Ellisys Expert Note | EEN_BT01
Rev. B

Bluetooth トラフィックの正しい解析方法

複雑なトポロジーのデバッグについて

スニッファの概要

当社のすべてのBluetoothアナライザ製品で使用されている記録手法である、広帯域、または広帯域を対象としたスニッファとは何を意味するのかという質問をよく受けます。このEllisysエキスパートノートでは、EllisysのBluetoothアナライザがこの技術を使ってどのようにBluetoothトラフィックを記録しているかをわかりやすく説明しています。広帯域のスニッファ技術を簡単に説明すると、すべてのBluetoothチャネル（BR/EDRおよびBluetooth LE）を非同期かつ同時に記録する機能です。この手法は、ホッピングするチャネルを監視するにあたっての欠点を解消します。

ホッピング同期型装置

Bluetooth開発者に広帯域同時記録型の装置を紹介する前は、Bluetoothが周波数ホッピング、ホワイトニング、プライバシー、暗号化などの高度な通信技術が使われているため、トラフィックを捕捉することは困難でした。Bluetoothはセキュリティ上の理由から監視することが難しいように設計されています。

Bluetooth機器は、ピコネットの接続時に定義されたホッピングシーケンスに従って、40（Bluetooth LE）から79（BR/EDR）のチャンネルをランダムに使用します。このため、Bluetoothの通信を監視することは困難であり、分析、特性評価、トラブルシューティングは、より難易度の高いものとなっていました。

私たちが広帯域型のアプローチを導入する前は、ホッピング同期型のアプローチが最も一般的なスニッファであり、Bluetoothが登場してから市場に投入されたすべてのスニッファが採用していました。ホッピング同期型の装置は、特定のホッピングシーケンスをターゲットに同期を行い、同期が成功した後にのみパケットを記録します。この種の監視装置にはいくつかの固有の制限があり、使用が難しく、信頼性が低く、限られた状況でしか使用できません。

図1に示すように、この監視手法では、利用可能なチャネルのうち1つだけを記録していました。例えば、Bluetoothデバイスは625µsごとに異なるチャネルを使用するため、この監視手法では、特定のピコネットからのパケットを捕捉するために、いつ、どこで、どのチャネルを記録するべきかを正確に知る必要がありました。

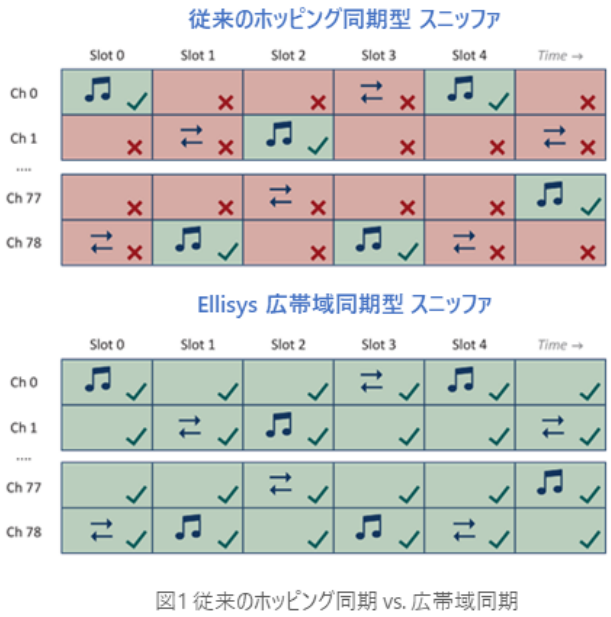

図1 従来のホッピング同期 vs. 広帯域同期

ホッピング同期型の方式は、標準的な無線チップと特定のファームウェアを利用しているため、標準的なBluetoothデバイスと同様に動作します。ホッピング同期型の装置は、選択したピコネットのホッピングシーケンスに従い、各スロットのパケットを記録します。そのため、パケットを記録する前に、対象となるピコネットとの同期が必要です。ホッピング同期型の装置は、他のデバイスと同様にこの同期を管理し、IDパケットを送信してピコネットのマスターに対しページングを行っていました。

マスターはこれらのパケットを見ると、それに応じてFHSパケットを送信します。FHSパケットには、マスターに同期するための情報と、マスターのホッピングシーケンスを追うための情報が含まれています。この時点から、ホッピング同期型の装置は、このピコネットからのパケットを受信することができます。しかし、このホッピングを同期する手法は、広帯域を監視する方法に比べて、非常に制限が大きなものでした。

> ヒント: ホッピング同期型の装置は、特定のホッピングシーケンスに積極的に同期しようとし、同期が成功した後にのみパケットをキャプチャします。広帯域同時記録型の装置は、シンプルかつ強力な手法で、いくつかのチャネルだけを記録するのではなく、すべてのチャンネルを同時に記録します。

広帯域スニッファ

もちろん、もうお分かりだと思いますが、Bluetooth通信を監視するもっと効果的で実用的な方法は、広帯域を同時に記録できるスニッファを使って、すべてのBluetoothチャンネルを同時に観測することです。このような監視装置は、ホッピングシーケンスを追いかけるのではなく、**すべてのチャンネルを確認し、**いずれかのチャンネルでパケットが送信されると、すぐにそれを記録します。監視装置のハードウェアはピコネットを気にする必要がなくなり、**何の設定もせずに、ステートレスにあらゆるトラフィックを捕捉する**ことができます。　膨大な数の非常に複雑な情報群は、高速で洗練されたソフトウェアによって管理されます。

図2は、Ellisysの広帯域監視装置で捕捉された複数のピコネットを含むパケットを示したもので、Piconetウィンドウを使用しています。

このような高度な技術は、標準的なBluetooth無線チップでは実現できません。いくつかのチャンネルだけでなく、すべてのチャンネルを同時に記録します。

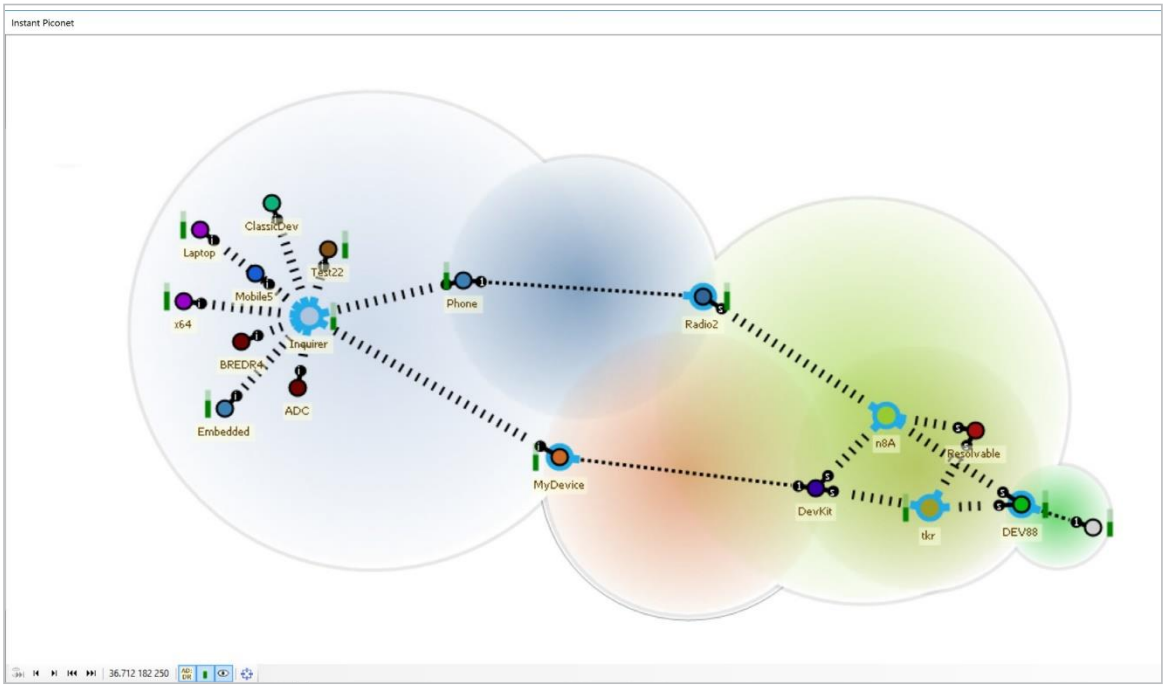

図2 Instant Piconetの特徴

ヒント: Ellisysの広帯域同時記録装置は、近くにあるすべてのBluetoothピコネット、スキャタネット、およびメッシュなどのトポロジーを、何の設定もなく、また一切の干渉無しに確認することができます。

広帯域監視装置の利点

このアプローチを採用することは、Ellisysアナライザを特に**将来性のあるもの**にするという点で、非常に意義があります。Bluetooth技術は、様々な方向に、驚くほどのスピードで進化しています。新しいページング技術、ベースバンドの改良、 セキュリティの強化、プロトコルやプロファイルの追加、その他の新機能などを、ハードウェアを一切変更することなく、ソフトウェアのアップデートだけで対応できます。これにより、ハードウェアの寿命が長くなり、お客様のコスト削減と利便性の向上につながります。

広帯域スニッフィングのもう一つの大きな利点は、**非同期のトラフィックを問題なく記録できること**です（**図3**参照）。

ページングや問い合わせを完璧に記録できます。この記録方法は、ロールスイッチ、ホッピング シーケンス（AFH: Adaptive Frequency Hopping)、ページングの状況などに影響されません。**タイムスロットの前、あるいは後にパケットが送信されたとしても、それは記録されます。**

ヒント: Ellisysのアナライザソフトウェアは、HCI上で交換されたリンクキーを自動的に抽出し、それを使用して無線トラフィックを一切の操作なしで復号化します。

広帯域の記録を行っても、精度125nsのタイムスタンプを付加して正確に記録します。超高精度で温度が安定化された内部オシレーターにより、様々なデバイス間の測定を行う際の完璧なリファレンスとなります。

このアプローチは、暗号化された接続を記録する際にも新しい可能性をもたらしました。Ellisysの広帯域監視装置は、Bluetoothトラフィックを解釈する必要がないため、暗号化されたトラフィックを記録し、すぐに、または後処理で復号化することもできます。

これにより、ホッピング同期型の装置では不可能な、PINコードの自動判定、SSPデバッグモードデバイスの自動記録、SSPペアリングの記録、そして記録後のリンクキー入力による100%のトラフィック復号化が可能になりました。

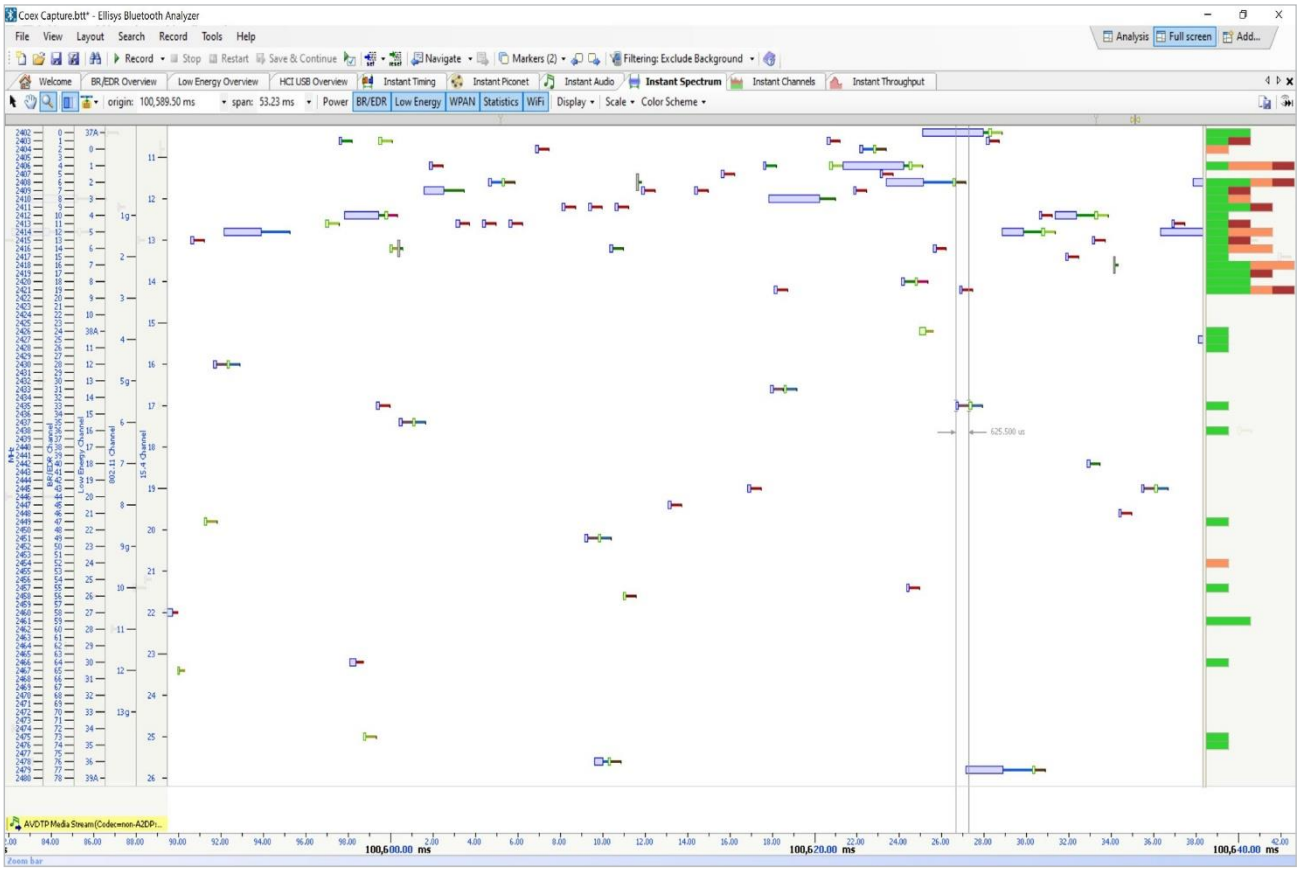

図3 Instant Spectrumの特徴

最後に、この監視装置手法は、単一のピコネットだけでなく、**近隣のすべてのピコネットやスキャタネット**を捕捉することができます。複雑なトポロジーのデバッグは、ユースケースが単純なポイント・ツー・ポイントの接続から、Bluetooth meshのようなマルチプロファイルの複雑なトポロジーへと着実に進化しているため、ますます重要になってきています。

おわりに

広帯域スニッフィングは、これまで不可能だったBluetoothのデバッグや相互運用性のテストを可能にします。広帯域スニッフィングは、よりエレガントなアプローチを提供し、ユーザーはすべてのパケットを即座に記録し、Ellisysアナライザソフトウェアアプリケーションの強力なフィルタリングを使用して、潜在的な問題を調査することができます。

詳細はellisys.comをご覧いただくか、es@gailogic.co.jp までご連絡ください。

本文書について

本文書は、" EEN_BT01 - Capturing Bluetooth Traffic, the Right Way (Rev. B Updated 2021-09)" を翻訳したものです。原文、本文書及び Ellisys 製品に関するお問い合わせは、Ellisys 日本総代理店 ガイロジック株式会社 (0422-26-8211, es@gailogic.co.jp) までご連絡ください。
その他の翻訳版エキスパートノートは、https://www.gailogic.co.jp/db/bt/expert_notes をご覧ください。

その他の関連資料

- EEN_BT03J- はじめての広帯域記録
- EEN_BT06J- Bluetooth セキュリティのウソ？ホント？

Bluetoothプロトコル・アナライザ販売窓口　(ガイロジック株式会社)

042-26-8211　　es@gailogic.co.jp　　https://www.gailogic.co.jp/db/bt