情報処理学会論文誌　コンシューマ・デバイス & システム　Vol.10　No.1　26–39 (Feb. 2020)

コンシューマ・システム論文

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,a)]　土屋 薫子[1]　石川 博一[1]　村上 隆史[1]　杉村 博[2]　森 信一郎[3]　一色 正男[2]

受付日 2019年7月8日, 採録日 2019年11月25日

概要：本論文では，無線 LAN 中継機のグループ鍵更新仕様に関するメーカ別の解釈の違いによって引き起こされる相互接続性問題に関して原因を調査し，端末側実装での相互接続性改善手法を提案する．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がある．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不能になり，相互接続できない問題が発生する．標準規格である IEEE 802.11i では GTK の更新条件や GTK 更新通知を行うタイミング，また端末切断時のアクセスポイント側の GTK の取り扱い方に関して明確に規定されていない．そのため開発者の仕様の解釈により中継機の GTK 更新の実装仕様に違いが生じ相互接続性を阻害していると考えた．そこで，このような仕様の解釈の違いが発生する原因を調査し端末側の実装で相互接続性を確保するための手法を提案した．さらに提案手法の評価と考察を行った．

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 to the Issue for Updating Group Temporal Keys in Wireless Range Extenders

Moe Hamamoto[1,2,a)]　Kaoruko Tsuchiya[1]　Hirokazu Ishikawa[1]　Takashi Murakami[1]
Hiroshi Sugimura[2]　Shinichiro Mori[3]　Masao Isshiki[2]

Received: July 8, 2019, Accepted: November 25, 2019

Abstract: This paper investigates interoperability issues caused by manufacturers interpreting standards for group key updates in wireless range extenders and proposes a method to improve interconnectivity with a device side implementation. When a wireless terminal connects to a router or wireless range extender, this terminal obtains two keys necessary for encryption or decryption. One is PTK (Pairwise Transient Key) used for unicast communications, and the other is GTK (Group Temporal Key) used for broadcast and multicast communications. Some home routers and wireless range extenders can be configured to update the GTK at regular time intervals to enhance the safety of communications by not sharing a specific GTK for a long period of time. However, implementations for updating the GTK in some wireless range extenders may result GTK inconsistency across the terminals in a wireless LAN network. This results in broken broadcast or multicast communications between terminals that have the old GTK and terminals that have the new GTK, causing the interconnectivity issue. The IEEE 802.11i standard does not clearly define GTK update conditions, the timing of GTK update notifications and how to handle the GTK within the access point when a terminal is disconnected. Therefore, we thought that the difference in the implementation of GTK updates in wireless range extenders is caused by differences in the interpretation of the standard by developers causing the interoperability issues. To this, we investigated why differences in interpreting the specification occur, and propose a method to improve interconnectivity through a device side implementation. Furthermore, we evaluated and considered the proposed method.

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

© 2020 Information Processing Society of Japan

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．たと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が発生している．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いる．**図 1** は日本国内向けルータのうち，2014 年 12 月時点のシェアランク上位 90 機種，2016 年 9 月時点のシェアランク上位 90 機種，2018 年 3 月時点のシェアランク上位 90 機種のルータに対してそれぞれ中継機能を保有するか否かを調査し，保有しているもののシェア合計の推移を示したものである．

ここで，本論文において記載する市場シェアは，GfK による POS トラッキング調査結果 [1] を利用して下記算出式により求めたものである．

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

図 1 より 2014 年 12 月時点から 2016 年 9 月時点では市場シェアがわずか 1%しか増加していないにもかかわらず，2016 年 9 月時点から 2018 年 3 月時点においては約 17%もシェアを伸ばしていることから，中継機はここ数年で急速に普及していることが分かる．

図 2 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．通常，ルータや中継機などの無線アクセスポイント機能を持つ製品は，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 [2]．WPA2 は IEEE802.11i [3] で規格化された無線 LAN セキュリティ仕様である．各端末は，それぞれが接続するルータあるいは中継機から 4-way handshake と呼ばれる鍵交換シーケンスを通じて取得す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暗号鍵を使用する．ここで暗号鍵には，ユニキャスト通信する際に使用する 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 種類の鍵がある．ここで端末が GTK を使用するのは，ブロードキャストあるいはマルチキャストで受信したパケットを復号化するときのみである．それは，端末がブロードキャスト/マルチキャストでパケットを送信する場合，端末から中継機への通信は無線レイヤではユニキャスト通信となるため，PTK で暗号化して送信するが，それを受け取ったルータ・中継機が GTK で暗号化してネットワーク内の全端末あるいは特定端末に転送し，端末が GTK で復号化するという仕組みによるためである．また，PTK は端末ごとに異なるが，GTK はルータ配下の全端末，あるいは中継機配下の全端末でそれぞれ共通である．ルータ・中継機の中には，この GTK を一定時間ごとに更新することにより通信の安全性を高めるものもある．GTK が更新された場合，通常であればルータ・中継機は自身に接続されたすべての端末に対して GTK 更新通知を行う必要がある．そうしなければ，ネットワーク上の端末間において GTK の不一致が発生し，GTK を利用した通信が行えなくなるためである．しかし，市場では実際に中継機配下の端末間で GTK が不一致となりブロードキャスト/マルチキャスト通信ができなくなるという問題が発生している．この問題はマルチキャスト通信を利用することを前提とした ECHONET Lite [4] 対応製品はサービスが利用できなくなるため深刻な問題である．原因として，標準規格である IEEE 802.11i では GTK 更新通知のタイミングは明記されていないことや，そもそも中継機の実装仕様に関しては特に標準規格がないため，各ルータメーカ，あるいは無線のチップベンダの開発者の仕様解釈により中継機の実装仕様に違いが生じ相互接続性を阻害していると考える．先述のとおり，中継機の市場への普及は進んでおり今後も市場におけるトラブルの増加は避けられないため早

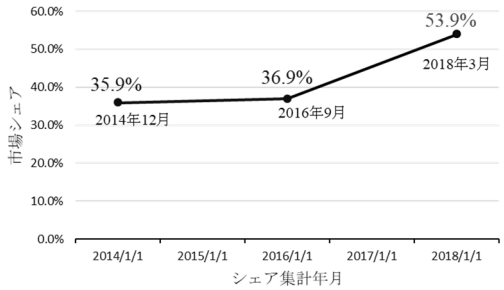


図 1　無線中継機能のシェア推移
Fig. 1　Trend of market share of wireless range extender.

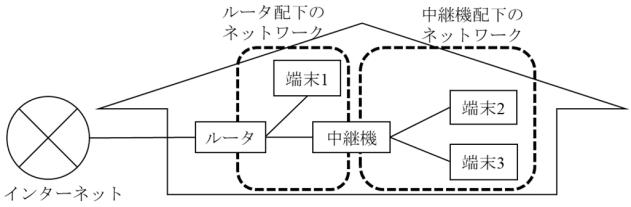


図 2　無線 LAN ネットワークの例
Fig. 2　Example of wireless network.

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
3　神奈川工科大学スマートハウス研究センター客員研究員
Kanagawa Institute of Technology, Atsugi, Kanagawa 243–0292, Japan
a)　hamamoto.moe@jp.panasonic.com

© 2020 Information Processing Society of Japan

急な解決が必要である．

本論文では，このような仕様の解釈の違いが引き起こすと考えられる相互接続性問題に関し，解釈の違いが発生する原因を調査し，端末側で相互接続性を確保するための手法の提案を行うとともに提案手法の評価と考察を述べる．

2. 無線中継機の実装調査

まず市場で発生した問題を再現し，課題が発生する原因を調査した．そしてその課題が，仕様のどの部分の解釈から生じたのかを明らかにした．またその課題に対処する方法を検討するにあたり，課題が発生する中継機の市場における普及率を調査した．

2.1 市場問題の解析と課題の発生原因の特定

市場問題として報告された内容は，「最初は相互接続可能だった端末どうしのいずれかが一時的に無線を切断し再接続すると相互接続できなくなる」というものであった．

この問題の再現環境および再現手順を確立すべく，報告されたルータ，中継機を用いて無線 LAN ネットワークを構築した．また市販されている無線製品である端末 A，端末 B として**図 3** の構成となるよう接続した．上位のルータの GTK 更新間隔はデフォルトの「30 分」のままとした．

この再現環境において，端末 A および端末 B を中継機に無線接続すると，いずれも中継機から同じ GTK を配布され，端末 B からブロードキャストで送信される機器検索要求に対して端末 A が応答を返し，相互接続可能であった（**図 4** の①）．その後端末 B の無線を切断し，すぐ再接続させると，端末 B が 4-way handshake を通じて中継機から配布される GTK は切断前の GTK と同じであり，相互接続可能であった．端末 B の切断時間が短い場合には再現しないと考え，端末 B を切断してから 12 時間経過後に端末 B を再度無線接続させたところ，4-way handshake を通じて中継機から配布される GTK が更新された（図 4 の②）．このとき中継機から端末 A への GTK 更新通知は送信されず，端末 A と端末 B の GTK が不一致となる状態となった．その後端末 B から端末 A を検索させると，端末 B から端末 A 宛に機器検索要求が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かった（図 4 の③）．その結果端末 B は機器検索応答を得られず端末 A を発見できなかった（図 4 の④）．つまり，GTK の不一致が発生したことにより，端末間でブロードキャスト通信が不能になり相互接続できない問題が引き起こされていた．このようにネットワーク上の端末間で GTK の不一致が発生することを，以降課題という．

ここで，中継機の GTK 更新条件についてより明確化を図るため，どのくらい端末 B を切断すれば中継機の GTK 更新が発生するのかを調査した．先述の再現環境では上位

図 3　再現環境
Fig. 3　Reproduction environment.

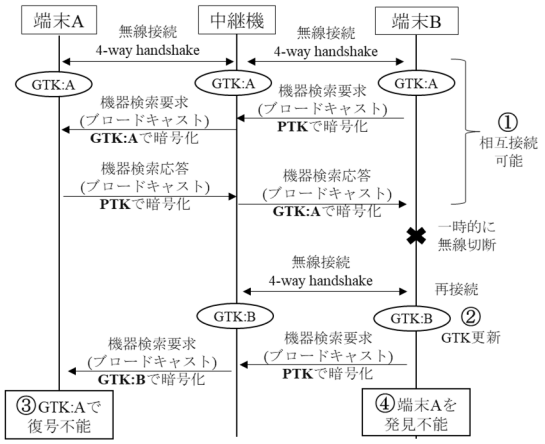


図 4　市場問題の解析
Fig. 4　Analysis of market problem.

表 1　ルータの GTK 更新間隔と端末切断期間の調査結果
Table 1　Investigation result of router's GTK update interval and terminal disconnected period.

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
	10 分	発生しない
	30 分	発生しない
	1 時間	発生しない
10 分	5 分	発生しない
	10 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
	10 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
	10 分	発生しない
	30 分	発生する
	1 時間	発生する

のルータの GTK 更新間隔はデフォルトの「30 分」で実施したため，このパラメータも変化させながら調査を行った結果が**表 1** である．表 1 によると，ルータの GTK 更新間隔が 5 分および 10 分の場合には端末の切断期間が何分であろうと発生しなかった．また端末の切断時間が 5 分および 10 分の場合にはルータの GTK 更新間隔が何分であろうが発生しなかった．このことによりルータの GTK 更新間隔あるいは端末の切断期間のいずれか一方が 10 分以内で

© 2020 Information Processing Society of Japan

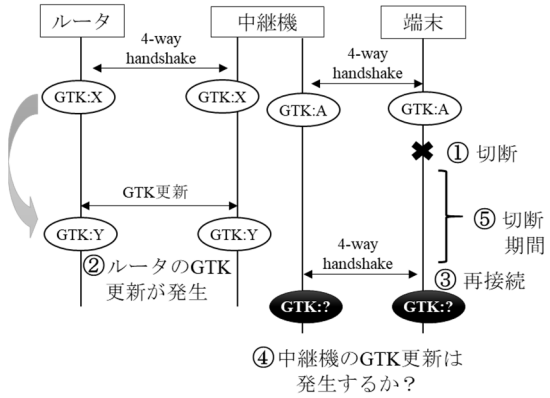


図 5　調査手順

Fig. 5　Investigation procedure.

表 2　端末切断期間中のルータの GTK 更新の関連性

Table 2　Relevance of router's GTK update during terminal disconnected period.

端末の切断期間	中継機の GTK 更新発生の有無	
	ルータが GTK 更新する場合	ルータが 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	-

あれば，中継機の GTK 更新は発生しないことが分かった．

また，表 1 の結果から，ルータの GTK 更新間隔が 15 分以上の場合に，端末の切断期間中にルータの GTK 更新が行われると，中継機の GTK 更新が発生するのではないかと考えた．そこで上記ルータの GTK 更新間隔を 30 分に固定した環境で，端末の切断期間中にルータの GTK 更新が行われる場合の中継機の GTK 更新調査を行った．まず端末を一時的に切断した後（**図 5** の①），ルータの GTK 更新が行われたタイミング（図 5 の②）で端末を再接続させ（図 5 の③），中継機の GTK 更新が発生するかどうかを確認した（図 5 の④）．対比のため，切断期間中に上位ルータの GTK 更新が行われない場合（図 5 の②がない場合）も確認した．そのときの端末の切断期間（図 5 の⑤）と中継機の GTK 更新発生の有無をまとめたものが**表 2** である．

表 2 より，端末の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分かった．そして，GTK 更新発生の条件は「端末の切断期間が 12 分以上」であることが分かった．

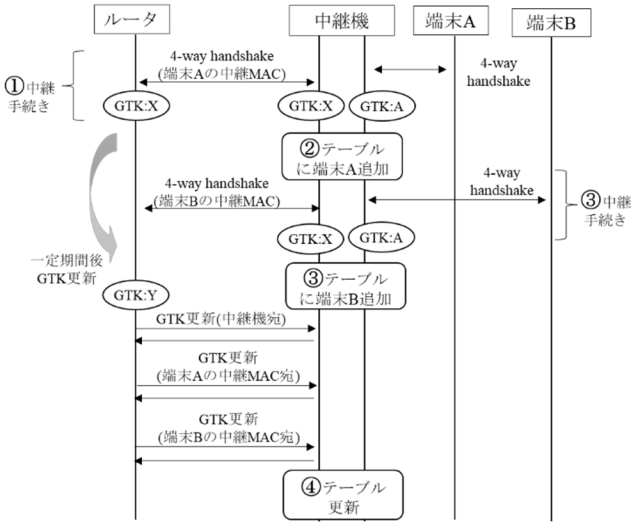


図 6　無線中継の仕組み

Fig. 6　Mechanism of wireless relay.

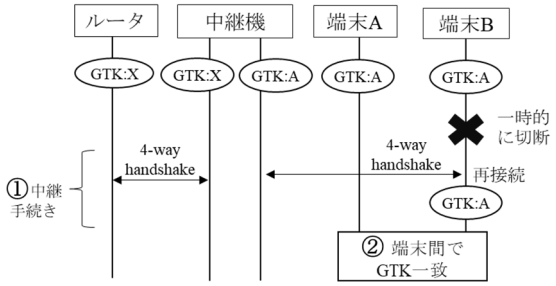


図 7　課題が発生しない中継機の場合

Fig. 7　In case of reconnecting to wireless range extender that does not have issue.

以上より，課題発生の原因は下記の 2 つであると判明した．

(1) 一定期間（12 分以上）切断された端末が再接続すると中継機が GTK を更新すること

(2) GTK 更新時に中継機が接続済み端末に GTK 更新通知を行わないこと

2.2　課題が発生する中継機の実装仕様

2.1 節で課題発生の原因は 2 つあることが判明したが，それぞれどのような仕様の解釈から生じる問題なのかを明らかにする必要がある．そもそも中継機の実装仕様には標準規格はないため，まず，無線中継の実装仕様を調査する．そこで，課題が発生しない中継機および課題が発生する中継機の無線 LAN 上のパケットをそれぞれ解析した．以下，**図 6**，**図 7**，**図 8** を用いて説明する．

まず端末 A 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ていた．中継機は無線ルータと端末の無線通信を中継するものであるため，端末が中継機に接続した際に，端末の代わりにルータに対して無線接続を行っていると考える．このとき中継機は端末 A 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（以

© 2020 Information Processing Society of Japan

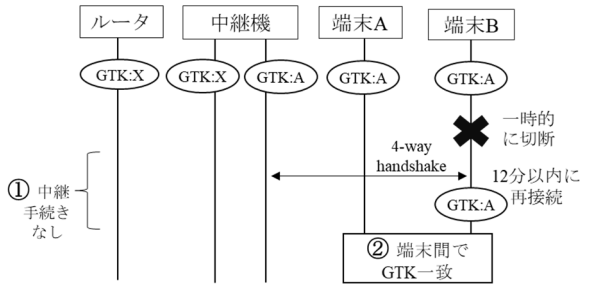


図 8　課題が発生する中継機に 12 分以内に再接続した場合
Fig. 8　In case of reconnecting within 12 minutes to wireless range extender that has issue.

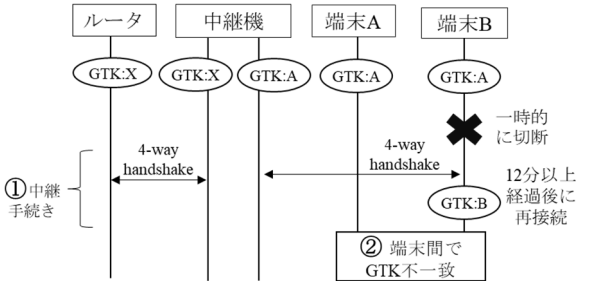


図 9　課題が発生する中継機に 12 分以上経過後に再接続した場合
Fig. 9　In case of reconnecting after more than 12 minutes to wireless range extender that has issue.

降，中継 MAC アドレスと呼ぶ）に付け替えて接続を行っていた．これで端末 A とルータとの無線中継手続きが完了する（図 6 の①）．この挙動から，中継機はルータに対しては無線クライアントとして，また自身に接続する端末に対しては無線アクセスポイントとして振る舞うことにより，つまり，無線の標準規格（IEEE 802.11 シリーズ）の無線クライアントと無線アクセスポイントの両方の規格を同時に実行することにより無線中継を実現していると判断できる．このとき中継機では，自身に接続する端末ごとにこの無線中継情報を記憶しておくため，管理テーブルを設けていると考える．つまり，自身で実行している無線クライアントとしての情報と無線アクセスポイントとしての情報を結び付けて管理するためのテーブルである．そしてその管理テーブルに「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」などの無線中継に必要な情報を対にしたエントリを追加していると考える（図 6 の②）．端末 B が中継機に接続する場合も同様である（図 6 の③）．その後ルータ側の 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 GTK 更新通知を行っていた．それらは中継機および中継 MAC アドレス宛となっており，中継機は自身と自身に接続する端末の分だけ応答を返していた．このとき中継機は管理テーブルのそれぞれエントリに対してルータの GTK を新しく配布されたものに更新していると考える（図 6 の④）．ここまでの挙動は，課題が発生しない中継機および課題が発生する中継機で共通であり，一般的な中継機の実装仕様であると考えられる．これをふまえて，課題発生の 2 つの原因がどのような仕様の解釈から生じるのかを考察する．

まず課題発生の原因 (1) に関して，課題が発生しない中継機の場合，端末 B が一定期間（30 分）切断し再接続すると，図 6 の①同様，中継機とルータの間で中継手続きが行われる（図 7 の①）．端末 B が 4-way handshake で取得する GTK は以前と同じ GTK であるため，端末 A と端末 B との GTK は一致する（図 7 の②）．また，課題が発生する

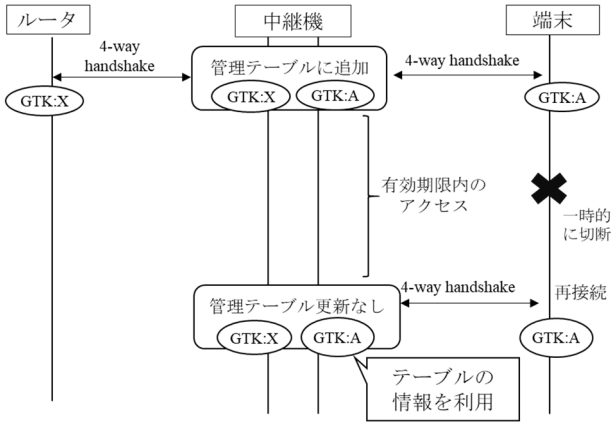


図 10　管理テーブルの仕様
Fig. 10　Specification of management table.

中継機に，端末 B が 12 分以内に再接続すると，中継機とルータの間で中継手続きが行われない（図 8 の①）．端末 B が再接続時に 4-way handshake で取得する GTK は以前と同じ GTK であり，端末 A と端末 B との GTK は一致する（図 8）．

一方，課題の発生する中継機に対して，切断後 12 分以上経過後に端末 B を再接続させると，中継機とルータの間で中継手続きが行われる（**図 9** の①）．このタイミングで中継機の GTK が更新され，端末 B が 4-way handshake で取得する GTK は新しい GTK であるため，端末 A と端末 B との GTK が不一致となる（図 9 の②）．

以上より，課題が発生する中継機において，切断した端末 B が 12 分以内に再接続した際に中継手続きを行わない理由は，端末の切断後も一定期間管理テーブルに有効期限を設けており，有効期限内に管理テーブルにアクセスがある場合，ルータとの中継手続きは行うことなくテーブルの情報を使用するためと考えられる（**図 10**）．このように管理テーブルに有効期限を設けている理由としては，無線の電波状況やアプリの仕様などにより無線切断・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端末から応答が返らない場合などの準正常系を考慮したものと考えることができる．

また切断した端末 B が 12 分以上経過後に再接続した際

© 2020 Information Processing Society of Japan

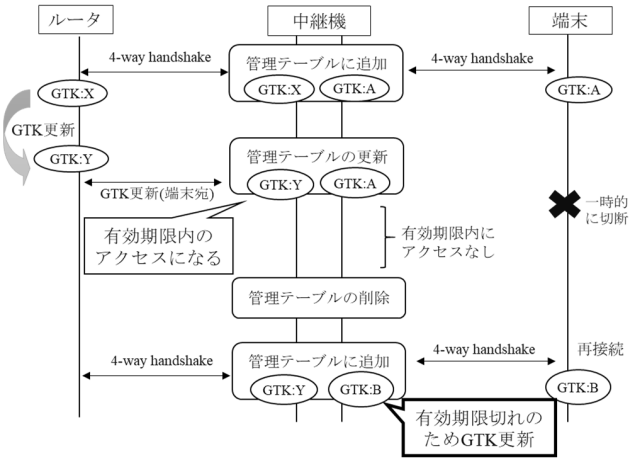


図 11　GTK 更新発生の理由
Fig. 11　Reason for GTK update occurrence.

に中継機の GTK が更新された理由は，テーブルの有効期限が切れていたためと考える．具体的には，表 2 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 更新が発生したため，この調査対象の中継機の管理テーブルの有効期限は約 12 分弱であると考えるのが妥当である．つまり，管理テーブルの有効期限内に端末からのアクセスがなければ管理テーブルからエントリが削除され，その後の端末接続時の 4-way handshake で新しい GTK が生成されるため中継機の GTK が更新される実装仕様であると考える（**図 11**）．ここで表 1 より，ルータの GTK 更新間隔が 10 分以内であれば端末の切断期間が何分であろうと，端末の再接続時に中継機の GTK 更新は発生しなかったことから，ルータの GTK 更新も管理テーブルへのアクセスと見なされると判断できる．

標準規格の IEEE 802.11i においては，端末がルータや中継機などのアクセスポイントから切断した際には，端末側での GTK 情報は破棄されるという記載はあるが，アクセスポイント側の振舞いに関しては特に規定されていない．よって中継機における管理テーブルの実装仕様として，中継機配下の端末が切断した場合の管理テーブルの扱い方に関してはメーカの実装依存部分であり，この実装仕様の違いが課題発生の原因 (1) を生じさせていると考える．

次に，課題発生の原因 (2) に関して，GTK を更新した場合，通常であれば中継機に接続済みのすべての端末に対してすみやかに GTK 更新通知を行い，ネットワーク上の端末間で GTK の不一致が発生しないよう実装されるべきである．しかしながら，IEEE 802.11i では GTK 更新を通知する際のプロトコルは規定されているが，GTK の更新通知のタイミングに関しては明確に規定されていないため，開発者の解釈の違いにより想定外の設計となった可能性がある．

表 3　無線中継機能を保有するルータ
Table 3　Home router with wireless range extender function.

無線中継機能	機種数	市場シェア
有り	57 機種	53.9%
無し	33 機種	25.2%
合計	90 機種	79.1%

表 4　市場での影響度の調査結果
Table 4　Result of investigating market impact.

課題の発生有無	機種数	市場シェア合計
課題発生あり	7 機種	6.1%
課題発生なし	50 機種	47.8%
合計	57 機種	53.9%

2.3　市場での影響度の調査

このような実装仕様である中継機が市場においてどのくらい普及しているかを調査するにあたり，まず日本国内向けルータ 723 機種（市場シェア合計 98.2%相当）のうち，シェアランク上位 90 機種（シェア合計 79.1%）を抽出した．このときの各販売累計台数は，GfK による POS トラッキング調査結果 [1] 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，無線中継機能を持つものを調査したところ，**表 3** に示すとおり 57 機種（シェア合計 53.9%）となり，これらを調査対象とした．

これらの合計 57 機種の中継機を，図 3 の構成となるよう各機器を接続し，下記の再現手順を実施し，課題が発生する中継機を洗い出した．

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 B を電源オフし，30 分後，電源オンする
4. 端末 B からブロードキャストによる機器検索要求を送信し，端末 A を発見できるかどうか確認

この調査の結果，**表 4** に示すとおり 57 機種中 7 機種（シェア合計 6.1%）において，課題発生により端末 B から端末 A を発見できないことが判明した．ここで無線に関する動作はルータメーカによる制約ではなく，ルータに実装している無線チップに依存する．課題のある中継機 7 機種に搭載されている無線チップベンダは合計 2 社である．

課題が発生する実装仕様である中継機（シェア合計 6.1%）は，2018 年 3 月時点における累計販売台数約 91 万 5 千台に相当するものであり，すでに市場で普及していると考えられるため，端末側の実装で課題を解決する必要がある．

3.　課題を解決する提案手法

2.1 節で判明した課題発生の原因 (1) を対処すれば原因 (2) も含めて課題を解決できると考え，その方法を検討した．

そこでまず，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

© 2020 Information Processing Society of Japan

へのアクセスを行えば，エントリを維持でき，他の端末の再接続時に中継機の GTK 更新が発生しないのではないかと考えた．図 3 の構成において，下記手順にて課題を解決でき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
5. 端末 B からブロードキャストによる機器検索要求を送信し，端末 A を発見できるかどうか確認

この結果，手順 4 の端末 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エントリを維持できず GTK 更新が発生することが判明した．ゆえに，接続済みの端末が一定期間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 更新の発生をすみやかに検知し新しい GTK の入手を可能とすることで，課題を解決できる手法を検討することにした．

3.1　GTK 更新発生検知のロジック

端末が GTK を使用するのは暗号化されたパケット受信時の復号化のときのみである．そのため，端末が GTK 更新の発生，すなわち自身の GTK が古くなっていることを検知するためには，ブロードキャストあるいはマルチキャストで受信した暗号化されたパケットを自身の GTK で復号化できるかどうかで判断しなければならない．復号化できない場合，自身の GTK が古いと判断すればよい．しかし，暗号化されたパケットを復号化できたかどうかの明確な判断はアプリケーションレイヤでは困難である．なぜなら実際に暗号化/復号化を行う下位レイヤの通信ライブラリにおいては，ブロードキャスト/マルチキャストで受信したパケットを自身の GTK で復号化に失敗した場合，復号したデータは解読不能であるためデータを破棄し，上位レイヤのアプリケーションにそのデータを渡すことができないためである．ゆえに上位レイヤのアプリケーションにおいて，受信すべきデータを受信すべきタイミングで受信できない場合に，自身の GTK による復号に失敗したと判断すればよいと考えた．この受信すべきタイミングに関しては，定期的に GTK で暗号化されたパケットを受信させる仕組みを実装すればよいと考えた．

以上をふまえて，端末が中継機の GTK 更新の発生をすみやかに検知し新しい GTK の入手を可能とするロジックとして下記を考案した．

(1) 端末が定期的に GTK で暗号化されたパケットを受信できるような仕組みを実装する（**図 12** の①）．
(2) アプリケーションで定期的に受信していた（すなわち復号化できていた）パケットが受信できなった場合，自身の GTK により復号化に失敗した（すなわち自身の保有する GTK が古くなった）と判断する（図 12 の②）
(3) GTK が古くなったと判断した場合，無線をいったん切断後，再度中継機に無線接続して 4-way handshake により新しい GTK を取得する（図 12 の③）．

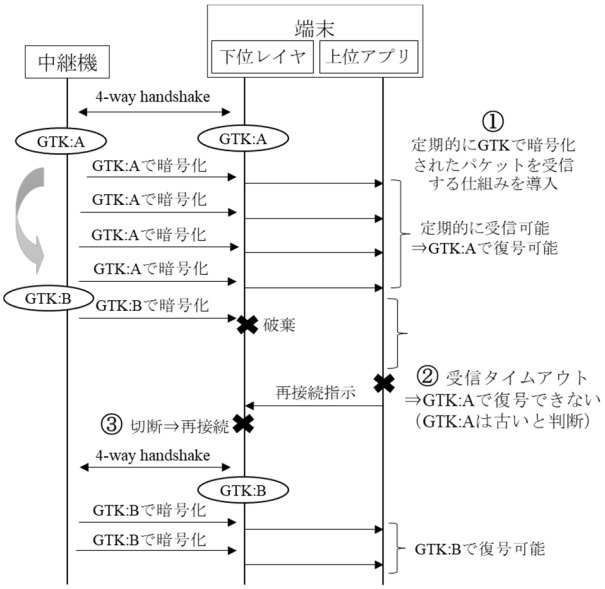


図 12　提案手法のロジック
Fig. 12　Logic of the proposed method.

上記により，ネットワーク内のほかの端末が一定期間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，つまり課題発生の原因 (1) が発生したとしても，課題の発生を防ぎ相互接続不能になることを回避可能である．

3.2　実環境における実装案検討

実環境において，提案手法を実現する方法を検討する．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，たと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．そこで，自端末にネットワークインタフェース（以降 I/F と呼ぶ）を 2 つ以上搭載させれば，一方の I/F から他方の I/F 宛（たとえば，有線 LAN 側 I/F から無線 LAN 側 I/F 宛や，無線 2.4 GHz 側 I/F から無線 5 GHz 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し対処することが可能であると考えた．この方法は比較的容易に実装可能と考えられるが，実際にはいずれか一方の I/F しか有効にできない端末が多い．また，特に白物家電などスペックが低い端末はそもそも I/F を複数持っていないことが多く，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

© 2020 Information Processing Society of Japan

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方法を検討した．

(1)　**UPnP を利用する方法**

市販のルータにはほぼ必ず UPnP（Universal Plug and Play [5]）の IGD（Internet Gateway Device）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様々であり，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 を利用する方法**

ルータに必ず搭載されている DHCP（Dynamic Host Configuration Protocol [6]）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，提案手法として DHCP を用いることとする．

3.3　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ととした．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る．メッセージ内の「broadcast flag」を「True（broadcast)」に設定して送信することにより，ルータに対して応答の 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，5 章で後述する図 16 に示すとおり，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 分間隔とした．

ここで, 1 分間隔でブロードキャスト送信する T2 Request のネットワーク全体へのトラフィック負荷を考察する．

T2 Request メッセージのサイズは約 350 byte（= 2,800 bits）である．またこの T2 Request に付随してルータから Ack が返信されるが，この Ack のメッセージサイズは約 330 byte（= 2,640 bits）である．それを 1 分間に 1 回送信するので, 仮にネットワークのトラフィックを 1 分間監視した場合，トラフィックはそれぞれ 2,800 bits/2,640 bits となる．**表 5** は一般的に普及しているネットワークサービスの通信レートと，そこから 1 分間のトラフィックを計算したものを示したものである．表 5 より，1 分間隔で T2 Request メッセージをブロードキャスト送信することは，

表 5　様々なネットワークサービスの通信レート
Table 5　Communication rate of various network services.

ネットワークサービス	画質/音質	通信レート	1 分間のトラフィック
YouTube[7]	SD(360p) 〜 HD(1080p)	0.7Mbps 〜 5Mbps	42Mbits 〜 300Mbits
	4k	20Mbps	1200Mbits
Hulu[8]	-	3Mbps 〜 6Mbps	180Mbits 〜 360Mbits
U-NEXT[9]	標準〜高画質	1.5Mbps 〜 3Mbps	90Mbits 〜 180Mbits
	4k	15Mbps	900Mbits
Netflix[10]	SD〜UHD(4k)	3Mbps 〜 25Mbps	180Mbits 〜 1500Mbits
Amazon Prime Video [11]	SD〜HD	0.9Mbps 〜 3.5Mbps	54Mbits 〜 210Mbits
Amazon Prime Music [12]	低音質〜高音質	-	0.9M 〜 4Mbits
DHCP T2 Request	-	-	2800bits
DHCP Ack	-	-	2642bits

4 K 動画ストリーミングサービス（Netflix）と比較すると約 53 万分の 1 程度，また低音質の音楽ストリーミングサービス（Amazon Prime Music）と比較しても約 320 分の 1 程度のトラフィックであることが分かる．よって本手法の実施によるネットワーク全体への負荷は小さいと考える．

また別の観点から，複数台の端末が提案手法を実装した場合の家庭内のネットワークトラフィックへの影響を，例として図 2 を用いて考察する．図 2 において，ネットワークの構成要素の中心であるルータの無線帯域を利用するのは，端末 1 と，中継機配下の端末 2 および端末 3 の合計 3 台と見なすことができるため，これら 3 台の端末が提案手法を実装していると想定した場合の，ルータの無線 LAN 速度に占める割合（帯域使用率）を算出する．国内ルータメーカの製品カタログ [13] には「家族の人数 × 1 人あたりの想定使用端末数」に適したスループット（無線 LAN 速度）を搭載したルータ（以降，推奨ルータと呼ぶ）が掲載されているためこれを参考とする．

このカタログでは，端末が 3 台の場合の推奨ルータの無線 LAN 速度は 300 Mbps である．提案手法において送信する T2 Request および Ack のメッセージサイズの合計は 5,442 bits であり，3 台の端末が同時に T2 Request を送信するタイミングが発生したとすると，最大 16,326 bits のデータを同時送信することとなる．その場合に推奨ルータの無線 LAN 速度 300 Mbps に対する帯域使用率は理論値として 0.005%となる．

同様の方法で，家庭内の端末台数に応じて提案手法の帯域使用率を算出したものを**表 6** に示す．ここで総務省統計局による 2018 年度の日本の統計 [14] によると，1 世帯あ

© 2020 Information Processing Society of Japan

表 6　提案手法の無線 LAN 帯域使用率
Table 6　Wireless LAN bandwidth usage rate of the proposed method.

家族の人数	家庭内の端末数	推奨ルータの無線 LAN 速度 (理論値)	提案手法のデータ量	提案手法の帯域使用率
1 人	3 台	300 Mbps	16326 bits	0.005%
2 人	6 台	1166 Mbps	32652 bits	0.003%
2.33 人	6.99 台	1166 Mbps	38039.6 bits	0.003%
4 人	12 台	1166 Mbps	65304 bits	0.006%
6 人	18 台	2533 Mbps	97956 bits	0.004%

たりの人員は 2.33 人という統計結果が出ており，この場合の推奨ルータの無線 LAN 速度は 1,166 Mbps と考えられるため，提案手法の帯域使用率は理論値として 0.003%となる．以上より，本手法の実施によるネットワーク全体への負荷は十分小さいと考える．

ここで，通常は無線ルータに DHCP サーバが搭載されており，T2 Request に対して Ack が返らないことはすなわち GTK 更新が発生して Ack を復号できないこととととらえて問題ないが，ホームネットワークの構成によっては，DHCP サーバが搭載されたルータに無線アクセスポイントを接続している構成も考えられる．その場合に T2 Request に応答が返らないという状況は単に Ack を復号できないという場合だけでなく，ルータが電源オフ状態となりネットワーク上に DHCP サーバが存在しなくなった場合も考えられる．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うことにした．ユニキャストパケットとして Ping Request を用いた．

これらをふまえて，課題を解決する手法として下記を提案する．

1. 端末からルータに定期的に DHCP T2 Request（ブロードキャスト）を送信する．
   ただしこのとき，DHCP メッセージ内の「broadcast flag」を「True（broadcast）」に設定して送信する（**図 13** 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 13 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 13 の③）．

ここで，実際にプログラムを実装する端末のソフトウェアスタック図を**図 14** に示す．wpa_supplicant は，各種 Linux，Windows，その他 OS 向けにフリーで提供されている WPA/WPA2 対応無線クライアント機能のパッケージである．

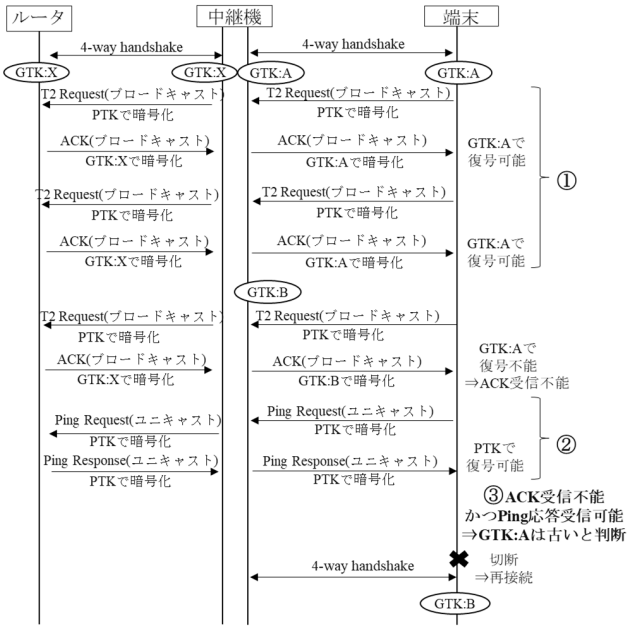


図 13　提案手法のシーケンス
Fig. 13　Sequence of the proposed method.

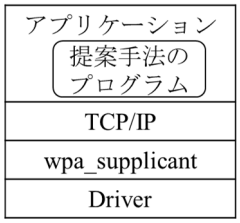


図 14　端末ソフトウェアスタック
Fig. 14　Software stack of terminal.

4. 実験

提案手法により，中継機の GTK 更新が発生した場合に端末がそれを検知し，中継機から新しい GTK を再取得することで課題を解決でき，また相互接続性を確保できることを実験を通じて確認した．また提案手法が，GTK 更新が発生しない中継機配下におけるブロードキャスト通信に影響を及ぼさないこともあわせて確認した．

4.1 実験環境

実験環境として，中継機の GTK 更新が必ず発生する環境を構築するため，表 4 に示した課題が発生する中継機 7 機種（シェア合計 6.1%）を使用し，**図 15** の構成となるよう各機器を接続した．また，GTK 更新が発生しない環境を構築するため，表 4 に示した課題が発生しない中継機 10 機種（シェア合計 20%）を選定し，図 15 の構成となるよう各機器を接続した．各機器（ルータ，端末，中継機）のスペックを**表 7** に示す．端末 B は，市販の無線製品（ス

© 2020 Information Processing Society of Japan

図 15　調査手順
Fig. 15　Experiment configuration.

表 7　各機器のスペック
Table 7　Specification of each device.

ルータ	無線対応規格	802.11ac/n/a(5GHz 帯) 802.11n/g/b(2.4GHz 帯)
	ストリーム数	2 ストリーム
	アンテナ数	2x2(5GHz 帯&2.4GHz 帯)
	伝送速度(規格値)	867Mbps(11ac/5GHz 帯)＋ 300Mbps(11n/2.4GHz 帯)
端末 A	OS	Fedora 20
	CPU	2.40GHz
	無線対応規格	802.11ac/n/a(5GHz 帯) 802.11n/g/b(2.4GHz 帯)
	最大通信速度	受信時 450Mbps
端末 B	OS	Android9.0
	CPU	2.8GHz + 1.7GHz
	無線対応規格	802.11ac/n/a(5GHz 帯) 802.11n/g/b(2.4GHz 帯)
	最大通信速度	受信時 1083Mbps
課題あり中継機	無線対応規格: 11ac/n/a(5GHz 帯) 11n/g/b(2.4GHz 帯)	最大通信速度:1750Mbps(4 台)
		最大通信速度:1900Mbps(3 台)
課題なし中継機	無線対応規格: 11ac/n/a(5GHz 帯) 11n/g/b(2.4GHz 帯)	最大通信速度:2533Mbps(1 台)
		最大通信速度:1166Mbps(7 台)
		最大通信速度:600Mbps(1 台)
	無線対応規格: 11n/g/b(2.4GHz 帯)	最大通信速度:300Mbps(1 台)

マートフォン）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 2.3 節の調査環境と同じ「30 分」とした．端末 A（ノート PC）には 3.3 節の提案手法を実行する実験ツールをインストールした．ここで開発した実験ツールに関して，通常は図 14 で実装されることが理想的であるが，今回の実装においては，DHCP の Request に対して応答を得られないことにより GTK 更新を検知する機能を確認することが目的であり，実験の容易さおよび正確さを考慮し，無線の切断/接続に関しては手動にて行うこととした．

4.2　実験方法

(1)　**提案手法の効果確認**

まず，課題が必ず発生する実験環境において，提案手法を実行する端末 A が中継機の GTK 更新を検知し新しい GTK を取得することにより，課題を解決できることを下記手順にて確認した．

1-1. ルータ・中継機・各端末を起動し無線接続
1-2. 端末 A で評価ツールの実行を開始
1-3. 端末 B を電源オフし，X 分後電源オンする
1-4. 端末 B の GTK が更新されていることを確認
1-5. 端末 A において中継機の GTK 更新を検知し，無線の再接続により新しい GTK を取得することを確認
1-6. 端末 B からブロードキャストによる機器検索要求を送信し，端末 A を発見できるかどうか確認

また手順 3 の X を変化させることにより，課題が発生する中継機 7 機種のテーブル有効期限も調査した．

(2)　**提案手法の影響度確認**

次に，課題が発生しない実験環境において，端末 A が提案手法を実行し続けてもブロードキャスト通信に影響を及ぼさないことを下記手順にて確認した．

2-1. ルータ・中継機・各端末を起動し無線接続
2-2. 端末 A で評価ツールの実行を開始
2-3. 端末 B を電源オフし，30 分後電源オンする
2-4. 端末 B の GTK が更新されていないことを確認
2-5. 端末 B からブロードキャストによる機器検索要求を送信し，端末 A を発見できるかどうか確認

4.3　実験結果

4.2 節の実験 (1) の実験ログを実験結果として**表 8** に示す．表 8 には，手順 1-1 において起動後に端末 A，端末 B が取得した GTK，手順 1-4 において再接続時に端末 B が取得した GTK，および手順 1-5 において端末 A の再接続時に取得した GTK をまとめている．また手順 1-6 で端末 B がブロードキャストの機器検索要求送信により端末 A を発見できたことを「○」で示している．表 8 より，表 4 に示した課題が発生する中継機 7 機種（シェア合計 6.1%）すべてにおいて，手順 1-4 で端末 B が再接続したタイミングで GTK が更新され端末 A と端末 B 間で GTK 不一致が発生したが，手順 1-5 で GTK 更新を検知した端末 A が再接続を行うことにより端末 B と同じ GTK を取得できること，すなわち課題が解決できることが分かった．さらにその後の手順 1-6 において，端末 B からブロードキャストによる機器検索要求を送信し，端末 A を発見できること，すなわち市場問題を解決できることが分かった．

次に，4.2 節の実験 (2) の実験ログを実験結果として表 9 に示す．**表 9** には，手順 2-1 において起動後に端末 A，端末 B が取得した GTK と，手順 2-4 において再接続時に端末 B が取得した GTK をまとめている．また手順 2-5 で

© 2020 Information Processing Society of Japan

表 8　提案手法の効果確認結果
Table 8　Result of confirming effect of proposed method.

中継機	各手順における GTK		1-6
1	1-1	6ce64f4a97dce3b0179ce53c424ec2d1	○
	1-4	a7e83b3d91fb47dcc9127574c2fe766e	
	1-5	a7e83b3d91fb47dcc9127574c2fe766e	
2	1-1	c90c6e5c8f8697b1e51cfdcffc7fb913	○
	1-4	c7a7bf76576d73109482dc2ba485a55f	
	1-5	c7a7bf76576d73109482dc2ba485a55f	
3	1-1	8f574e2e2bed4fdf76912021a4a69b9b	○
	1-4	017087deaaae751053edc65f4fa4ad94	
	1-5	017087deaaae751053edc65f4fa4ad94	
4	1-1	769062565fa4b53b3cde395dc21fa473	○
	1-4	d51d114839c18ec0d5af6de62bfdceb3	
	1-5	d51d114839c18ec0d5af6de62bfdceb3	
5	1-1	6ae11a9e6cc63882c5f6a76a853137de	○
	1-4	fbe094aba710a2d8fbcf0e7a1bc2f8db	
	1-5	fbe094aba710a2d8fbcf0e7a1bc2f8db	
6	1-1	890d227a4abf414ea06f09d2d2b31701	○
	1-4	07226f3b9c131d296621d147bf3e4386	
	1-5	07226f3b9c131d296621d147bf3e4386	
7	1-1	b5e187990e8f77ff67d18c3733d4269f	○
	1-4	34bad21415b8b6ff58edc0ebf6af8bc4	
	1-5	34bad21415b8b6ff58edc0ebf6af8bc4	

端末 B がブロードキャストの機器検索要求送信により端末 A を発見できたことを「○」で示している．表 9 より，表 4 に示した課題が発生しない中継機 10 機種（シェア合計 20%）すべてにおいて，端末 A が 30 分間提案手法を実行し続けても，その後の手順 2-5 において，端末 B からブロードキャストによる機器検索要求を送信し，端末 A を発見できること，すなわち提案手法がブロードキャスト通信に影響を及ぼさないことを確認できた．

また，実験 (1) により判明した各中継機のテーブル有効期限を**表 10** に示す．

表 10 より，中継機のテーブル有効期限は無線のチップベンダの実装仕様により異なることが分かった．今回の 2.3 節の調査ではルータの GTK 更新間隔 30 分および端末の切断期間 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．つまり 2.3 節の調査では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，組み合せるルータ

表 9　提案手法の影響確認結果
Table 9　Results of confirming the impact of proposed method.

中継機	各手順における GTK		2-5
1	2-1	640bc271bb1f9f7cb365995511d88fe2	○
	2-4	640bc271bb1f9f7cb365995511d88fe2	
2	2-1	745b5b10c44d6124bcd689d1acccc6af	○
	2-4	745b5b10c44d6124bcd689d1acccc6af	
3	2-1	6a9557de174ae76d10adc6ba283c81ca	○
	2-4	6a9557de174ae76d10adc6ba283c81ca	
4	2-1	5644bfef9ce19f8119ddc680f9853d93	○
	2-4	5644bfef9ce19f8119ddc680f9853d93	
5	2-1	3fe6f6525db89cd89a6dbee31b42418b	○
	2-4	3fe6f6525db89cd89a6dbee31b42418b	
6	2-1	896fdd9e8a030c41b2ec01d353504ef7	○
	2-4	896fdd9e8a030c41b2ec01d353504ef7	
7	2-1	810120ac3c565dead3d9b01d96960443	○
	2-4	810120ac3c565dead3d9b01d96960443	
8	2-1	e62e520232be34fd136991f14bdcdc32	○
	2-4	e62e520232be34fd136991f14bdcdc32	
9	2-1	bf5de523dabbdd1439e580dc27597d56	○
	2-4	bf5de523dabbdd1439e580dc27597d56	
10	2-1	3891225aa3c4a263bac4934396d8df3e	○
	2-4	3891225aa3c4a263bac4934396d8df3e	

表 10　中継機のテーブル有効期限調査の結果
Table 10　Result of the table valid term.

有効期限	機種数	シェア合計
約 12 分	1 機種	2.1%
約 20 分	3 機種	2.4%
約 22 分	2 機種	1.0%
約 25 分	1 機種	0.6%

の GTK 更新間隔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，その場合でも本手法により問題なく課題は解決でき，端末間の相互接続性を確保できる．

5. 考察

ルータの設定変更による課題解決手法についても検討を行った．2.2 節の考察に基づき，ルータの GTK 更新間隔をテーブル有効期限内に設定することにより，中継機の管理テーブルのエントリは維持され GTK 更新が発生しないため課題は解決可能である．つまり，表 2 において 11 分 30 秒までは課題が発生しないことを確認できているため，

© 2020 Information Processing Society of Japan

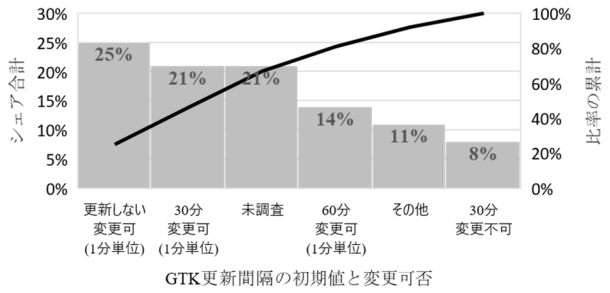


図 16　GTK 更新間隔の初期値と変更可否
Fig. 16　Sequence of the Experiment tool.

本論文では 11 分 30 秒以内に設定することを提案する．そこで 2.3 節の調査で用いたルータ 90 機種に対して GTK 更新の設定仕様を調査した．調査結果を図 16 に示す．

図 16 より，GTK 更新間隔の初期値と設定変更の可否の組合せで一番多かったのは「更新なし/変更可（1 分単位）」（シェア合計 25%）であり，続いて「30 分/変更可（1 分単位）」（シェア合計 21%），「60 分/変更可（1 分単位）」（シェア合計 14%）であった．これら合計 60%は中継機の課題が発生する可能性はあるものの，ユーザが GTK 更新間隔を 11 分 30 秒以下に設定すれば課題は解決可能である．

しかしながら，残りの 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．つまりルータの GTK 更新間隔を 11 分 30 秒以内に設定変更できない可能性があり，その場合課題が発生する中継機の管理テーブルのエントリを維持することができない．そのため，ルータの設定変更による課題解決手法だけでは不十分であるといえる．

6. 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．たとえば，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 [15]．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あ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 [16], [17]．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，このとき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や [18]，暗号鍵を定期更新・不定期更新することにより暗号鍵の漏洩を防止する管理サーバを用いた鍵の配布・共有方式がある [19]．前者の手法では，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．また後者の手法を用いたシステムにおいては，すべての端末に更新された暗号鍵が届いていない場合においても，端末間で新しい鍵を転送することにより鍵の同期を実現することが可能である．しかしながら，いずれにおいても，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，これらの手法は適用できない．

7. まとめと今後の展開

本論文では，仕様の解釈の違いによって引き起こされる中継機の相互接続性問題に関し，解釈の違いが発生する原因を調査し明らかにした．また端末側の実装で端末間の GTK が不一致となる課題を解決し，相互接続性を確保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 機種のうち，提案手法導入前は 50 機種のルータでしか相互接続ができていなかったが，提案手法導入することにより全 57 機種に関して相互接続性を確保することができた．

GTK 不一致による相互接続性問題が発生する原因は，そもそも標準規格である IEEE 802.11i において，GTK の更新条件や GTK 更新通知を行うタイミング，また端末切断時のアクセスポイント側の GTK の取り扱い方に関して明確に規定されていないことによるものであり，メーカの開発者の仕様の解釈の違いによって実装仕様に違いが生じるのはやむを得ないことではあるが，その仕様を変更すると市場規模での混乱が想定されるため，端末側の仕様を策定しその効果を示した．もちろん中継機を実装するルータメーカへ仕様改善の提案を行っていくことは重要であるため今後対応を検討していく．またそもそも開発者の仕様の解釈に違いが出ないように標準規格の改訂を行うことも課題解決に有効なアプローチであると考える．今後は標準規格団体にも仕様改善提案を行うよう対応を検討していきたい．

またルータ側の設定変更による解決手法も検討したが，市場のルータの 60%までしか解決できないことが分かった．

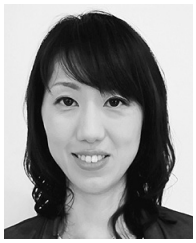
以上のことから，端末側での対処が社会に最も影響が少なく対処できると考え，本論文の提案手法をエコーネットコンソーシアムに提案した．その結果 ECHONET Lite 製品の相互接続性を向上させる手法であると認められ，“ECHONET Lite システム設計指針 [2]” に採択された．

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，今後は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，さらなる改善仕様の検討を進める予定である．

© 2020 Information Processing Society of Japan

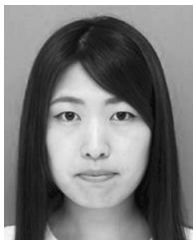
参考文献

[1] GfK, 生活家電の POS トラッキング調査, 入手先 ⟨http://www.gfk.com/jp/industries/consumer-goods/home-appliances/⟩.
[2] Wi-Fi Alliance: Security, available from ⟨https://www.wi-fi.org/discover-wi-fi/security⟩.
[3] IEEE Std 802.11i, available from ⟨https://ieeexplore.ieee.org/document/1318903⟩.
[4] ECHONET Lite 規格 Ver.1.12 第 2 部, 入手先 ⟨https://echonet.jp/wp/wp-content/uploads/pdf/General/Standard/ECHONET_lite_V1_12_jp/ECHONET-Lite_Ver.1.12_02.pdf⟩.
[5] UPnP-arch-DeviceArchitecture-v2.0-20150220.pdf, available from ⟨https://openconnectivity.org/developer/specifications/upnp-resources/upnp⟩.
[6] RFC 2131, Dynamic Host Configuration Protocol, available from ⟨https://www.ietf.org/rfc/rfc2131.txt⟩.
[7] Google：YouTube ヘルプ-システム要件, 入手先 ⟨https://support.google.com/youtube/answer/78358?hl=ja⟩.
[8] Hulu：ヘルプセンター-コンテンツ／サービスについて, 入手先 ⟨https://help.happyon.jp/faq/show/1882?site_domain=jp⟩.
[9] U-NEXT：ヘルプセンター-推奨の回線速度を知りたい, 入手先 ⟨https://help.unext.jp/guide/detail/recommended-line-speed⟩.
[10] Netflix：ヘルプセンター-推奨されるインターネット接続速度, 入手先 ⟨https://help.netflix.com/ja/node/306⟩.
[11] Amazon：ヘルプ&カスタマーサービス-コンピューターでのストリーミング再生のシステム要件, 入手先 ⟨https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=201422810⟩.
[12] NetSetsu：AmazonMusic のデータ通信量と 1 GB までの目安や節約方法, 入手先 ⟨https://net-torisetsu.jp/amazonmusic-traffic/⟩.
[13] BUFFALO：スマホ・テレビ・パソコン周辺機器カタログ 2019 夏 Vol.222, 入手先 ⟨https://www.buffalo.jp/support/other/__icsFiles/afieldfile/2019/06/11/vol222.pdf⟩.
[14] 総務省統計局：日本の統計 2018, 2-11 都道府県, 世帯人員別一般世帯数と世帯の種類別世帯人員 (平成 27 年), 入手先 ⟨https://www.stat.go.jp/data/nihon/pdf/18nihon.pdf⟩.
[15] 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, pp.113–116 (2003).
[16] Burmester, M.V.D. and Desmedt, Y.: A secure and efficient conference key distribution system, Advances in Cryptology – *EUROCRYPT'94*, pp.275–286 (1995).
[17] 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).
[18] 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, Vol.2005-DSM-39, No.9, pp.49–54 (2005).
[19] 辻　宏郷, 米田　健, 水野忠則, 西垣正勝：放送型高頻度鍵更新方式による超広域モバイル環境向けセキュアリアルタイム通信の実現, 情報処理学会論文誌, Vol.50, No.9, pp.2103–2117 (Sep. 2009).
[20] エコーネットコンソーシアム：ECHONET Lite システム設計指針, 第 2 版, 2.12 無線 LAN ネットワークに関する注意事項 (2019).



濱本 望絵　（正会員）

2001 年九州工業大学大学院工学研究科博士前期課程修了．同年松下電器産業株式会社（現，パナソニック株式会社）に入社．以来，UPnP や DLNA 等のホームネットワーク技術や NAT 越えによる P2P 接続技術を用いた方式・システムの研究開発，および IoT 機器の相互接続性向上の取り組みに従事．



土屋 薫子

2015 年東京理科大学理工学部電気電子情報工学科卒業．同年パナソニック株式会社に入社．家電製品を対象とした相互接続性向上の取り組みに従事．現在，メディアエンターテインメント事業部で企画を担当．

石川 博一

1998 年信州大学大学院工学系研究科電気電子工学専攻博士前期課程修了．同年松下電器産業株式会社（現，パナソニック株式会社）に入社．ホームネットワークシステムに関する研究開発，標準化活動，およびネットワーク機器の相互接続性向上に関する取り組みに従事．2012 年より，一般社団法人エコーネットコンソーシアム規格認証 WG 主査．

村上 隆史　（正会員）

1999 年東京大学工学部電子工学科卒業．同年松下電器産業株式会社（現，パナソニック株式会社）に入社．以来，白物家電，設備系家電，センサ系，AV 家電等を対象とした様々なホームネットワークシステムに関する研究開発，標準化活動に従事．2006 年より，一般社団法人エコーネットコンソーシム技術委員長．博士（工学）．

© 2020 Information Processing Society of Japan

杉村 博　（正会員）

2012 年神奈川工科大学大学院情報工学専攻博士後期課程修了．2012 年同大学スマートハウス研究センター特別研究員．2013 年同大学創造工学部ホームエレクトロニクス開発学科助教．2016 年准教授．博士（工学）．

森 信一郎　（正会員）

1987 年関西大学工学部卒業．同年富士通株式会社入社．2003 年株式会社富士通研究所，2016 年千葉工業大学先進工学部教授．博士（情報学）．ユビキタスコンピューティング，携帯端末による測位技術に関する研究に従事．

一色 正男　（正会員）

1982 年東京工業大学大学院理工学研究科修了．2009 年慶應義塾大学教授，2012 年より神奈川工科大学教授，スマートハウス研究センター所長．（株）東芝で約 30 年勤務．博士（工学）．情報処理学会 CDS 研究会幹事（2010～2012 年）．機械学会会員，ECHONET コンソーシアム 2008 運営委員長，現フェロー．W3C Site Manager（2009～2014 年）．経済産業省 HEMS タスクフォース座長．HEMS 認証支援センター長．本会シニア会員．本会フェロー．

© 2020 Information Processing Society of Japan