Illumi Packet: 通信パケットを可視化するLANケーブル

麻生 航平[1,a)]　小池 英樹[1,b)]

概要：コンピュータネットワークの通信において，どのようにパケットがやり取りされているのかを見ることはできないため，これまで様々なパケットの可視化手法が提案されてきた．しかし，それらはネットワーク構成を画面上に仮想的に描画される場合がほとんどである．本研究では，実世界の LAN ケーブルそのものに，通過したパケットを可視化する手法を提案する．パケットの種類と方向に応じてリアルタイムで LAN ケーブルが発光するため，コンピュータの操作内容と発生するパケットの種類との対応がとれる．パケットの存在をより身近にさせることができ，直感的なネットワークの理解を促進する．

1. はじめに

コンピュータネットワークの通信は，幾種類ものパケットが階層化されたプロトコルによって情報伝達し合うことによって実現されている．その仕組みは，複雑かつ不明瞭であるがゆえに，初学者にとっては学習が難しい．

ネットワークのトラフィックを解析するには，主に tcpdump や Wireshark[1] が使われる．これらは，パケットの宛先，送信元アドレス，プロトコルやペイロードなどの詳細な情報を記録する反面，文字列の羅列であるために人が解釈するのに時間を要する．そのため，時間差でパケットを解析することになり，コンピュータを操作したタイミングとそのときに発生したパケットとの対応が取れなくなってしまう．

本研究では，LED テープを用いて LAN ケーブル自体にパケットを可視化する手法を提案する．このシステムでは，パケットに見立てた LED の光が送信方向へ向かって通過するかのように可視化される．発光の色はパケットの種類ごとに 8 色を割り当てた．これにより，コンピュータを操作したと同時に，どのようなパケットが発生するかを直感的に理解することが可能となる．

ネットワークを流れるパケットに慣れ親しみ，ネットワークの仕組みの理解を支援する目的で開発した．

2. 関連研究

ネットワーク通信の視覚化に関する研究を紹介する．パケットの情報を可視化する手法は，画面上に仮想的に描画される場合がほとんどである．NIRVANA[2] は，組織のネットワークを流れるトラフィックをネットワークトポロジの背景とともにパケットオブジェクトを三次元的にリアルタイムで描画する．

一方で，実世界の物体でパケットの情報を表現する手法も存在する．インターネット物理モデル [3] は，インターネットで情報が伝わるしくみを，白と黒のボールの動きで視覚化した．ネットワークとして機能するように実際の仕組みを忠実に再現しているが，限られたネットワーク構成の中で特定のパケットしか表現されていない．SecureSense[4] は，セキュリティ監視のイベント情報に基づいて環境音やランプで情報を提示し，生活空間内にセキュリティを知覚

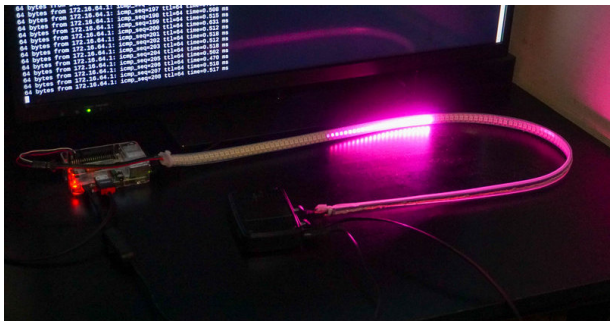

図 1　Illumi Packet の図．Raspberry Pi(左) からルータ (中央下) へ ICMP のパケットを送信したことが可視化された様子．

表 1　パケットの種類と発色

種類	ARP	ICMP	DNS	DHCP	IGMP
色	橙色	桃色	緑色	水色	紫色

種類	その他 TCP	その他 UDP	それ以外
色	青色	黄色	□ 白色

[1] 東京工業大学
[a)] aso.k.aa@m.titech.ac.jp
[b)] koike@acm.org

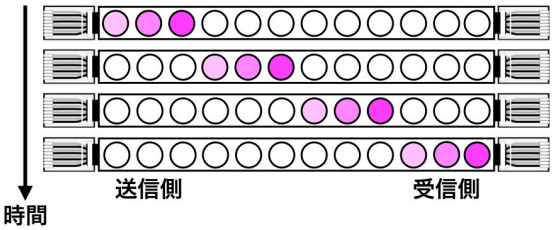

図 2　LAN ケーブルの可視化の概要図.

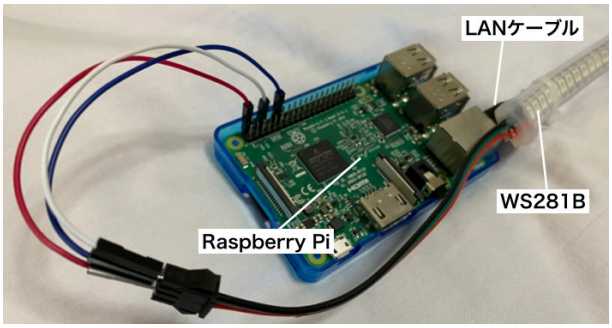

図 3　ハードウェア構成図.

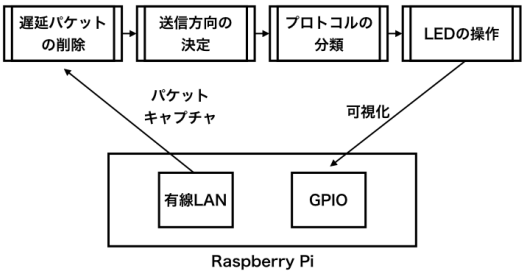

図 4　ソフトウェア構成図.

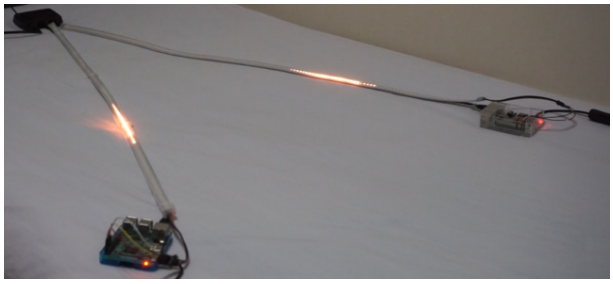

図 5　ARP(橙色) がブロードキャストされる様子.

できるようにしている.

本研究では，制限が多いが影響力がある実世界において，多様なパケットの動きの視覚化を試みる.

3. 提案手法

本研究では，LAN ケーブル自体にパケットを可視化する手法 (**図 1**) を提案する.

図 2 に示すように，パケットが送信方向へ通過するように可視化する．1 つのパケットに見立てた光が，一定時間 (約 0.25 秒) を要して送信側から受信側まで到達する.

また，パケットの種類ごとに異なる色で可視化を行う．種類と発色の対応を**表 1** に示す．家庭内のネットワークで観測されやすいプロトコルを識別可能となるように種類を選出した.

4. システム構成

4.1 ハードウェア構成

ハードウェアの構成を**図 3** に示す．パケットの可視化には LED テープ (WS281B) を用いた．それを Raspberry Pi 3 Model B+の GPIO に接続し，LAN ケーブルに固定した.

4.2 ソフトウェア構成

ソフトウェアの構成を**図 4** に示す．Go 言語のパケットライブラリ gopacket を用いて，Raspberry Pi の有線 LAN インターフェースにおけるパケットをキャプチャする．パケットが到着するごとに，遅延パケットの破棄，送信方向の決定，プロトコルの分類を行い，対応する色で送信側から受信側に向けて順番に LED を操作して可視化する．およそのリアルタイム性を確保するために，可視化する時刻とパケットのタイムスタンプとの差が 5 秒以上ある場合は，それらの可視化処理を行わない.

LED テープは rpi_ws281x[5] のライブラリを用いて PWM で操作した.

ソースコードは，オープンソースとして公開しており，

`https://github.com/souring001/illumi-packet`

からダウンロード可能である.

5. 実用例

Illumi Packet を用いた場合に，特に教育的な効果が期待できる PC の操作と発生するパケットの例を紹介する.

Web アクセス

ブラウザで Web サイトにアクセスをすると，DNS(緑色) のパケットが往復したのちに TCP(青色) のパケットが発生する (**図 6**)．これは，DNS で URL のドメイン名から対応する IP アドレスを解決したのちに，その IP アドレスから TCP で Web ページをダウンロードすることを示す.

ブロードキャストの観測

Illumi Packet 複数台を同じネットワークに接続すると，ルータからブロードキャストされたパケットが同心円状に放出される (**図 5**)．ARP の要求パケットが発生した際などに，その様子が確認できる.

疎通確認

IP 層における到達確認に用いる ping コマンドを使用すると，到達可能な場合は毎秒 ICMP(桃色) のパケットが往復する様子を確認できる (図 1).

LAN ケーブルの接続

LAN ケーブルを挿すと，IP アドレスを自動で割り振る際

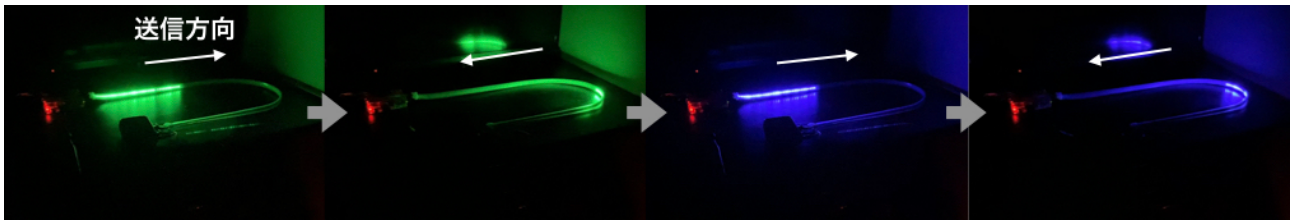

図 6　Web サイトにアクセスしたときの Illumi Packet．DNS(緑色) のパケットが往復したのちに TCP(青色) のパケットが発生する．

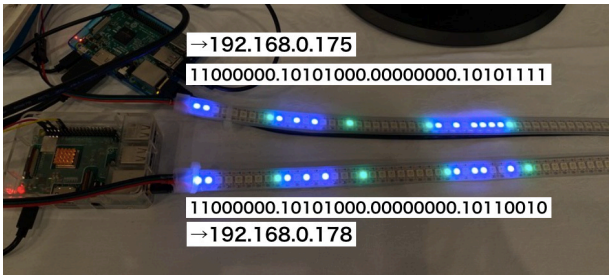

図 7　IP アドレス表示機能．白色の光が 1，光っていない状態が 0，緑色の光が区切りを表す．上のアドレスは 192.168.0.175，下のアドレスは 192.168.0.178 を示しており，ネットワーク部が一致しており，ホスト部が異なる．

に使う DHCP(水色) のパケットが観測可能となる．

その他応用例

・IP アドレス表示機能 (図 7):
それぞれの LED の光の有無を 2 進数の 0 と 1 に対応させることで，IP アドレスを表示することが可能となる．ネットワークアドレスやクラスなど，IP アドレスは 2 進数の表記で意味を成すことが多い．図のように，同一ネットワーク内の 2 つの IP アドレスを比較することで，サブネットマスクの理解にも繋がる．

・異常パケットの発見:
ネットワーク型 IDS 等で異常検知されたパケットを赤色で示すことで攻撃的なパケットの早期発見に繋がる．赤いパケットがインターネット側から向かってくる場合は侵入を試みられており，自分から発している場合は，既に感染している可能性があるとわかる．

6. 議論

実際のパケットの通信速度は 1Gbps と高速であるが，パケットの可視化が低速であるため，通信速度が低速であるという誤解を招く恐れがある．実際に，SNS 上で動画を公開したところ，コメントにてパケットの速度に関して誤解している様子が伺えた．こうした誤った解釈をされないために，実際の通信速度と同等の速度で可視化するモードなどを用意するなどして対応したい．

提案手法では，パケットを可視化するのに一定の時間を要する．本研究では，一定時間以上のタイムラグがある場合は可視化をしないことでおおよそのリアルタイム性を維持した．しかし，一度に大量のパケットが到達した場合は，それらの大部分が可視化されず，重要なパケットを発見する機会を逃してしまう．可視化をするパケットに優先度をつけるなどの要約手法を検討する必要がある．

また，可視化の様子から第三者が通信内容を部分的に推測できてしまうため，通信の秘密に反する恐れがある．第三者の目に触れない範囲で扱い，日常的な使用は避けるなどの配慮が必要となる．

7. まとめと今後の課題

本論文では，パケットの種類と方向に応じて可視化する LAN ケーブル Illumi Packet を提案して実装し，その機能と実用例について概説した．

今後は，ネットワークの初学者に Illumi Packet を使ってもらい，教育用途として有用であるかを評価する必要がある．Illumi Packet をさらに実用的にするために，パケットのフィルタリングや速度などの設定をカスタマイズ可能とし，多様な状況で活用できるようにしたい．また，本研究では教育目的としての用途に着目したが，システム管理などに応用が可能である．Illumi Packet のその他用途における有用性を見出していきたい．

謝辞　本研究は，国立研究開発法人情報通信研究機構によるセキュリティイノベータ育成プログラム SecHack365 における成果である．

参考文献

[1] Wireshark. https://www.wireshark.org
[2] 鈴木 宏栄, 衛藤 将史, 井上 大介, 実ネットワークトラフィック可視化システム NIRVANA の開発と評価, 情報通信研究機構研究報告, 2011, 57 巻, 3.4 号, p. 63-80.
[3] 江渡 浩一郎, 杉原 聡, 島田 卓也, 東泉 一郎, 岩 政隆一, ボールの流れで Internet の仕組みを表現した「インターネット物理モデル」の構築について, 第 64 回全国大会講演論文集, 2002, p. 607-608.
[4] 大橋 正興，塚田 浩二，小池 英樹，安村 通晃，Secure Sense: 生活空間でセキュリティを「感じる」ための情報提示環境, 情報処理学会 インタラクション 2003 対話発表, (Feb. 2003).
[5] rpi_ws281x. https://github.com/jgarff/rpi_ws281x