Network intrusion (ネットワークへの侵入)

機能の視点

Attack reference
Attack type
Sub-category of attack
Host information
Malicious scripts
Etc

通信の視点

Imbalanced number of harmful attacks

これに対応するために、Transformerでtransferを学習する侵入検知システム
IDS-INT: Intrusion Detection System- Imbalanced Network Traffic

ネットワーク侵入検出はAIを活用する時代に

これまでのNIDS

Flow-based

パケットの通信ヘッダー情報による検出システム

パケットに事前定義したラベルを当てはめて分類

新しいNIDS

Packet-level

パケットに含まれる全情報による検出システム

パケットの特徴に基づいたタグを生成しこのタグを使ってパケットの内容と潜在的なリスクを表示

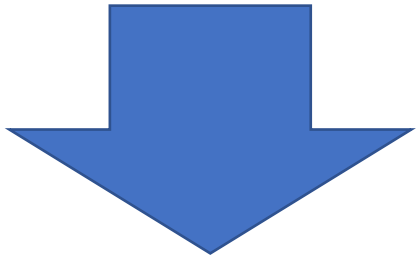
Embeddingを使用したタグ分類

1. Transformerを用い、各パケットにembeddingを生成。← セマンティック情報を含む
2. ネットワーク専用コーパスを使い、パラグラフレベルで近しいembeddingを特定 ← N-gram word extraction
3. クラスタリングで、パケットを24クラスに分類 ← K-means Cluster Analysis
4. 入力パケットに対し、単純なクラス分類より説明的なラベルを付与できる。

事前に定義されたクラスに属さないパケットに対しても近しいタグを割り当てることができる。

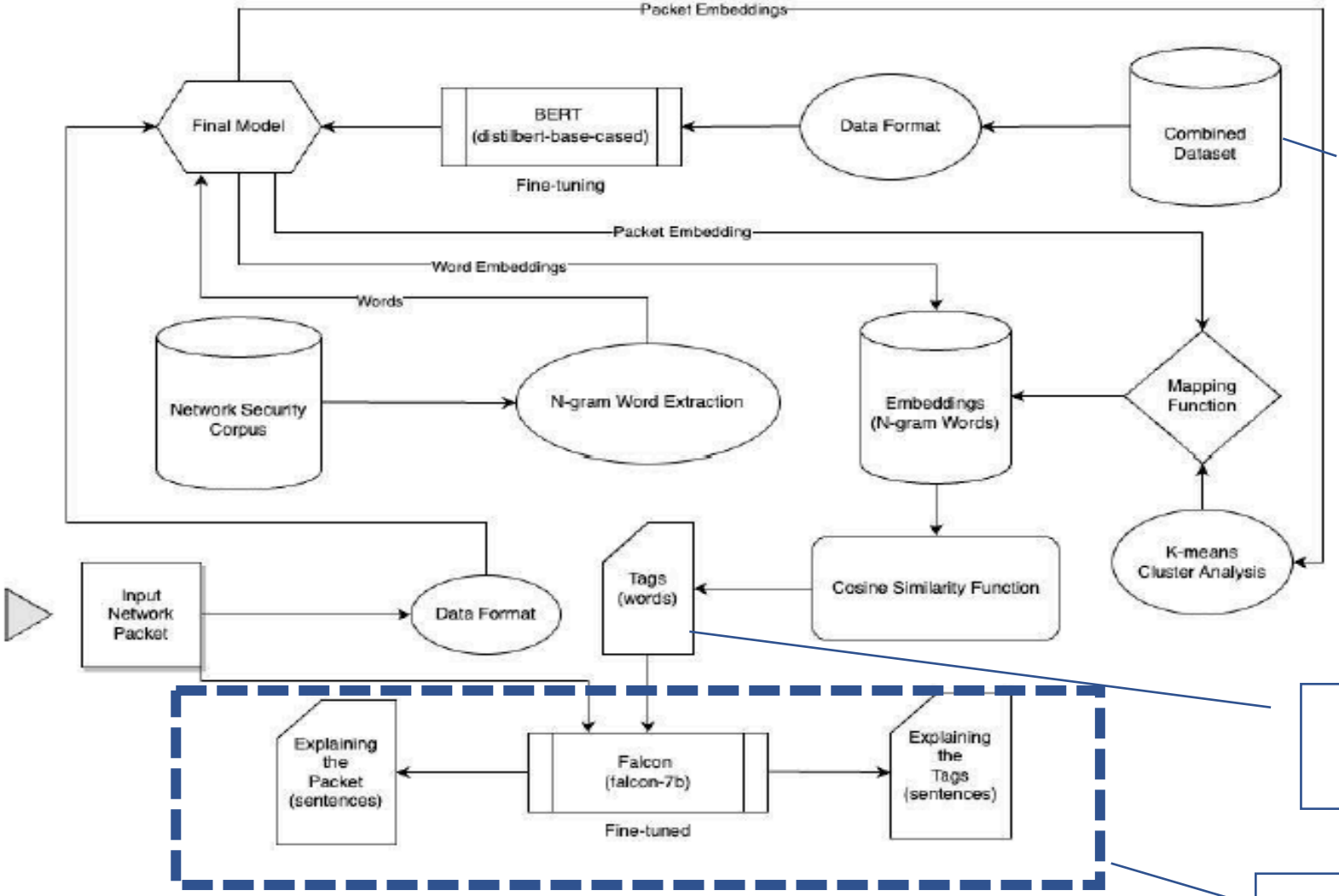
専用データセットを使用

CIC-IDS2017 (packetフォーマットはEthernet)
2.27M 通常フロー
557K 攻撃フロー
UNSW-NB15 (packetフォーマットはCooked Linux)
1.96M 通常フロー
99.6K 攻撃フロー



Combined Dataset
専用に加工して統合。24クラスの分類に整理

全体処理フロー



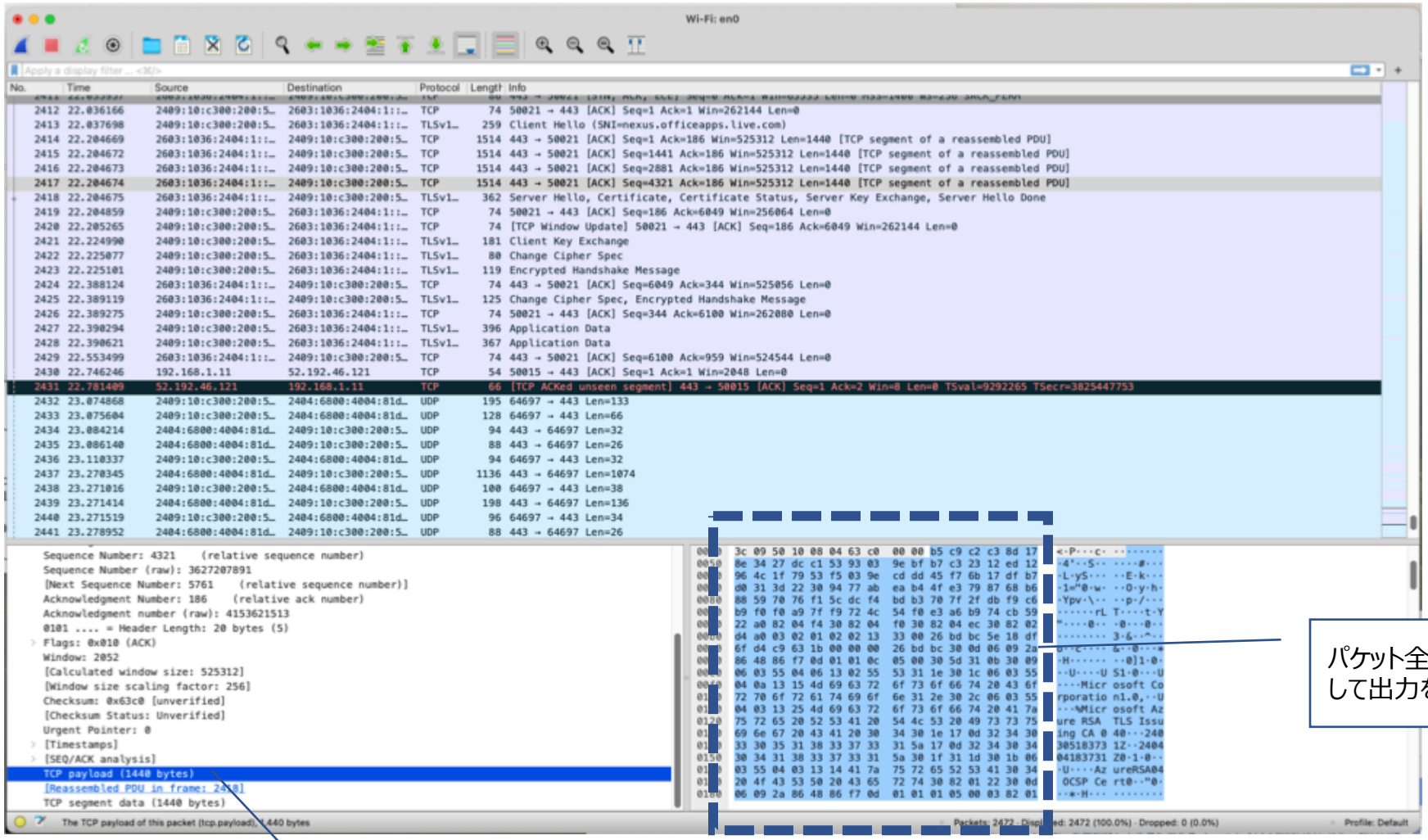
前ページ

これがアウトプット

今回は対象外

Figure 12: High-level Overview of Tag and Text Generation Processes

入力するパケット例


Wi-Fi: en0
No. Time Source Destination Protocol Length Info
2412 22.036166 2409:10:c300:200:5… 2603:1036:2404:1::… TCP 74 50021 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2413 22.037698 2409:10:c300:200:5… 2603:1036:2404:1::… TLSv1… 259 Client Hello (SNI=nexus.officeapps.live.com)
2414 22.204669 2603:1036:2404:1::… 2409:10:c300:200:5… TCP 1514 443 → 50021 [ACK] Seq=1 Ack=186 Win=525312 Len=1440 [TCP segment of a reassembled PDU]
2415 22.204672 2603:1036:2404:1::… 2409:10:c300:200:5… TCP 1514 443 → 50021 [ACK] Seq=1441 Ack=186 Win=525312 Len=1440 [TCP segment of a reassembled PDU]
2416 22.204673 2603:1036:2404:1::… 2409:10:c300:200:5… TCP 1514 443 → 50021 [ACK] Seq=2881 Ack=186 Win=525312 Len=1440 [TCP segment of a reassembled PDU]
2417 22.204674 2603:1036:2404:1::… 2409:10:c300:200:5… TCP 1514 443 → 50021 [ACK] Seq=4321 Ack=186 Win=525312 Len=1440 [TCP segment of a reassembled PDU]
2418 22.204675 2603:1036:2404:1::… 2409:10:c300:200:5… TLSv1… 362 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done
2419 22.204859 2409:10:c300:200:5… 2603:1036:2404:1::… TCP 74 50021 → 443 [ACK] Seq=186 Ack=6049 Win=256064 Len=0
2420 22.205265 2409:10:c300:200:5… 2603:1036:2404:1::… TCP 74 [TCP Window Update] 50021 → 443 [ACK] Seq=186 Ack=6049 Win=262144 Len=0
2421 22.224990 2409:10:c300:200:5… 2603:1036:2404:1::… TLSv1… 181 Client Key Exchange
2422 22.225077 2409:10:c300:200:5… 2603:1036:2404:1::… TLSv1… 80 Change Cipher Spec
2423 22.225101 2409:10:c300:200:5… 2603:1036:2404:1::… TLSv1… 119 Encrypted Handshake Message
2424 22.388124 2603:1036:2404:1::… 2409:10:c300:200:5… TCP 74 443 → 50021 [ACK] Seq=6049 Ack=344 Win=525056 Len=0
2425 22.389119 2603:1036:2404:1::… 2409:10:c300:200:5… TLSv1… 125 Change Cipher Spec, Encrypted Handshake Message
2426 22.389275 2409:10:c300:200:5… 2603:1036:2404:1::… TCP 74 50021 → 443 [ACK] Seq=344 Ack=6100 Win=262080 Len=0
2427 22.390294 2409:10:c300:200:5… 2603:1036:2404:1::… TLSv1… 396 Application Data
2428 22.390621 2409:10:c300:200:5… 2603:1036:2404:1::… TLSv1… 367 Application Data
2429 22.553499 2603:1036:2404:1::… 2409:10:c300:200:5… TCP 74 443 → 50021 [ACK] Seq=6100 Ack=959 Win=524544 Len=0
2430 22.746246 192.168.1.11 52.192.46.121 TCP 54 50015 → 443 [ACK] Seq=1 Ack=1 Win=2048 Len=0
2431 22.781409 52.192.46.121 192.168.1.11 TCP 66 [TCP ACKed unseen segment] 443 → 50015 [ACK] Seq=1 Ack=2 Win=8 Len=0 TSval=9292265 TSecr=3825447753
2432 23.074868 2409:10:c300:200:5… 2404:6800:4004:81d… UDP 195 64697 → 443 Len=133
2433 23.075604 2409:10:c300:200:5… 2404:6800:4004:81d… UDP 128 64697 → 443 Len=66
2434 23.084214 2404:6800:4004:81d… 2409:10:c300:200:5… UDP 94 443 → 64697 Len=32
2435 23.086140 2404:6800:4004:81d… 2409:10:c300:200:5… UDP 88 443 → 64697 Len=26
2436 23.110337 2409:10:c300:200:5… 2404:6800:4004:81d… UDP 94 64697 → 443 Len=32
2437 23.270345 2404:6800:4004:81d… 2409:10:c300:200:5… UDP 1136 443 → 64697 Len=1074
2438 23.271016 2409:10:c300:200:5… 2404:6800:4004:81d… UDP 100 64697 → 443 Len=38
2439 23.271414 2404:6800:4004:81d… 2409:10:c300:200:5… UDP 198 443 → 64697 Len=136
2440 23.271519 2409:10:c300:200:5… 2404:6800:4004:81d… UDP 96 64697 → 443 Len=34
2441 23.278952 2404:6800:4004:81d… 2409:10:c300:200:5… UDP 88 443 → 64697 Len=26
Sequence Number: 4321 (relative sequence number)
Sequence Number (raw): 3627207891
[Next Sequence Number: 5761 (relative sequence number)]
Acknowledgment Number: 186 (relative ack number)
Acknowledgment number (raw): 4153621513
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window: 2052
[Calculated window size: 525312]
[Window size scaling factor: 256]
Checksum: 0x63c0 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (1440 bytes)
[Reassembled PDU in frame: 2418]
TCP segment data (1440 bytes)
The TCP payload of this packet (tcp.payload), 1440 bytes
Packets: 2472 · Displayed: 2472 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
パケット全体をHex streamとして出力を取り出すことが可能
1440バイトのTCP payload

タグの出力例

24クラス、上位5クラスを表示

```
{'considered regular expected':
0.9683609760620078, 'malicious intent':
0.9615794211373029, 'typical':
0.9613007669189144, 'standard network':
0.9597006785861135, 'reference point':
0.9590239229010236}
```