルータ・中継機はそのパケットを PTK で暗号化して端末 B に転送する（図 3 の①）．端末 A からブロードキャスト通信を行う場合，端末 A からルータ・中継機への通信は無線レベルではユニキャスト通信となるため，ブロードキャストパケットを PTK で暗号化して送信する．ルータ・中継機

Vol.2019-GN-106 No.36
Vol.2019-CDS-24 No.36
Vol.2019-DCC-21 No.36
2019/1/25

はそれを GTK で暗号化してネットワーク内の全端末に転送する（図 3 の②）．マルチキャスト通信についてもブロードキャスト通信と同様である．

### 2.2 無線中継の仕組み

端末が中継機に接続すると，中継機とルータ間でも無線接続が行われる．中継機は端末の MAC アドレスではなく，中継機自身が管理する MAC アドレス（中継 MAC アドレス）に付け替えて接続を行う．これで端末とルータとの無線中継手続きが完了する（図 4 の①）．この時中継機では，管理テーブルに「ルータの SSID，選択した暗号スイート，中継 MAC アドレス，ルータから中継 MAC に配布された鍵情報」および「中継機の SSID，選択した暗号スイート，端末の MAC アドレス，中継機が端末に配布する鍵情報」などを対にしたエントリを追加する（図 4 の②）．ルータ側の GTK が更新されると，ルータは自身に接続されたすべての端末に対して Group key handshake により各端末に対して GTK 更新を行う．それらは中継機および中継 MAC アドレス宛となるため，中継機は自身と自身に接続する端末の分だけ応答を返す．この時中継機は管理テーブルのエントリをそれぞれ更新する（図 4 の③）．同様に，中継機側の GTK が更新されると，中継機は自身に接続されたすべての端末に対して GTK 更新を行い，管理テーブルを更新する．

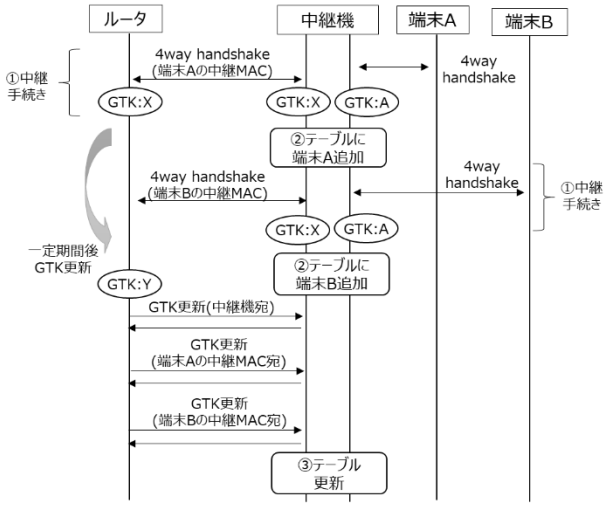


図 4 無線中継の仕組み

Figure 4 Mechanism of wireless relay.

### 2.3 GTK 更新の実装仕様により発生する課題

中継機配下に接続した端末同士で，最初はブロードキャスト／マルチキャスト通信が行えていたにも関わらず，一方の端末が一時的に切断して再接続すると，ブロードキャスト／マルチキャスト通信ができなくなるという接続性問題がある．無線 LAN 上のパケットをキャプチャして解析すると，最初は端末 A，端末 B はそれぞれ同じ GTK を配布され相互接続可能な連携状態であった（図 5 の①）．その後外出などでいったん切断した端末 B が再接続した際の 4-way handshake にて中継機から配布される GTK が新しくなっていた（図 5 の②）．端末 B から端末 A 宛の機器検索要求はブロードキャストで送信されるが，中継機が新しい GTK で暗号化するため，古い GTK を持つ端末 A がそれを復号できない（図 5 の③）．その結果端末 B は機器検索応答を得られず端末 A を発見できなくなっていることが判明した（図 5 の④）．GTK 更新時に中継機が接続済みの端末に GTK 更新通知を行わない実装により，古い GTK を持つ端末が通信不能となる．つまり中継機の GTK 更新の実装仕様により家庭内の IoT 機器の GTK の不一致を引き起こし，様々な IoT サービスを阻害することが課題である．とりわけ，マルチキャスト通信を利用することを前提とした ECHONET Lite[3]対応製品はサービスが利用できなくなる．特にスマートフォンで家電製品の操作を行うようなシステムの場合，ユーザがスマートフォンを持って外出し帰宅した際に発生するため容易に起こりうる．

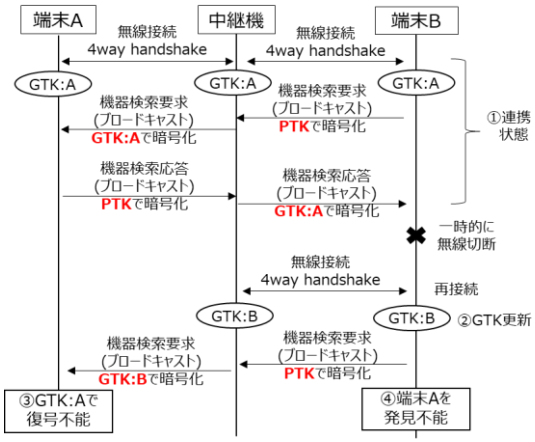


図 5 接続性問題の解析

Figure 5 Analysis of connectivity problem.

また，連携したい端末だけでなく，サービスに無関係な他の端末が一時的に切断し再接続した場合にも発生する（図 6）．この場合，ブロードキャスト通信で相互接続している端末 A および端末 B はいずれも古い GTK のままとなり，中継機の GTK 更新後は新しい GTK で暗号化されたパケットは復号できなくなるため，端末 A と端末 B は相互接続できなくなる．

これは例えば家族の誰かが外出から戻ってきてスマートフォンを接続すると，ユーザが今まで操作できていた家電を操作できなくなるケースである．さらに Web アクセスなどのユニキャスト通信は GTK ではなく PTK を使用するため可能である．スマートフォンから Web アクセスは可能であるにも関わらず家電操作だけができないという状況が発生し，接続障害の切り分けが付きにくく，ユーザの混乱を招く恐れがある．

Vol.2019-GN-106 No.36
Vol.2019-CDS-24 No.36
Vol.2019-DCC-21 No.36
2019/1/25

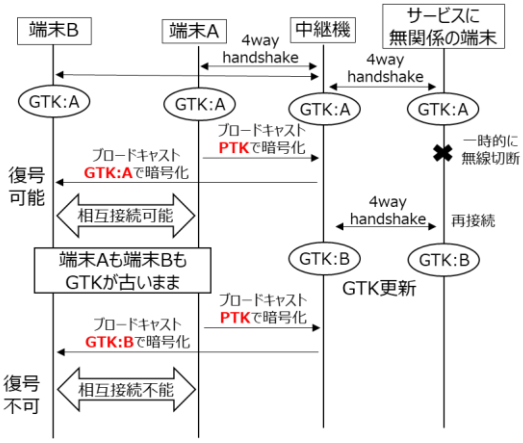


図 6　接続性問題の影響

Figure 6　Influence of connectivity problem.

## 3. 関連研究

グループ鍵を複数のメンバに対して配布する手法やセキュリティ向上のために鍵更新を行う技術は数多く提案されている．例えば，アクセス制御とグループ鍵管理方式により，セキュアにグループ鍵の配布を実現する手法がある[4]．しかしグループ鍵の更新やメンバの離脱に関しては考慮されていないため本論文の構成に当てはめることができない．また，メンバの離脱などグループの動的な変化に追随してグループ鍵の更新を行える手法がある[5][6]．各ノードがサーバとの間で 1 対 1 に保持するマスタ鍵を用い，サーバがグループ鍵をグループ内のノードに個別に配布する．あるノードがグループから脱退する際にグループ鍵の更新を行うが，この時新しいグループ鍵をそのノードのマスタ鍵で暗号化して送信する手法である．しかし，メンバ間におけるグループ鍵の不一致に関しては考慮されていないため課題は解決できない．これに対し，グループ鍵の更新をメンバ間で同期させる手法がある[7]．この手法では鍵サーバの鍵更新の期間ごとに鍵を配布されるが，鍵を使用しはじめる前の期間内にそれを配布しておくことで全メンバの鍵を同期させることができる．しかし本論文で示すような GTK 更新時に端末に通知を行わない中継機に対しては，この手法は適用できない．

本論文では，市販されている中継機の GTK 更新に関する実装状況を明らかにし，実環境において相互接続性を向上させる手法を検討する．

## 4. 中継機の実装調査と GTK 更新条件の解析

GTK の更新条件に関しては，IEEE802.11i などの標準規格では特に規定がなくメーカの実装依存となっているため，GTK 更新に関する課題が発生する中継機が市場にどのくらい存在するのかをまず調査した．また課題を解決するにあたり，中継機の GTK の更新条件を解析した．

### 4.1 中継機の実装調査

本論文で述べている中継機には，中継専用機を使用する場合と，中継機能を保有するルータを中継機として使用する場合がある．なお，中継機能を保有するルータについて，ルータとして使用しているときは「ルータ」と記載し，中継機として使用しているときは「中継機」と記載する．

パナソニック株式会社製品セキュリティセンターにて保有する日本国内向けルータ 723 台（市場シェア合計 98.2% 相当）のうち，シェアランク上位 90 台（シェア合計 79.1%）を抽出した．ここで，市場シェアの算出には下記の計算式，

$$\textit{対象ルータの市場シェア}(\%) = \frac{\textit{対象ルータの販売累計台数}}{\textit{全ルータの販売累計台数}}$$

を用いる．この時の各販売累計台数は，GfK による POS トラッキング調査結果[8]を利用して，2012 年 1 月から 2018 年 3 月の期間の販売累計台数を独自に集計したものである．

これらのルータの中で，まず無線中継機能を持つものを調査したところ，表 1 に示す通り 57 台（シェア合計 53.9%）となり，これらを調査対象とした．

表 1　無線中継機能を保有するルータ

Table 1　Home router with wireless range extender function.

| 無線中継機能 | 台数 | 市場シェア |
|---|---|---|
| 有り | 57 台 | 53.9% |
| 無し | 33 台 | 25.2% |
| 合計 | 90 台 | 79.1% |

また，保有する中継専用機 20 台（市場シェア合計 98.3% 相当）のうち，シェアランク上位 10 台（シェア合計 86.51%）を抽出した．（2016 年 1 月から 2017 年 12 月の期間において上記ルータのシェアの計算式と同様の式で算出）

これらの合計 67 台の中継機を，図 7 の構成となるよう各機器を接続した．端末 A，端末 B は，それぞれ市販されている無線製品を使用した．上位のルータは 1 製品で固定し，GTK 更新間隔はデフォルトの「30 分」のままとした．


図 7　調査構成

Figure 7　Investigation configuration.

この調査環境において，下記の手順にて中継機の GTK 更新が発生するかどうかを確認した．

1. ルータ・中継機を起動し中継機をルータに無線接続
2. 端末 A・端末 B を起動し中継機に無線接続

Vol.2019-GN-106 No.36
Vol.2019-CDS-24 No.36
Vol.2019-DCC-21 No.36
2019/1/25

3. 端末 B を電源オフし，30 分後電源オンする
4. 端末 B から端末 A を発見できるかどうか確認

この調査の結果，表 2 に示す通り 57 台中 7 台(シェア合計 6.1%)において，端末 B から端末 A を発見できないこと，つまり GTK 更新における課題が発生することが判明した．中継専用機 10 台に関しては全て課題は発生しなかった．

表 2 調査結果

Table 2 Investigation result.

| GTK 不一致の発生有無 | 台数 | 市場シェア合計 |
|---|---|---|
| 中継機能を保有するルータ | 57 台 | 53.9% |
| GTK 更新不一致あり | 7 台 | 6.1% |
| GTK 更新不一致なし | 50 台 | 47.8% |
| 中継専用機 | 10 台 | 86.51% |
| GTK 更新不一致あり | 0 台 | 0% |
| GTK 更新不一致なし | 10 台 | 86.51% |

### 4.2 GTK の更新条件の解析

GTK 更新条件についてより明確化を図るため以下の調査を行った．

- ルータの GTK 更新間隔と端末の切断期間
- 端末の切断期間中のルータの GTK 更新

ここで，表 2 に示す 7 台の中継機（中継機能を保有するルータ）のうち 1 番シェアの高い 1 台を使用して下記の解析を行った．

#### (1) ルータの GTK 更新間隔と端末の切断期間

「ルータの GTK 更新間隔」と「端末の切断期間」をそれぞれ変化させて，中継機の GTK 更新が発生するかどうかを調査した．表 3 に調査結果を示す．

表 3 の調査結果によると，ルータの GTK 更新間隔 5 分，もしくは端末の切断時間 5 分では発生しなかった．したがって端末の切断期間に関して，5 分超～30 分未満でも発生するかどうか，より詳細に調査が必要である．そこで下記(2)の「端末の切断期間中のルータの GTK 更新の調査」の中で，これらも合わせて詳細に調査を行った．

表 3 調査結果

Table 3 Investigation result.

| ルータの GTK 更新間隔 | 端末の切断期間 | 中継機の GTK 更新発生の有無 |
|---|---|---|
| 5 分 | 5 分 | 発生しない |
| | 30 分 | 発生しない |
| | 1 時間 | 発生しない |
| 15 分 | 5 分 | 発生しない |
| | 30 分 | 発生する |
| | 1 時間 | 発生する |
| 30 分 | 5 分 | 発生しない |
| | 30 分 | 発生する |
| | 1 時間 | 発生する |

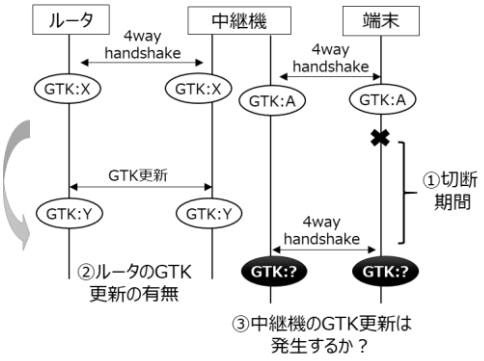


図 8 調査手順

Figure 8 Investigation procedure.

#### (2) 端末の切断期間中のルータの GTK 更新

端末の切断期間中にルータの GTK 更新が行われることが中継機の GTK 更新条件かどうかを調べるため，まず端末を一時的に切断した後，ルータの GTK 更新が行われたタイミングで端末を再接続させ，中継機の GTK 更新が行われるかどうかを確認した（図 8）．さらに，切断期間中に，上位ルータの GTK 更新が行われない場合も対比して確認した．調査結果を表 4 に示す．

表 4 調査結果

Table 4 Investigation result.

| 端末の切断期間 | 中継機の GTK 更新発生の有無 | |
|---|---|---|
| | ルータの GTK 更新する場合 | ルータの GTK 更新しない場合 |
| 3 分 | 発生しない | 発生しない |
| 6 分 | 発生しない | 発生しない |
| 8 分 | 発生しない | 発生しない |
| 10 分 | 発生しない | 発生しない |
| 10 分 30 秒 | 発生しない | 発生しない |
| 11 分 | 発生しない | 発生しない |
| 11 分 30 秒 | 発生しない | 発生しない |
| 12 分 | 発生する | 発生する |
| 15 分 | 発生する | 発生する |
| 20 分 | 発生する | 発生する |
| 30 分 | 発生する | - |

表 4 より，切断期間中にルータの GTK 更新が発生することは中継機の GTK 更新発生条件とは無関係であることがわかった．また，調査対象の中継機においては「切断期間：12 分」が GTK の更新条件であると判明した．

### 4.3 中継機の GTK の更新条件のまとめ

4.2 節の(2)の調査より中継機に接続していた端末が，12 分以上切断し再接続すると，中継機の GTK 更新が発生することがわかった．つまり，中継機の管理テーブルの有効期限が約 12 分弱と推測できる．

ここで，管理テーブルの有効期限に関して考察する．無

Vol.2019-GN-106 No.36
Vol.2019-CDS-24 No.36
Vol.2019-DCC-21 No.36
2019/1/25

線の電波状況やアプリの仕様等により無線切断・再接続を何度か繰り返す端末も存在すること，またパケットロスにより GTK 更新通知に対して端末から応答が返らない場合などを考慮して管理テーブルに有効期限を設けていると考える．有効期限内に管理テーブルの情報にアクセスがない場合にエントリが無効となり，端末の再接続時の 4-way handshake で新しい GTK が生成さるため中継機の GTK 更新が発生すると考えられる．ルータからの GTK 更新の通信もこの管理テーブルへのアクセスとなるため，**表** 3 の調査結果において，ルータの GTK 更新間隔が 5 分では発生しないが 15 分以上の場合に発生したのはこのためと考えられる．

## 5. 課題を解決する提案手法

課題が発生するほぼすべての中継機が過去 3 年以内に発売された新しいものであり今後も市場シェアを伸ばしていくことが予想されるため，課題の解決が必要である．課題を解決するためには，そもそも中継機側の実装を改善することが重要であるが，すでに市場に出回っている中継機も多数あるためそれだけでは不十分である．そこで，ルータの設定変更や端末側の実装で解決できる方法を検討した．

### 5.1 ルータの設定変更による提案手法

4.3 節の考察に基づき，ルータの GTK 更新間隔を 11 分 30 秒以内に設定することにより課題は解決可能である．そこで 4.1 節の調査で用いたルータ 90 台に対して GTK 更新の設定仕様を調査した．調査結果を表 5 に示す．表 5 より市場シェア 68%のルータが GTK 更新間隔 30 分以上，つまり中継機の GTK 更新が発生しうる状況で，そのうち 60%においてこの方法で課題は解決可能であることがわかった．しかしながら，残り 40%は本課題を解決可能な GTK 更新間隔を設定変更できる保障はないため，これだけでは不十分である．端末側の実装で課題を解決できる手法も考案して接続性を高める必要がある．

表 5　家庭用ルータの GTK 更新設定仕様
Table 5　Key update setting of home router.

| 初期値 | 設定変更の可否 | シェア合計 |
|---|---|---|
| GTK 更新しない | 変更可(1 分単位) | 25% |
| 60 分 | 変更可(1 分単位) | 14% |
| 30 分 | 変更可(1 分単位) | 21% |
| | 変更不可 | 8% |
| 上記以外 | - | 11% |
| 未調査 | - | 21% |

### 5.2 端末側の実装による提案手法

中継機配下のネットワーク内で定期的に GTK を使用した通信を発生させ，中継機の管理テーブルへのアクセスを行えば，エントリを維持でき端末再接続の際に中継機の GTK 更新が発生しないのではないかと考え，図 7 の構成において，下記の手順にて中継機の GTK 更新が発生するかどうかを確認した．

1. ルータ・中継機を起動し中継機をルータに無線接続
2. 端末 A・端末 B を起動し中継機に無線接続
3. 端末 A から 1 分おきにブロードキャスト通信（GTK 利用）を発生させる
4. 端末 B を電源オフし，30 分後電源オンする

この結果，端末 B の再接続後に中継機の GTK 更新が発生した．つまり，他端末から中継機の管理テーブルへアクセスしても解決できないことが判明した．ゆえに，接続済みの端末が切断し再接続すると中継機の GTK 更新が発生するのは避けられないとして，端末が中継機の GTK 更新の発生を検知して新しい GTK を入手できる方法を考案した．

#### 5.2.1 GTK 更新発生検知のロジック

端末が中継機の GTK 更新の発生を検知するロジックは，

- 端末が自分の保有する GTK が古くなっていないかどうかを常に監視する
- GTK が古くなったと判断した場合に，無線の再接続を行い新しい GTK を取得する

上記により，ネットワーク内の他の端末が切断し再接続を行った際に中継機の GTK が更新されたとしても，通信不能に陥ることを回避可能である．

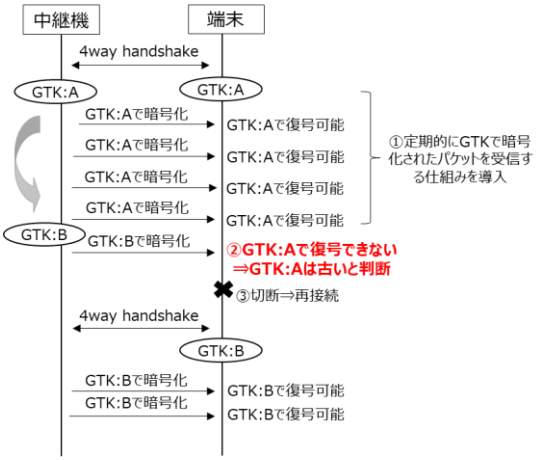


図 9　提案手法のロジック
Figure 9　Logic of the proposed method.

ここで，自分の保有する GTK が古いかどうかを確認する手段として，定期的に GTK で暗号化されたパケットを受信するような仕組みを実装すればよい（図 9 の①）．中継機の GTK 更新が行われると，定期的に受信し復号化できていたパケットが復号できなくなる．そのことにより自分の保有する GTK が古くなっていると判断し（図 9 の②），

Vol.2019-GN-106 No.36
Vol.2019-CDS-24 No.36
Vol.2019-DCC-21 No.36
2019/1/25

無線をいったん切断後，再接続して新しい GTK を取得すればよい（図 9 の③）.

### 5.2.2 実環境における実装案

端末が定期的に GTK で暗号化されたパケットを受信する仕組みを実現するために，例えばネットワーク内に存在する他端末から定期的に ARP などのブロードキャストパケットを送信してもらえば実現可能である．しかし，提案手法を実装した端末とのセット売りは非現実的であるため，端末単体で気付ける仕組みが必要である.

自端末にネットワークインタフェース(以降 I/F と呼ぶ)が 2 つ以上存在する場合，一方の I/F から他方の I/F 宛（例えば，有線 LAN 側 I/F から無線 LAN 側 I/F 宛や，無線 2.4GHz 側 I/F から無線 5GHz 側 I/F 宛など）に，定期的に ARP などのブロードキャストパケットを送信することにより端末単体で検知することが可能である．この方法は比較的容易に実装可能であるが，いずれか一方の I/F しか有効にできない端末も多い．また，特に白物家電などスペックが低い端末は 2 つも I/F を持ってないことが多く，そのような端末では実現不能である．そこで，I/F を 1 つしか持たない（または 1 つしか有効にできない）端末でも実現できる手法として，ホームネットワーク内に必ず存在するであろう「ルータ」を利用してブロードキャストあるいはマルチキャストのパケットを受信できる手法を検討した.

#### (1) UPnP を利用する手法

市販のルータにはほぼ必ず UPnP(Universal Plug and Play)の IGD(InternetGatewayDevice)機能が搭載されており，デバイス利用可能通知(ssdp:alive)メッセージが定期的にマルチキャストで送信されるためこれを監視すればよい．ただし，ルータによって送信間隔はさまざまであり，60 秒程度で送信するものもあれば 5 分以上の間隔が開くものもあるため，GTK が古くなったことを判断するまでに時間がかかるという問題点がある.

#### (2) DHCP を利用する手法

ルータに必ず搭載されている DHCP サーバを利用して，DHCP のブロードキャストで送信されるメッセージを定期的に受信する方法もある．DHCP のパケットは端末が要求を送信しそれに対してルータが応答を返すシーケンスとなるため，送信間隔を端末が自由に決めることができるという利点があり，実現性が高いため，DHCP を用いることとする.

### 5.2.3 提案手法

定期送信する DHCP のブロードキャストパケットとしては，T2 Request メッセージを使用する．これは端末が最初に IP アドレスを取得した後，その IP アドレスのリース延長を要求するメッセージであり，メッセージ内の「broadcast flag」を「True(broadcast)」に設定して送信することで，ルータからの応答である ACK メッセージをブロードキャスト送信させることができる．このことにより，GTK で暗号化されたパケットを定期的に受信する仕組みが導入できる．また定期間隔としては，表 5 に示す通りルータの GTK 更新間隔は 1 分単位で設定可能であり，GTK 更新を検知するタイミングもそれと思想を合わせて 1 分間隔とする.

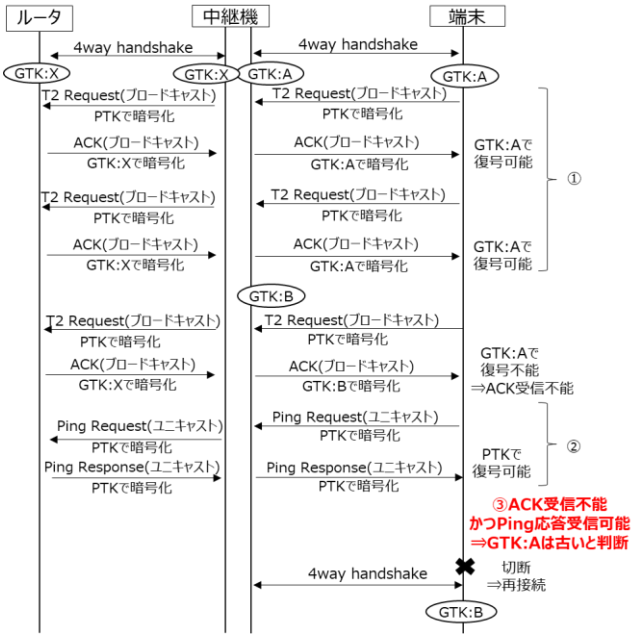


図 10 提案手法のシーケンス

Figure 10 Sequence of the proposed method.

ここで，ルータが電源オフ状態となりネットワーク上に存在しなくなった場合にも，ブロードキャストパケットが受信できなくなる．この場合と切り分けるため，ルータに対する生存確認の目的としてユニキャスト通信を行っても良い．ユニキャストパケットとして Ping Request を用いることとする．これらを踏まえて，課題を解決するため以下の仕様を端末側で実装することを提案する.

1. 端末からルータに定期的(1 分毎)に DHCP T2 Request(ブロードキャスト)を送信する.
   ただしこの時，DHCP メッセージ内の「broadcast flag」を「True(broadcast)」に設定して送信する（図 10 の①）.
2. T2 Request に対する ACK(ブロードキャスト)を受信できない場合，端末からルータに Ping Request(ユニキャスト)を送信する（図 10 の②）.
3. T2 Request に対する ACK(ブロードキャスト)を受信できず，かつ Ping 応答(ユニキャスト)を受信できる場合 GTK が古くなったと判断し，無線切断後再接続を行い，新しい GTK を取得する（図 10 の③）.

Vol.2019-GN-106 No.36
Vol.2019-CDS-24 No.36
Vol.2019-DCC-21 No.36
2019/1/25

## 6. 実験

実験環境として,4.1 節における中継機調査の環境(図 7)と同様の環境を用いた．端末 A には 5.2.3 項の提案手法を実装した評価ツールをインストールした．中継機は表 2 に示した課題が発生する中継機 7 台(シェア合計 6.1%)を使用した．この実験環境において，下記の手順にて提案手法の効果を確認した．また同時に課題が発生する中継機 7 台のテーブル有効期限も調査した．

1. ルータ・中継機・各端末を起動し無線接続
2. 端末 A で評価ツールの実行を開始
3. 端末 B を電源オフし，X 分後電源オンする
4. 端末 B の GTK が更新されていることを確認
5. 端末 A において GTK 更新を検知し，再接続により新しい GTK を取得することを確認
6. 端末 B から端末 A を発見できるかどうか確認

この結果，表 2 に示した GTK 更新時に端末に通知しない中継機 7 台(シェア合計 6.1%)において，端末 B から端末 A を発見できること，つまり課題を解決できることがわかった．また，手順 3 の X を変化させることにより判明した各中継機のテーブル有効期限を 表 6 に示す．表 6 より，中継機のテーブル有効期限はチップメーカの実装仕様により異なることがわかった．今回の 4.1 節の調査ではルータの鍵更新時間 30 分および端末の切断時間 30 分で調査したため,管理テーブルの有効期限が 30 分以内の中継機しか洗い出せていない．課題が発生しなかった中継機の管理テーブルの有効期限は「30 分以上」あるいは「有効期限なし」と考えられる．そのような中継機においてもルータの鍵更新の仕様によっては中継機の GTK 更新問題が発生する可能性があるが，本手法により課題は解決できる．また有効期限で 1 番短いものは約 12 分であったため，5.1 節の提案手法におけるルータ側の鍵更新間隔を 11 分半以下にする手法も有効であることがわかった．

表 6　中継機のテーブル有効期限調査の結果
Table 6　Result of the table valid term.

| 有効期限 | 台数 | シェア合計 |
|---|---|---|
| 約 12 分 | 1 台 | 2.1% |
| 約 20 分 | 3 台 | 2.4% |
| 約 22 分 | 2 台 | 1.0% |
| 約 25 分 | 1 台 | 0.6% |

## 7. まとめと今後の展開

本論文では，中継機の GTK 更新に関する実装状況を調査し，相互接続性を阻害する中継機の GTK 更新条件を明らかにした．また中継機の GTK 更新の実装仕様により，無線 LAN ネットワーク上で古い GTK を持つ端末と，新しい GTK を持つ端末との間でブロードキャストやマルチキャスト通信が不能になり相互接続ができない問題に関し，ルータ側の設定と端末側の実装で相互接続性を確保可能とする手法の提案を行った．その結果，今回調査した中継機能を保持するルータ 57 台のうち，提案手法導入前は 50 台のルータでブロードキャストおよびマルチキャスト通信の相互接続ができていたが，提案手法導入することにより全 57 台に関して相互接続性を確保することができた．

ルータの設定は一般ユーザには困難であるため，ECHONET Lite 対応製品は本提案手法を実装することで市場における接続性問題の発生を未然に防ぐことができる．そのため,本論文で調査した内容を 2019 年 1 月にエコーネットコンソーシアムに報告し，2019 年 4 月の採択を目指して提案活動を行い，各社の市場製品の通信品質向上に貢献できるよう取り組んでいく予定である．

今回の提案手法においては，DHCP のブロードキャストメッセージを使用し，定期間隔として 1 分間隔で送信を行ったが，他のプロトコルを用いた評価や最適な定期送信間隔の調査を行い，更なる改善仕様の検討を進める予定である．

## 参考文献

[1] Wi-Fi Alliance, “Security”. https://www.wi-fi.org/discover-wi-fi/security
[2] “IEEE Std 802.11i”, https://ieeexplore.ieee.org/document/1318903.
[3]“ECHONET Lite 規格 Ver.1.12 第 2 部”. https://echonet.jp/wp/wp-content/uploads/pdf/General/Standard/ECHONET_lite_V1_12_jp/ECHONET-Lite_Ver.1.12_02.pdf.
[4] 上野英俊，田中希世子，原下貴志，鈴木偉元，石川憲洋，高橋修．マルチキャストセキュリティアーキテクチャの提案と実装．DICOMO 2003 シンポジウム. 2003, pp.113-116.
[5] Burmester, M.V.D. and Desmedt, Y.: A secure and efficient conference key distribution system, Advances in Cryptology – EUROCRYPT’94, pp.275-286(1995).
[6] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, D.E.: SPINS: Security protocols for sensor networks, Wireless Networks, Vol.8, No.5, pp.521-534(2002).
[7] 浅野歩，岸田崇志，前田香，河野英太郎．鍵の同期を考慮した鍵の配布・更新の提案と実装．情報処理学会研究報告. 2005-DSM-39(9), pp.49-54.
[8] “GfK，生活家電の POS トラッキング調査”. http://www.gfk.com/jp/industries/consumer-goods/home-appliances/.