DHCP サーバによる学生名の識別における ARP リクエストにもとづく同時刻に接続された端末の所有者の特定

遠藤 空[1]　高橋 風太[2]　串田 高幸[1]

概要：出席管理を手動で行うことは人為的ミスの発生につながる．ネットワーク接続を利用することで学生がいつ出席したかを判断することは可能であるが，誰が出席したかを特定することはできない．そのため，この手法による出席管理の自動化を実現するには，誰がどの端末を所有しているかを特定する必要がある．これに対し，DHCP サーバと DDNS サーバをもちいて授業開始時刻までに IP アドレスが割り当てられた端末の MAC アドレスと，授業に出席した学生から端末の所有者の特定を行う方法がある．課題は，この時全て同じ授業を履修している学生の端末の特定が行えないことである．本稿では，SNS を利用した定期報告のメッセージを受信した時及び Ubuntu Server へログインした時に，ネットワーク上で使用中の端末が持つ MAC アドレスと学生の端末の候補リストを照合し，一致する MAC アドレスが一意であったときに，学生を端末の所有者として特定する方法を提案する．評価実験では，実際に学生が所有する端末の MAC アドレスと，提案により所有者を特定した端末の MAC アドレスの照合を 3 週間の期間で行い，正解率，未特定率，誤特定率を求めた．学生が所有する端末の総数は 54 個あり，提案で特定した MAC アドレスを持つ端末は 39 個で，正解数は 29 個であった．したがって，特定した端末の MAC アドレスの正解率は約 53.7%，未特定率は約 27.8%，誤特定率は約 18.5%であった．また，1 週間単位でプライベートネットワークに 1 度も接続していない端末を除外した場合，学生が所有する端末の総数は 44 個，提案で特定した MAC アドレスを持つ端末は 34 個，正解数は 29 個となり，正解率は約 65.9%，未特定率は約 22.7%，誤特定率は約 11.4%であった．

1. はじめに

背景

東京工科大学コンピュータサイエンス学部の Cloud and Distributed Systems Laboratory(CDSL) では，学生自身の研究内容に関連する論文を要約して発表する論文輪講会や，各自の研究内容の進捗を発表する Cadence がある．上記の授業は全て学生が出席管理を手動で行っている．授業開始時に出席確認を行うため遅刻した学生がいた場合，その都度出席名簿の出席状況を更新する必要がある．出席管理を手動で行う場合，出席名簿への記入に時間がかかり，誤記入を例とする人為的ミスの発生につながる [1,2].

教育機関では顔認証，QR コード認証，Moodle や Canvas を例としたネットワーク接続による学生管理システムを使用した出席管理の方法がある [3,4]．上記の方法はいずれも，学生側が入力操作やカメラで顔を読み取る動作があり，自動で出席管理を行うことはできていない．

ネットワーク接続を利用することで学生が出席した時刻の特定はできるが，誰が出席したかを特定することはできない．そのため，この手法による出席管理の自動化を実現するには，対象の端末を所有している学生を特定する必要がある．

CDSL にはプライベートネットワークがあり，以下のサーバが存在する．

- Dynamic Host Configuration Protocol Server (DHCP サーバ)
- Domain Name System Server(DNS サーバ)
- Dynamic Domain Name System Server (DDNS サーバ)

プライベートネットワークとは，ローカルエリアネットワーク内で使用されるネットワークのことである [5]．通信を行う際はグローバル IP アドレスではなく，プライベート IP アドレスを使用する．

DHCP サーバとは，ネットワークに接続されたデバイスが IP アドレス，デフォルトゲートウェイ，DNS の IP アドレスを例とするネットワーク構成を自動で行うクライアン

[1] 東京工科大学コンピュータサイエンス学部
〒 192–0982 東京都八王子市片倉町 1404-1
[2] 東京工科大学大学院バイオ・情報メディア研究科コンピュータサイエンス専攻
〒 192–0982 東京都八王子市片倉町 1404-1

© 2024 Cloud and Distributed Systems Laboratory

トサーバプロトコルである [6,7]．DHCP サーバは Media Access Control address（MAC アドレス）をもとに，ネットワーク接続されたデバイスに IP アドレスを割り当てる [8]．MAC アドレスとは，ネットワーク内でデバイス間通信を行うための一意の識別子であり，48 ビットで表される [9]．

DNS サーバとは，IP アドレスとドメイン名の変換を行うクライアントサーバプロトコルである [10]．

DDNS サーバとは，DHCP サーバによって動的 IP アドレスが割り当てられた際に，自動的に IP アドレスとホスト名を紐づけて DNS サーバへレコードを追加し，リースが切れた際には自動的に DNS サーバからレコードを削除するサーバである [11,12]．DDNS サーバが追加するレコードは，ホスト名に対して IPv4 アドレスを紐づける A レコードと，IPv4 アドレスに対してホスト名を紐づける PTR レコードの 2 つがある [13]．

端末の所有者の特定方法として，DHCP サーバと DDNS サーバをもちいて，授業開始時刻までに IP アドレスが割り当てられた端末の MAC アドレスと，授業に出席した学生から端末の所有者の特定を行う方法がある [14]．上記の方法では，出席名簿データベース (出席名簿 DB) から学生の名前と出席状況をメンバーリストとして保持する．また，授業開始時刻までに IP アドレスが割り当てられた端末の MAC アドレスを，MAC アドレスのリストとして保持する．この流れを図 1 に示す．

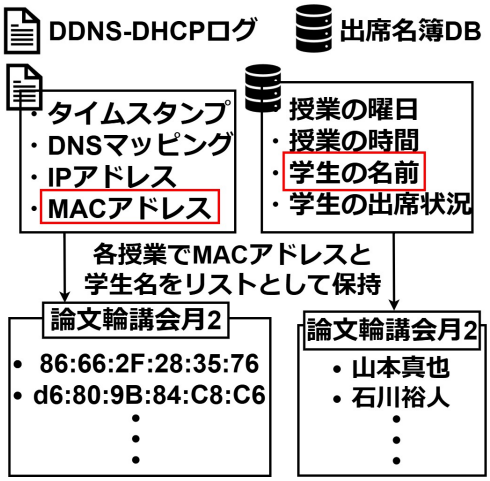

図 1: 学生名，MAC アドレスをリストに保持

図 1 では，月曜日 2 時限にある論文輪講会の開始時刻までに IP アドレスが割り当てられた MAC アドレスと，出席者の学生の名前をそれぞれ MAC アドレスのリストとメンバーリストとして保持する．図 1 の DDNS-DHCP ログは DDNS サーバと DHCP サーバのログをもとに作成したログである．DDNS サーバからタイムスタンプ，IP アドレス，DNS マッピングを取得している．DHCP サーバのログにはリースが切れたログが残らないため，DDNS サーバのタイムスタンプを使用している．MAC アドレスは，DHCP サーバから DDNS サーバに送信されるタイムスタンプと同じ時刻のログから取得している．本稿における DNS マッピングは，DHCP サーバが DNS サーバへレコードを追加することを add とし，レコードを削除することを remove とする．DDNS-DHCP ログの例をログファイル 1 に示す．

ログファイル 1: DDNS-DHCP ログの例

```
1 2024-10-10T10:39:45.91,add,192.168.100.173,2
      e:58:93:51:a0:78,iphone
2 2024-10-10T12:41:47.86,remove,192.168.100.173,
      iphone
```

ログファイル 1 の 1 行目では，2024 年 10 月 10 日 10 時 39 分 45.91 秒に DNS マッピングが add として記録されている．これは，2e:58:93:51:a0:78 の端末に 192.168.100.173 の IP アドレスを割り当て，DNS サーバへレコードを追加したことを示す．2 行目では，2024 年 10 月 10 日 12 時 41 分 47.86 秒に DNS マッピングが remove として記録されている．これは，192.168.100.173 に対応するレコードを DNS サーバから削除したことを示す．また，DHCP サーバのログにはレコードを削除したログとリースが切れたログが残らず，DDNS サーバのログには MAC アドレスが含まれないため，DNS マッピングが remove の際には，IP アドレスのみを記述している．

次に，リストの中身をメンバーリスト同士及び MAC アドレスのリスト同士で授業ごとに比較する．リストの比較を行う回数は 1 週間の授業回数分である．理由は 1 週間に全員同じメンバーで行う授業が存在しないためである．この比較の結果，MAC アドレスのリストで共通した MAC アドレスを，メンバーリストで共通した学生の所有している端末とする．リストの共通部分から端末の所有者を特定する流れを図 2 に示す．

図 2 のメンバーリストでは，木曜日 2 時限にある 3 年生 Cadence と月曜日 2 時限にある論文輪講会，火曜日 1 時限にある 4 年生 Cadence の 3 つの授業に共通して出席していた学生が「山本真也」であることを示している．また，図 2 の MAC アドレスのリストは，上記の 3 つの授業開始時刻までに IP アドレスが割り当てられた端末の MAC アドレスを保持している．3 つの MAC アドレスのリストに共通している MAC アドレスは 86:66:2f:28:35:76 である．そのため，MAC アドレスが 86:66:2f:28:35:76 である端末の所有者を「山本真也」として特定する．

また，上記のアルゴリズムをもとに作成したソフトウェアが 2 つある．1 つ目は，DDNS-DHCP ログを作成する log_output である．2 つ目は，DDNS-DHCP ログと出席簿から授業ごとのリストを作成し，リストの中身をメンバーリスト同士，MAC アドレスリスト同士で授業ごとに比較を行い，端末の所有者の特定を行う identify である．

© 2024 Cloud and Distributed Systems Laboratory

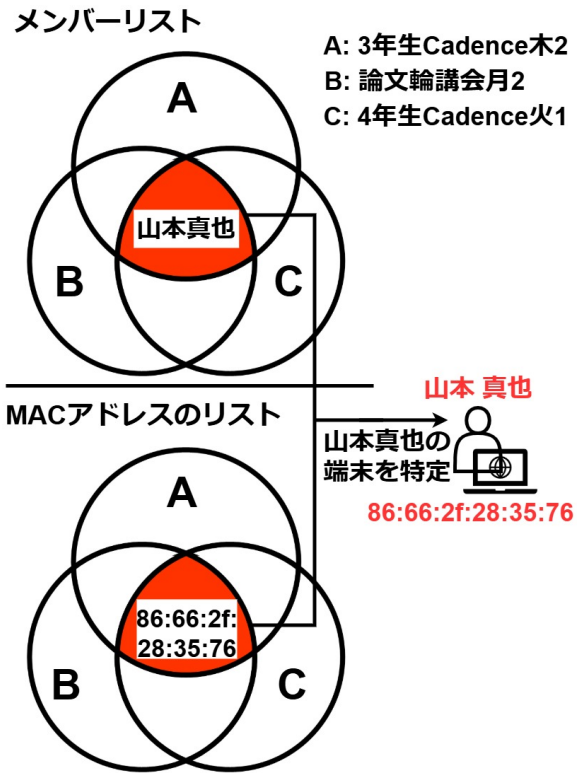

図 2: リストの共通部分から端末の所有者を特定

課題

課題は，DHCP サーバと DDNS サーバや出席簿をもちいて，同じ授業を履修している学生が所有する端末を特定出来ない点である．本稿の課題を図 3 に示す．

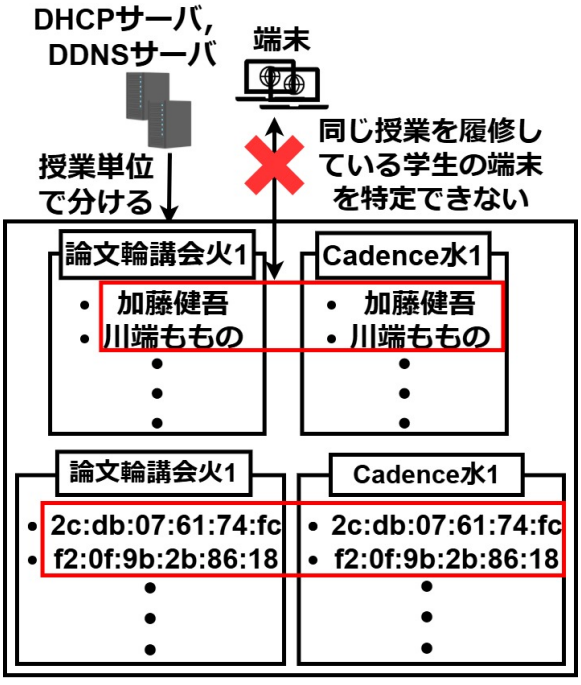

図 3: 複数の学生が同じ授業を履修している場合

図 3 では，学生である「加藤健吾」と「川端ももの」が火曜日 1 時限の論文輪講会と，水曜日 1 時限の Cadence の両日を履修している．そのため，2 つの MAC アドレスが上記のどちらの学生が所有している端末の MAC アドレスなのかが分からない．これにより，出席管理の自動化に必要な全ての端末の所有者を特定することができない．

各章の概要

第 2 章では，本稿の関連研究について述べる．第 3 章では，本稿の課題を解決するための提案方式とユースケース・シナリオについて述べる．第 4 章では，提案方式をもとに作成したソフトウェアの実装について述べる．第 5 章では，提案方式の評価と実験結果について述べる．第 6 章では，本稿の議論について述べる．第 7 章では，本稿のまとめを述べる．

2. 関連研究

Address Resolution Protocol request(ARP リクエスト) を使用した自動出席管理システムを提案している研究がある [15]．ARP リクエストとは，対象の IP アドレスと一致する MAC アドレスを返すように要求するパケットのことである [16]．ARP リクエストはブロードキャストであり，同一ネットワークに接続されている全コンピュータに送信される．ARP リクエストの結果からネットワーク上で使用中の MAC アドレスを確認し，出欠が決定される．上記の研究では，出席者と出席者が所有する端末の MAC アドレスを事前に入力している．そのため，端末の所有者の特定を自動で行う必要がある．

プローブ要求を使用した自動出席管理システムを提案している研究がある [17]．Wireshark を使用し，学生の SmartPhone(スマートフォン) が検出されれば出席と判定するシステムを提案している．上記の研究では，プローブ要求に応答する MAC アドレスが，学生の所有する端末であるかは，事前に確認している．そのため，端末の所有者の特定を自動で行う必要がある．

大学のキャンパスネットワークをもちいた出席管理システムを提案している研究がある [18]．ルータやスイッチとの信号強度と ARP リクエストからキャンパスネットワークに接続された端末がどこで使用中であるかを判断している．しかし，上記の研究では，認証確認として学生にユーザ ID，パスワード，カメラをもちいた顔写真を入力操作として要求している．そのため，端末の所有者の特定を自動で行う必要がある．

3. 提案

本稿では，SNS を利用した学生からの定期報告を受信した時及び Ubuntu Server へログインした時に，ネットワーク上で使用中の端末が持つ MAC アドレスと学生の端末の候補リストを照合し，一致する MAC アドレスが一意であったときに，学生を端末の所有者として特定する手法を

© 2024 Cloud and Distributed Systems Laboratory

提案する．端末の候補リストとは，DHCP サーバと DDNS サーバをもちいて，端末の所有者が一意に定まらなかった端末の集合のことである．本稿における定期報告とは，Social Networking Service（SNS）を通じて毎週送信しなければならないメッセージのことである．例として CDSL では毎週，研究室の掃除当番が割り当てられており，掃除を行った際に Slack にて掃除完了報告を行っているメッセージがあげられる．端末の候補リストは DHCP サーバと DDNS サーバや出席簿を使用した方法により作成する．1 週間に 2 コマある授業がないことから，DHCP サーバと DDNS サーバや出席簿をもちいて授業の比較を行う期間は最低 1 週間とする．1 週間であれば，学生全員に対してこの方法を適用でき，端末の候補リストを作成できるためである．また本稿の提案を適用する際には，DDNS-DHCP ログ，出席簿から作成した授業ごとの MAC アドレスのリストをもちいる．

提案方式

本稿では，定期報告を受信した時と Ubuntu Server へログインした時にネットワーク上で使用中の MAC アドレスを取得し，この MAC アドレスを授業ごとの MAC アドレスと比較する．Ubuntu Server へログインした時にネットワーク上で使用中の MAC アドレスを取得する流れを図 4 に示す．

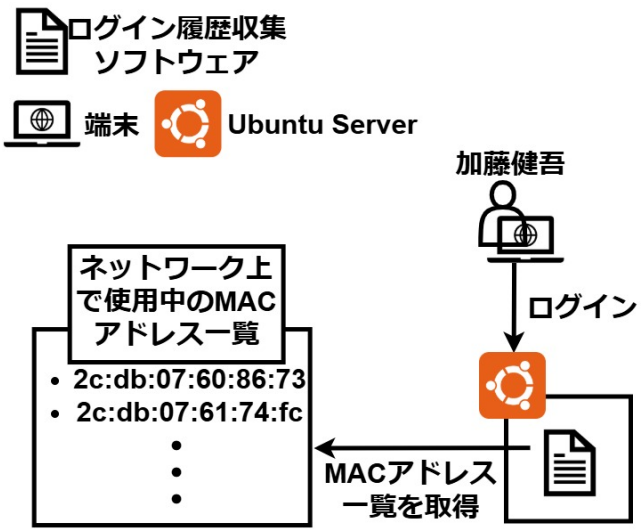

図 4: Ubuntu Server へログイン時にネットワーク上で使用中の MAC アドレスを取得

図 4 では学生である加藤健吾が，Ubuntu Server にログインする．ログインが確認されたら，ネットワーク上で使用中の MAC アドレスの一覧を取得する．ログインの判断及びネットワーク上で使用中の MAC アドレスの取得はログイン履歴収集ソフトウェアが行う [19]．また，上記のソフトウェアは学生がログインする Ubuntu Server で実行する．この時，Ubuntu Server へのログインが Virtual Private Network(VPN) を使用して外部からのログインであるか，研究室のネットワークを使用したログインであるかどうかは，Jump Server(踏み台サーバ) のログイン履歴をもちいて判断する．踏み台サーバとは，ネットワーク外部からのアクセスを処理するための中継サーバである [20]．

同じように定期報告を受信した時にネットワーク上で使用中の MAC アドレスを取得する流れを図 5 に示す．図 5

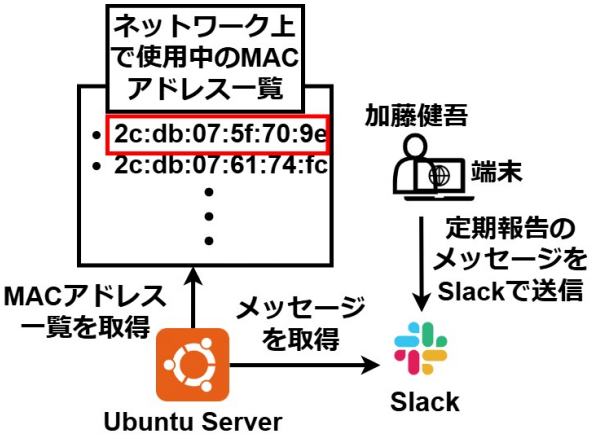

図 5: 定期報告を受信した時にネットワーク上で使用中の MAC アドレスを取得

では学生である加藤健吾が，定期報告のメッセージを Slack をもちいて送信している．Slack で定期報告のメッセージが送信されたことを検知した後に，ネットワーク上で使用中の MAC アドレスの一覧を取得する．

上記で作成したネットワーク上で使用中の MAC アドレスの一覧と，加藤健吾の所有している端末の候補リストの MAC アドレスを比較する．比較の結果，一致する MAC アドレスが存在するかを確認する．この流れを図 6 に示す．図 6 では「2c:db:07:5f:70:9e」が，ネットワーク上で使

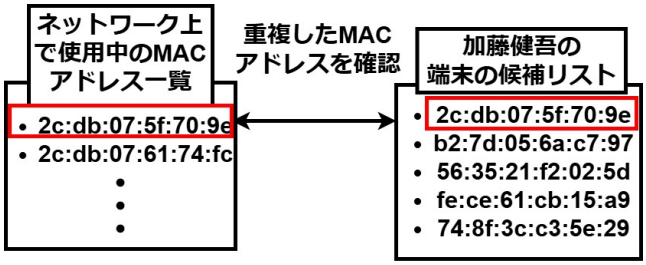

図 6: ネットワーク上で使用中の MAC アドレスと端末の候補リストの MAC アドレスを比較

用中の MAC アドレス一覧と，加藤健吾の所有している端末の候補リストの両方に存在する．また，端末の候補リストの MAC アドレスが一意に定まっていることから，この MAC アドレスの端末を加藤健吾の所有する端末として特定する．

© 2024 Cloud and Distributed Systems Laboratory

ユースケース・シナリオ

本稿ではユースケースとして，Slack を使用した連絡手段と，DHCP サーバや DDNS サーバ及び DNS サーバを備えたプライベートネットワークを有する研究室を想定する．上記の例として CDSL があげられる．図 7 に提案ソフトウェアを使用した本稿のユースケース・シナリオを CDSL を例として示す．

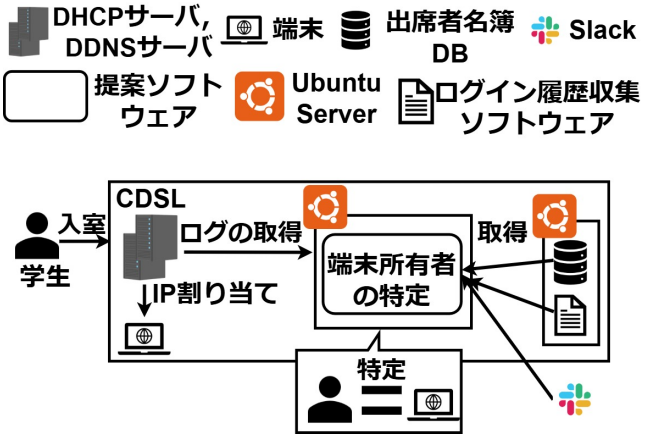

図 7: ユースケース・シナリオ

学生が CDSL に入室した際に DHCP サーバは学生が所持している端末に IP アドレスを割り当てる．IP アドレスを割り当てられた DHCP サーバのログと DDNS サーバのログを提案ソフトウェアが取得する．本稿の提案ソフトウェアでは出席名簿 DB から学生の名前と出席状況，ログイン履歴収集ソフトウェアから学生の Ubuntu Server へのログイン履歴及び Slack から定期報告のメッセージを取得し，端末の所有者を特定することが可能である．

4. 実装

本稿では，log_output，identify の他に，Ubuntu Server へログインした時にネットワーク上で使用中の MAC アドレスと identify で作成したリストの比較により，端末の所有者を特定するソフトウェア login-arp と，定期報告を受信した時にネットワーク上で使用中の MAC アドレスと identify で作成したリストの比較により，端末の所有者を特定するソフトウェア report-arp を Python で作成した．上記の 2 つの提案ソフトウェアの処理の流れを図 8 に示す．

図 8 の括弧数字は login-arp の処理の流れ，丸数字は report-arp の処理の流れを示している．ソフトウェアごとに説明する．

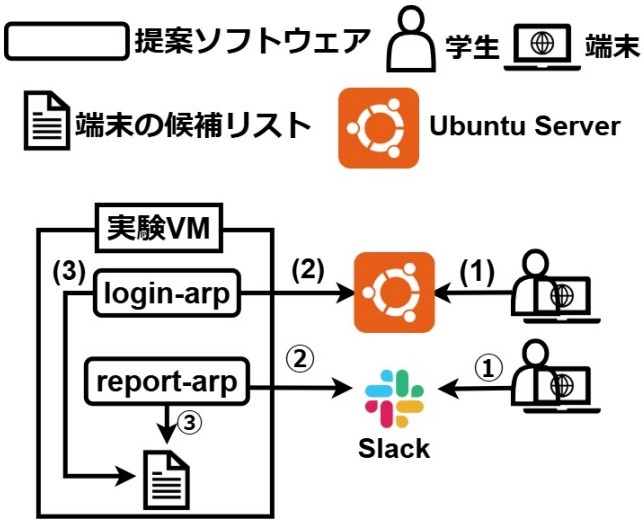

図 8: 提案ソフトウェアの処理の流れ

login-arp

Ubuntu Server へログインした時にネットワーク上で使用されている MAC アドレス一覧を取得するソフトウェアである login-arp の処理の流れを以下に示す．

(1) 学生が Ubuntu Server へ SSH 接続によりログインする．

(2) Ubuntu Server へのログインを検知したら，arp-scan コマンドを実行し，ネットワーク上で使用中の MAC アドレス一覧を取得する．学生が Ubuntu Server へログインしているかを判断するプログラムはシェルスクリプトをもちいて作成し，学生が所有する全ての VM 内の Ubuntu Server で実行する．systemd により，上記のシェルスクリプトを毎分実行する．学生が CDSL の Wireless Fidelity(Wi-Fi) を使用し，Ubuntu Server へログインしたかを踏み台サーバをもちいて判断する．踏み台サーバで全ユーザの last コマンドを実行し，この結果をもちいる．上記の結果，Ubuntu Server へアクセスと同時刻に踏み台サーバにもログイン履歴があれば，CDSL の Wi-Fi を使用せずにアクセスしているとみなし，この arp-scan の結果を除外する．除外する理由は，CDSL の Wi-Fi に接続していない端末は ARP リクエストに応答せず，arp-scan で出力されないためである．Ubuntu Server と踏み台サーバの両方へのログインが確認された場合，その時間は研究室外からのアクセスとして除外する．

(3) 取得した arp-scan の MAC アドレスと，その学生の端末の候補リストを記述した txt ファイルから，一意となる MAC アドレスを，学生が所有する端末として特定する．

report-arp

次に定期報告のメッセージがある場合に，ネットワークで使用中の MAC アドレス一覧を取得するソフトウェアである report-arp の処理の流れを以下に示す．

① 学生が定期報告のメッセージを Slack で送信する．

② Slack の API をもちいて，Slack に送信されたメッセージを取得する．定期報告のメッセージを検知した場合，

© 2024 Cloud and Distributed Systems Laboratory

arp-scan コマンドを実行し，ネットワーク上で使用中の MAC アドレス一覧を取得する．

③ 取得した arp-scan の MAC アドレスと，その学生の端末の候補リストを記述した txt ファイルから，一意となる MAC アドレスを，学生が所有する端末として特定する．

5. 評価実験

提案によって特定した端末の所有者が，正しい端末の所有者であるかの正解率と，学生が所有する端末全てに対して所有者を特定できなかった端末の割合を示した，未特定率を評価する．また，提案ソフトウェアによって端末の所有者を誤って特定した，誤特定率を評価する．

実験環境

本稿で使用する実験環境を図 9 に示す．図 9 の K3s cluster は 4 台の Node で構築され，全て master として稼働している．DHCP サーバのログを dhcp.log，DDNS サーバのログを ddns.log として取得し，背景で述べた log_output を使用して DDNS-DHCP ログを作成する．DDNS-DHCP ログと，学生の出席簿である meeting_member.csv から identify を使用した方法により，端末の所有者の特定を行い，特定できなかった学生の端末の候補リストを作成し，txt ファイルへ保存する．

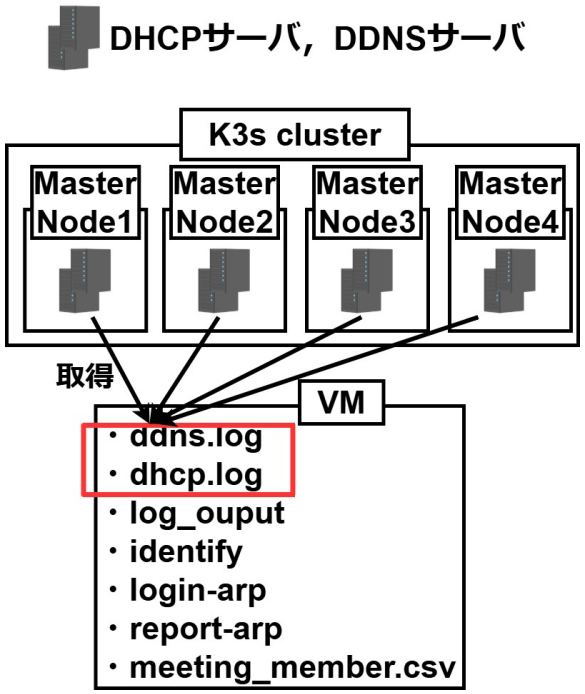

図 9: 実験環境

以下に提案ソフトウェアを配置している VM と，DHCP サーバと DDNS サーバを配置している Node の構成情報を示す．DHCP サーバと DDNS サーバには kea の 22.0 をインストールした．

- 提案ソフトウェアを配置している VM
  OS: Ubuntu Server 22.04.1 LTS
  vCPU: 2 [Core]
  RAM: 5 [GB]
  HDD: 25 [GB]

- DHCP サーバと DDNS サーバを配置している Node
  OS: Ubuntu Server 22.04.1 LTS
  vCPU: 2 [Core]
  RAM: 8 [GB]
  HDD: 50 [GB]

実験結果と分析

提案ソフトウェアによって特定した MAC アドレスの正解率を評価するために，CDSL の学生全員が所有する端末の MAC アドレスを Google Form をもちいて収集し，評価対象として用意した．また，実験を行った期間は 2024 年 10 月 7 日から 2024 年 10 月 18 日と，2024 年 11 月 18 日から 2024 年 11 月 22 日の合計 3 週間である．実験を行った際の正解率を，図 10 に示す．

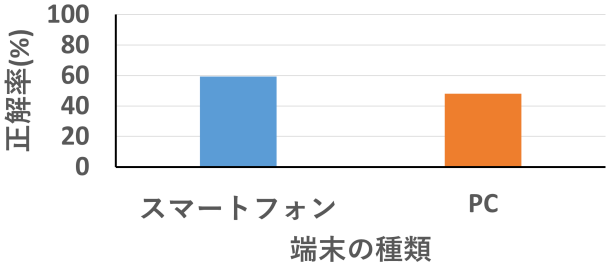

図 10: 端末の種類ごとの正解率

実験結果では，学生が所有する端末の総数は 54 個であり，内訳はスマートフォン及び Personal Computer(PC) が 27 個ずつである．スマートフォンと PC の分類はホスト名をもちいて行い，desktop，laptop，air，mac の表記がある端末を PC とし，それ以外をスマートフォンとした．上記の総数のうち，提案ソフトウェアによって学生の所有する端末として特定した MAC アドレスの正解数は 29 個で，正解率は約 53.7%であった．29 個の端末のうち，スマートフォンの正解数は 16 個で，正解率は約 59.3%であった．また，PC の正解数は 13 個で，正解率は約 48.1%であった．

また，未特定率を，図 11 に示す．所有者を特定できなかった端末の総数は 15 個で，未特定率は約 27.8%であった．15 個の端末のうち，スマートフォンは 7 個存在し，未特定率は約 25.9%であった．また，PC は 8 個存在し，未特定率は約 26.6%であった．

© 2024 Cloud and Distributed Systems Laboratory

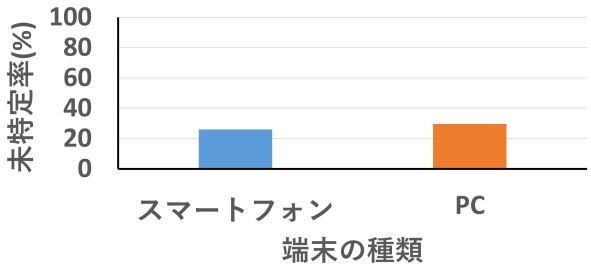

図 11: 端末の種類ごとの未特定率

図 11 の実験結果のうち，学生が所有する端末全体に対して提案ソフトウェアが端末の所有者を誤って特定した割合を誤特定率とし，図 12 に示す．

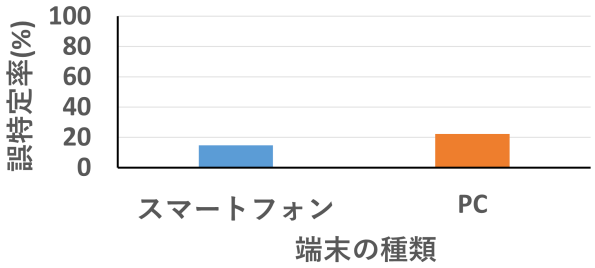

図 12: 端末の種類ごとの誤特定率

端末全体の誤特定率は約 18.5%で，スマートフォンの誤特定率は約 14.8%であり，PC の誤特定率は約 22.2%であった．

例えば，学生である「川端ももの」の実際のスマートフォンの MAC アドレスは fe:ce:61:cb:15:a9 であり，PC の MAC アドレスは 22C-db-07-61-74-fc である．しかし，提案ソフトウェアでは，「川端ももの」の所有するスマートフォンの MAC アドレスは b6:b8:eb:1b:7b:8a，PC の MAC アドレスは 2c:db:07:61:74:fc であった．上記の場合の正解数は 1 となり，正解率と誤特定率は 50.0%となる．

正解率が低くなった要因として，CDSL のプライベートネットワークに接続していない学生が存在したことがあげられる．本稿の実験期間として 3 週間の期間を要し，最初の 1 週間は入室してきた学生にプライベートネットワークを接続しているかの確認を行った．これは，端末のネットワークを切断している学生や，大学のプライベートネットワークに自動接続するように設定している学生が存在するためである．確認の結果，CDSL のプライベートネットワークに接続していない場合は，ネットワークの接続を変更する対応を行った．しかし，2 週間目以降はプライベートネットワークに接続するよう Slack を通して依頼はしたが，確認は行っていなかった．その結果，所有者本人に確認をすると，研究室にいるが，プライベートネットワークに接続していない学生が複数人存在した．プライベートネットワークに接続していない場合，DHCP サーバと DDNS サーバのログに残らず，ネットワークを使用した出席管理の自動化に必要な，端末所有者を特定することができない．

実験期間中に，1 週間単位でプライベートネットワークに 1 度も接続していなかった学生を除外した実験結果から，正解率を図 13 に示す．端末の総数は 44 個で，正解率

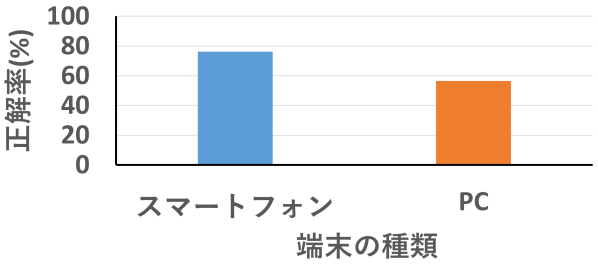

図 13: プライベートネットワークに接続した端末の種類ごとの正解率

は約 65.9%であった．44 個の端末のうち，スマートフォンの数は 21 個で，正解率は約 76.2%であった．また，PC の数は 23 個で，正解率は約 56.5%であった．

実験期間中に，プライベートネットワークに 1 度も接続していなかった学生を除外した実験結果から，誤特定率を図 14 に示す．誤特定した端末の総数は 5 個で，誤特定率

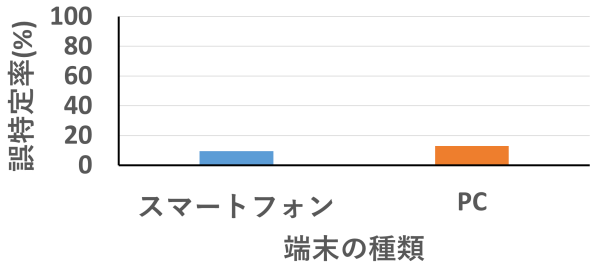

図 14: プライベートネットワークに接続した端末の種類ごとの誤特定率

は約 11.4%であった．上記の総数のうち，スマートフォンの数は 2 つで，誤特定率は約 9.5%であった．また，PC の数は 3 つで，誤特定率は約 13.0%であった．

実験期間中に，プライベートネットワークに 1 度も接続していなかった学生を除外した実験結果から，未特定率を図 15 に示す．上記の実験結果で，所有者を特定できなかった端末の総数は 10 個で，未特定率は約 22.7%であった．10 個の端末のうち，スマートフォンの数は 3 個で，未特定率は約 14.3%であった．また，PC の数は 7 個で，未特定率は約 30.0%であった．

プライベートネットワークに接続していない学生を除外した結果，正解率は向上し，未特定率，誤特定率は減少した．しかし，全ての端末に対して所有者を特定できなかった．この要因は 4 つある．1 つ目は，実験期間中にランダ

© 2024 Cloud and Distributed Systems Laboratory

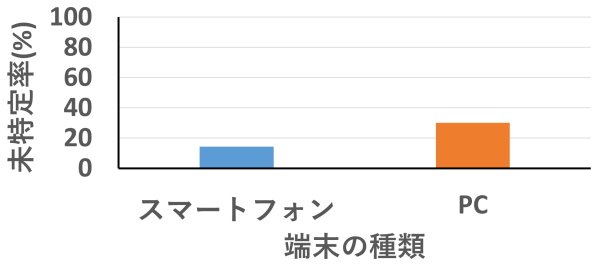

図 15: プライベートネットワークに接続した端末の種類ごとの未特定率

ム MAC アドレスとデバイスの実際の MAC アドレスを切り替えている学生がいたことである．そのため，端末の候補リストとネットワークで使用中の MAC アドレスが一致せずに，所有者を特定することができない端末が存在した．2 つ目は，Ubuntu Server 内の 1 つのユーザアカウントを複数人が使用してログインしていることである．本稿では Ubuntu Server へのログイン履歴をユーザアカウントごとに取得している．そのため，複数人が 1 つのユーザアカウントでログインした場合，Ubuntu Server にログインしている学生が誰であるかを判断することができない．また，これは PC の誤特定率が増加した要因である．3 つ目は実験期間中に Ubuntu Server へのログインがなく，Slack での定期報告もしていない学生がいたことにより，本稿の提案を適用出来なかったことである．この学生に対して本稿の提案を適用できなかったため，端末の候補リストから一意の MAC アドレスを持つ端末を所有者として特定できなかった．4 つ目は授業開始後に，PC をネットワークに接続する学生が存在したため，授業開始時刻までに割り当てられた端末に PC が含まれていないケースが存在した．そのため，本稿で使用した端末の候補リストに，実際に学生が所有する PC の MAC アドレスが含まれていないことがあった．

6. 議論

本稿では，ネットワークを使用した出席管理の自動化を実現するために，端末の所有者の特定をすることを目的としている．しかし，本稿の提案では出席管理の自動化まで行えていない．上記を実現するには，研究室からのネットワーク接続であるか，研究室外からのネットワーク接続であるかを判別しなければならない．これは，Wi-Fi 信号の CSI をもちいて屋内測位を行い，端末の位置情報を取得することで改善可能である [21]．

本稿で使用した端末の候補リストは，対象の学生が履修している授業全てで共通した MAC アドレスを保持している．そのため実験期間中に出席した学生が，授業開始時刻までにネットワークに 1 度でも繋いでいないと端末の候補リストに MAC アドレスが追加されない．これは，共通した MAC アドレスではなく，学生が履修している授業全てに割り当てられた MAC アドレスを保持し，端末の種類ごとに，IP アドレスが割り当てられた回数が最も多い MAC アドレスをもつ端末を所有者として判断することで改善可能である．端末の種類の判断にはホスト名を使用し，desktop や laptop，mac の記述がない端末はスマートフォンとして判断する．

また，端末の候補リストは，授業開始時刻までにプライベートネットワークに接続された端末を全数として，DHCP サーバと DDNS サーバや出席簿を使用した方法から作成している．そのため，授業に出席している学生が，授業開始時刻の後にプライベートネットワークに接続した場合を考慮できていない．授業開始時刻の後にプライベートネットワークに接続すると，MAC アドレスのリストに追加されないためである．例として，学生が研究室に入室した際にスマートフォンはプライベートネットワークに接続されたが，PC の電源は落としていたため，PC を起動してプライベートネットワークに接続するタイミングが授業開始時刻の後であったケースがあげられる．これは，MAC アドレスのリストに端末を追加する期間を授業開始時刻までではなく，授業期間中も含めるように変更することで改善可能である．

本稿では，提案を適用する期間を 3 週間とした．しかし，同じ授業を履修している学生の全てに提案を適用できなかった．この理由として，Ubuntu Server へのログインがなく，Slack での定期報告もしていない学生が存在したことがあげられる．これは，全ての学生が定期報告を行うまで，実験期間を延ばすことで改善可能である．ユースケースであげている CDSL では，全員が定期報告を行うための周期は 7 週間である．そのため，本稿の提案を適用する期間は，3 週間から 7 週間になる．

7. おわりに

課題は DHCP サーバと DDNS サーバや出席簿をもちいて，同じ授業を履修している学生が所有する端末を特定出来ない点である．本稿では，定期報告を受信した時及び Ubuntu Server へログインした時に，ネットワーク上で使用中の MAC アドレスのリストと出席者の端末の候補リストから，一致した MAC アドレスをもつ端末を所有者として特定することを提案した．評価実験では，学生の実際の MAC アドレスと提案によって特定した MAC アドレスを比較した正解率を評価する．学生が所有する端末の総数は 54 個あり，提案で特定した MAC アドレスを持つ端末は 29 個であった．したがって，特定した端末の MAC アドレスの正解率は約 53.7%であった．また，ネットワークに接続していない端末を除外した場合，学生が所有する端末の総数は 44 個となり，正解率は約 65.9%であった．

© 2024 Cloud and Distributed Systems Laboratory

謝辞

本稿の執筆にあたり，名前と MAC アドレスの使用を許可していただいた，東京工科大学コンピュータサイエンス学部の山本真也さん，加藤健吾さん，川端ももものさんに御礼申し上げます．また，Ubuntu Server のログイン履歴を取得するツールを提供してくださった，東京工科大学コンピュータサイエンス学部の山野倖平さんに御礼申し上げます．

参考文献

[1] Samet, R. and Tanriverdi, M.: Face Recognition-Based Mobile Automatic Classroom Attendance Management System, *2017 International Conference on Cyberworlds (CW)*, pp. 253–256 (online), DOI: 10.1109/CW.2017.34 (2017).

[2] Oo, S. B., Oo, N. H. M., Chainan, S., Thongniam, A. and Chongdarakul, W.: Cloud-based web application with NFC for employee attendance management system, *2018 International Conference on Digital Arts, Media and Technology (ICDAMT)*, IEEE, pp. 162–167 (2018).

[3] Kodali, R. K. and Hemadri, R. V.: Attendance management system, *2021 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, pp. 1–5 (2021).

[4] Conijn, R., Snijders, C., Kleingeld, A. and Matzat, U.: Predicting Student Performance from LMS Data: A Comparison of 17 Blended Courses Using Moodle LMS, *IEEE Transactions on Learning Technologies*, Vol. 10, No. 1, pp. 17–29 (online), DOI: 10.1109/TLT.2016.2616312 (2017).

[5] Krithikaa, M., Priyadharsini, M. and Subha, C.: Virtual Private Network – A Survey, *International Journal of Trend in Research and Development*, Vol. 3, No. 1, pp. 78–81 (2016).

[6] AbdulGhaffar, A., Paul, S. K. and Matrawy, A.: An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures, *2023 Biennial Symposium on Communications (BSC)*, pp. 119–124 (online), DOI: 10.1109/BSC57238.2023.10201458 (2023).

[7] Brik, V., Stroik, J. and Banerjee, S.: Debugging DHCP performance, *Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement*, pp. 257–262 (2004).

[8] Imam, M. A. Y. and Biswas, M. P. K.: MAC Address Cloning Technique Results, *Contemporary Perspective on Science, Technology and Research*, p. 120 (2023).

[9] Jayavel, S.: NETWORK SECURITY–MAC ADDRESS BLOCK.

[10] Yang, Z., Hongzhi, Y., Lingzi, L., Cheng, H. and Tao, Z.: Detecting DNS Tunnels Using Session Behavior and Random Forest Method, *2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC)*, pp. 45–52 (online), DOI: 10.1109/DSC50466.2020.00015 (2020).

[11] bis Router, G. S.: P-791R v2.

[12] Erlandsson, E., Englund, F., Schulze, J. and Sjöblom, M.: Setup of a DNS Server with Dynamic Updates, PhD Thesis (2009).

[13] Kamilaris, A., Papakonstantinou, K. and Pitsillides, A.: Exploring the Use of DNS as a Search Engine for the Web of Things, *2014 IEEE World Forum on Internet of Things (WF-IoT)*, IEEE, pp. 100–105 (2014).

[14] 遠藤空，高橋風太，串田高幸：複数の授業で MAC アドレスと出席者が重複した時間による端末所有者の特定，技術報告 CDSL-TR-201，Tokyo University of Technology CDSL Technical Report (2024). (online), Available at: https://ja.tak-cslab.org/tech-report.

[15] Prabowo, O. M. and Saputra, D. E.: Design and Implementation of Automatic Attendance System using ARP Request Detection, *2018 International Conference on Information Technology Systems and Innovation (ICITSI)*, pp. 139–142 (online), DOI: 10.1109/ICITSI.2018.8695933 (2018).

[16] Zhang, Z., Esaki, H. and Ochiai, H.: Unveiling malicious activities in lan with honeypot, *2019 4th International Conference on Information Technology (InCIT)*, IEEE, pp. 179–183 (2019).

[17] Low, C. F.: Automated attendance taker using passive mac address probing, PhD Thesis, UTAR (2018).

[18] Xu, Z., Chen, P., Zhang, W., Liu, X. and Wu, H.: Research on Mobile Phone Attendance Positioning System Based on Campus Network, *2019 International Conference on Smart Grid and Electrical Automation (ICSGEA)*, pp. 387–389 (online), DOI: 10.1109/ICSGEA.2019.00094 (2019).

[19] 倖平山野，真斗平尾，高幸串田：VM 内での作業時間を用いた重みづけによる VM 使用状況の予測にもとづく物理マシンの停止による消費電力の削減，技術報告 16，東京工科大学コンピュータサイエンス学部, 東京工科大学大学院バイオ・情報メディア研究科コンピュータサイエンス専攻クラウド・分散システム研究室, 東京工科大学コンピュータサイエンス学部 (2024).

[20] Steinhoff, M.: Using Software Containers for Privileged Access Management in Cloud Environments: A Novel Approach to Handle Access Management for Cloud-based Networks, *Nordic and Baltic Journal of Information & Communications Technologies*, pp. 297–310 (2020).

[21] Dang, X., Tang, X., Hao, Z. and Liu, Y.: A device-free indoor localization method using CSI with Wi-Fi signals, *Sensors*, Vol. 19, No. 14, p. 3233 (2019).

© 2024 Cloud and Distributed Systems Laboratory