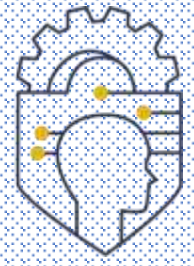
NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors



Investigating the Privacy Risk of using Robot Vacuum Cleaners in Smart Environments

Benjamin Ulsmå, Jia-Chun Lin, Ming-Chang Lee

Department of Information Security and Communication Technology

Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

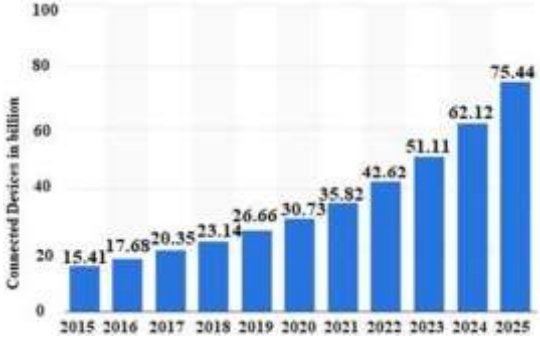
NTNU | Norwegian University of Science and Technology

Outline

- Introduction
- Related Work
- Research Gaps
- Research Objective
- Methodology
- Analysis Results and Identified Signatures
- Evaluation
- Conclusions and Future Work
- Acknowledgement

Introduction (1/2)

- The use of IoT devices in smart environments is rapidly expanding.
  - Common devices include robot vacuum cleaners, smart lighting, door locks, and air quality sensors.
  - These devices simplify tasks and enhance comfort.
  - They also improve quality of life through automation and personalized settings.



Introduction (2/2)

- Robot vacuum cleaners are popular for their autonomous navigation and learning capabilities.
  - Users can customize their operation via smartphone apps.
  - Integration with other IoT devices enhances functionality.
  - This allows optimized operations based on user presence and activity.

Related Work

- Previous research has focused on the security of robot vacuum cleaners through vulnerability assessments and penetration tests.
- Penetration testing of Roborock S7:
  - Sundström and Nilsson [10]: Evaluated Roborock S7 security, found vulnerability to DHCP starvation attacks, recommended basic network authentication.
- Laser Sensor Data Eavesdropping:
  - Sami et al. [17]: Used a side-channel attack on robot vacuum cleaner laser sensors to detect object vibrations and spoken words, identifying songs and TV shows with high accuracy.
- Cloud Service Security:
  - Ullrich et al. [19]: Assessed Neato robot vacuum cleaner's cloud service and application, identifying significant privacy risks due to weak cryptography and shared private keys.

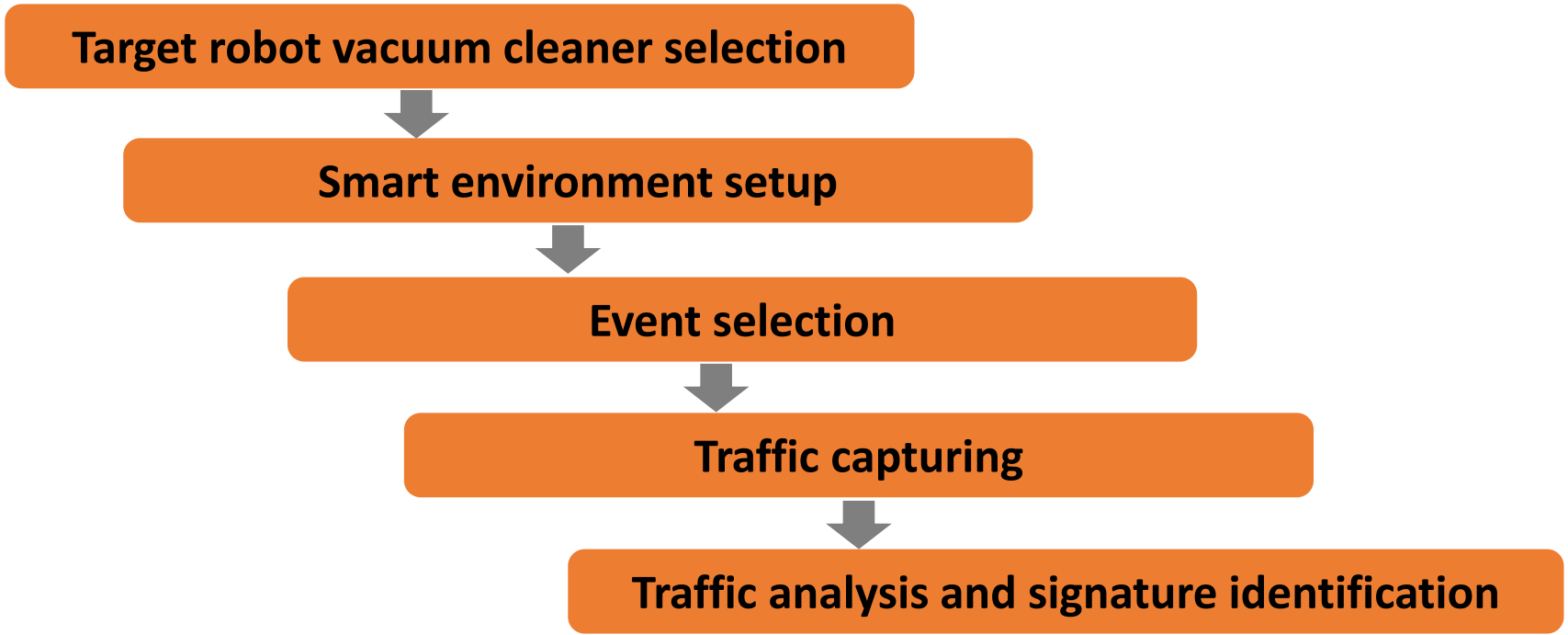
Research Gaps

- However, passive eavesdropping, which involves silently monitoring data traffic, remains underexplored and poses potential privacy risks.
- It is unclear what privacy information about users might be exposed from robot vacuum cleaners' unencrypted network header metadata.

Research Objective

Explore the risk of private information exposure in a smart environment by analyzing the network traffic metadata of a robot vacuum cleaner.

Methodology



Methodology - Target robot vacuum cleaner selection

- To choose a robot vacuum cleaner for our study, we surveyed various brands, including iRobot, Roborock, Neatsvor, Ecovacs, and iLife.
- We selected the iRobot Roomba i7, influenced by its popularity and positive reviews highlighting its features and reasonable price in 2023.
- Our findings may also apply to other vacuum cleaners with similar functionalities.

Fig. 1. The iRobot Roomba i7.

Methodology - Smart environment setup (1/2)

- A real smart environment in Oslo, Norway.
- Deployed and reset the iRobot Roomba i7 to factory default settings.

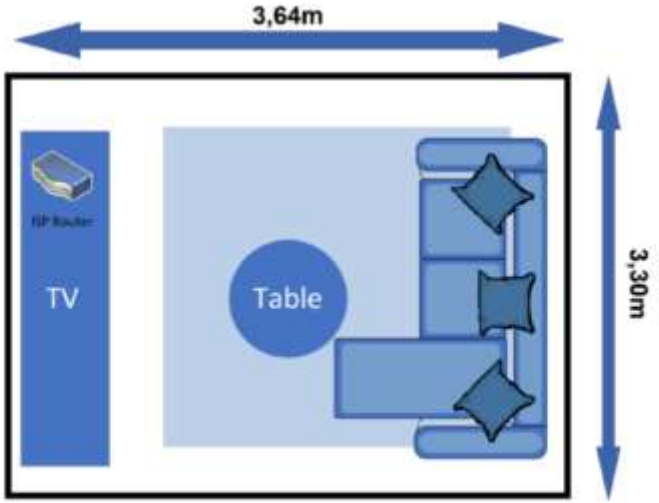


Fig. 2. The smart environment in Oslo, Norway.

Methodology - Smart environment setup (2/2)

- Replicated and forwarded traffic from the LAN switch to the capturing platform.

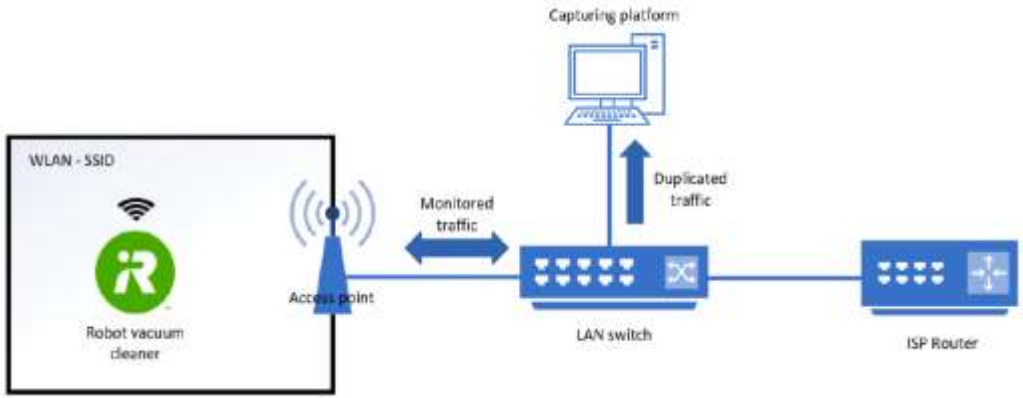


Fig. 3. The network infrastructure for passive eavesdropping.

Table 1. Details of all the devices used in our smart environment.

Device	Details
Capturing platform	Raspberry Pi 3B+ with Kali Linux
Analysis platform	HP Elitebook with Windows 11
Access point (AP)	TP-Link archer MR 200, version 5.30
LAN switch	Cisco catalyst 2960 series 8 port
ISP router	Sagemcom Telia

Methodology - Event selection

1. **Automated Cleaning**
   - Triggered by integration with third-party IoT systems or other smart devices such as smartphones.
   - Detect this event could indicate user absence and expose their routines.
2. **App-Triggered Cleaning**
   - Initiated via the iRobot app, revealing smartphone usage and users' daily routines.
3. **Scheduled Cleaning**
   - Starts based on a user-defined schedule, inferring user routines and absence.
4. **Physical-Triggered Cleaning**
   - Activated by pressing the "Clean" button, indicating user presence.
5. **App Engagement**
   - Occurs when the user interacts with the iRobot app on their smartphones.
6. **Bin Removal**
   - Happens when the vacuum cleaner's bin is removed, indicating user presence alongside the cleaner.

Methodology - Traffic capturing

- **Capture Setup**:
  - Used two TShark processes on Raspberry Pi: one for WAN traffic (eth0) and one for WLAN traffic (wlan1).
  - TShark is the command-line version of Wireshark, a widely used network protocol analyzer.
- **Preliminary Operation**:
  - Operated the vacuum cleaner for one month, ensuring that the traffic we collect was generated during the vacuum cleaner's operational state rather than during the setup phase.
- **Standby Traffic Capture**:
  - Afterwards, we conducted continuous traffic capture for 14 days without any physical or application interaction.
  - Standby traffic analysis: 49.2% DNS, 26.2% TCP (mainly TLS), and remaining ARP.
- **Filtering Process**:
  - Excluded DNS, TCP-keep-alive, ARP, DHCP, and NTP traffic.
  - Reduced packets from 5,052,284 to 4,010 (0.8% of traffic remained).
- **Event Traffic Capture**:
  - Triggered and recorded each of the six selected events, storing the traffic in a single file.
  - Repeated each event 10 times.

Methodology - Traffic analysis and signature identification

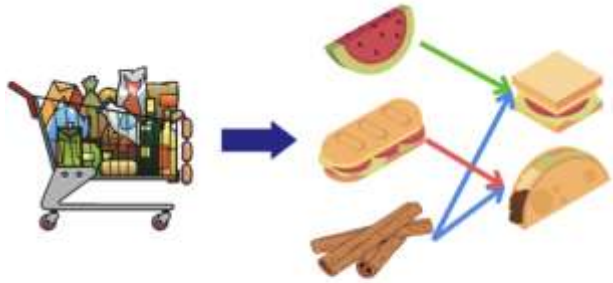
- We analyzed network traffic in two phases:
  1. **Protocol Identification**:
     - Imported event traffic files into Wireshark, used protocol hierarchy tool, and filtered out irrelevant traffic
     - Identified event-specific packets larger than 97 bytes.
  2. **Signature Identification**:
     - Searched for unique packets for each event, calculated total packets for each event, extracted the first few packet sizes from each event as a sequence, and discovered associations between different packet sizes using **Association Rule Learning (ARL).**
       - ARL is rule-based unsupervised machine learning method.
       - It is used to identify common associations or relationships among a set of items in a dataset.
       - ARL It is widely employed to discover which items tend to co-occur.

Methodology - Association Rule Learning (ARL)

The rule X → Y implies that whenever X occurs, Y is likely to occur as well.

The key metrics used in ARL are:

- **Support:** measures how frequently a particular item or itemset appears in the dataset.
- **Confidence:** This says how likely item B is purchased when item A is purchased, expressed as (A -> B).
- **Lift:** the strength of the association compared to random chance.



"93% of people who purchased item A also purchased item B"

$$\text{Support}(X) = \frac{\text{Number of transactions containing } X}{\text{Total number of transactions}}$$

$$\text{Confidence}(X \Rightarrow Y) = \frac{\text{Support}(X \text{ and } Y)}{\text{Support}(X)}$$

$$\text{Lift}(X \Rightarrow Y) = \frac{\text{Confidence}(X \Rightarrow Y)}{\text{Support}(Y)}$$

Analysis Results and Identified Signatures (1/7)

- **Automated cleaning**
  - Identified two consistent DNS response packets:
    - “0550315.ingest.sentry.io”
    - “s3.amazonaws.com”
  - The average total number of packets (2425.4) had a high standard deviation (767.27), making the total number of packets an unreliable signature for this event.
  - A consistent pattern: six packet sizes [S175, S176, S179, S446, D1100, D1106]
  - Attempts to find an alternative, smaller subset of packet sizes for signatures were unsuccessful, as ARL consistently yielded the same set of six packet sizes.

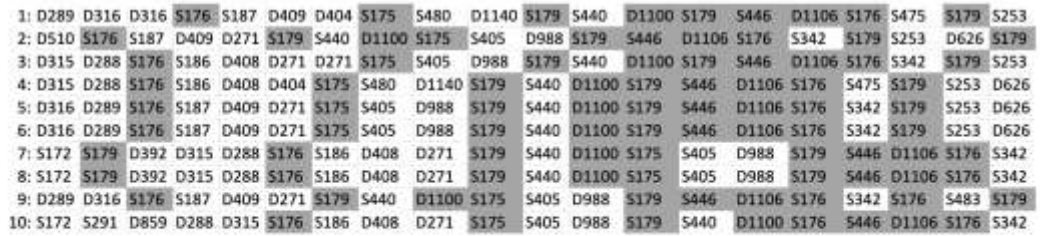


Fig. 4. Extraction of the first 20 packet sizes from each of the ten automated cleaning events performed in the Oslo environment. The strict signature we identified, representing the consistent pattern found in all events, is highlighted in grey.

Analysis Results and Identified Signatures (2/7)

- **App-triggered cleaning**
  - The same two DNS response packets are identified.
  - The total number of packets of an App-triggered cleaning event was not a reliable indicator for event identification, given the high standard deviation observed.
  - A consistent pattern: three packet sizes [S176, S179, D1239]
  - The following three sets of packet sizes could serve as alternative, less strict signatures:
    - [S176, D1239]
    - [S179, D1239]
    - [S176, S179]

1:	D208	D288	D315	S176	S186	D408	S176	S1285	D555	S175	S561	D1239	S179	S439	D1099	S179	S445	D1105	S176	S625
2:	S179	S160	D346	D209	D289	D316	S176	S187	D409	S176	S1201	D555	S175	S561	D1239	S179	S439	D1099	S179	S445
3:	D208	D289	D316	S176	S187	D409	S176	S1514	S1064	D555	S175	S561	D1239	S179	S439	D1099	S179	S445	D1105	S176
4:	S179	S160	D346	D208	D288	D315	S176	S186	D408	S176	S1200	D055	S170	S061	D1239	S179	S439	D1099	S179	S445
5:	S179	S160	D346	D208	D288	D315	S176	S186	D408	S176	S1200	D555	S175	S561	D1239	S179	S439	D1099	S179	S445
6:	S179	S160	D346	S172	S233	D551	D209	D289	D316	S176	S187	D409	S176	S1201	D555	S175	S561	D1239	S179	s439
7:	D209	D315	D288	S176	S186	D408	S176	S1201	S179	S160	D346	D055	S175	S061	D1239	S179	S439	D1099	S179	S445
8:	S179	S160	D346	D209	D316	D289	S176	S187	D409	S176	S1201	D555	S179	S439	D1099	S175	S561	D1239	S179	S445
9:	D209	D+510	S176	S1201	S176	S187	D409	D555	S175	S561	D1239	S179	S439	D1109	S179	S445	D1105	S176	S625	S179
10:	D209	D280	D315	S176	S1201	S176	S186	D408	D555	S175	S561	D1239	S179	S439	D1099	S179	S445	D1105	S176	S625

Fig. 5. Extraction of the first 20 packet sizes from each of the ten App-triggered cleaning events performed in the Oslo environment. The strict signature we identified is highlighted in grey.

Analysis Results and Identified Signatures (3/7)

- **Scheduled cleaning**
  - We observed the same two DNS responses across all 10 scheduled cleaning events.
  - A consistent pattern: six packet sizes [176, S179, S253, S448, D626, D1108]
  - Unable to identify another smaller set of packet sizes as an alternative signature because ARL consistently grouped these six packet sizes together.

1:	S179	S160	D346	S175	S482	D1142	S179	S441	D1101	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108
2:	S175	S482	D1142	S179	S442	D1102	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108	S179	S448	D1108
3:	S179	S160	D346	S175	S482	D1142	S179	S442	D1102	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108
4:	S179	S442	D1102	S175	S482	D1142	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108	S179	S448	D1108
5:	S179	S253	D626	S179	S448	D1108	S179	S448	D1108	S176	S674	S176	S812	D151	S583	D1494	D1494	D1494	D1210	S192
6:	S179	S442	D1102	S175	S482	D1142	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108	S179	S448	D1108
7:	S179	S160	D346	S175	S482	D1142	S179	S442	D1102	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108
8:	S179	S160	D346	S175	S482	D1142	S179	S442	D1102	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108
9:	S179	S160	D346	S175	S482	D1142	S179	S442	D1102	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108
10:	S175	S482	D1142	S179	S442	D1102	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108	S179	S448	D1108

Fig. 6. Extraction of the first 20 packet sizes from each of the ten scheduled cleaning events in the Oslo environment. The strict signature we identified is highlighted in grey.

Analysis Results and Identified Signatures (4/7)

- **Physical-triggered cleaning**
  - We also observed the same two DNS responses across all the events.
  - A consistent pattern: nine packet sizes [S175, S176, S179, D626, D903, S253, S290, S369, D1106]
  - However, a less strict signature could not be established due to the strong association among these nine packet sizes.

1:	S179	S440	D1100	S179	S448	D1106	S176	S475	S175	S369	D903	S176	S290	S179	S253	D626	S179	S446	D1106	S179
2:	S179	S159	D345	S179	S446	D1106	S176	S290	S175	S369	D903	S176	S290	S179	S253	D626	S172	S179	D392	S179
3:	S179	S160	D346	S179	S440	D1100	S179	S446	D1106	S175	S369	D903	S176	S290	S176	S290	S179	S253	D626	S179
4:	S179	S160	D346	S179	S440	D1100	S179	S446	D1106	S175	S369	D903	S176	S290	S176	S290	S179	S253	D626	S179
5:	S179	S440	D1100	S179	S446	D1106	S176	S290	S175	S369	D903	S176	S290	S179	S253	D626	S179	S446	D1106	S179
6:	S179	S440	D1100	S179	S446	D1106	S175	S369	D903	S176	S290	S176	S290	S179	S253	D626	S179	S446	D1106	S179
7:	S172	S179	D392	S179	S446	D1106	S176	S290	S175	S369	D903	S176	S290	S179	S253	D626	S179	S446	D1106	S179
8:	S179	S440	D1100	S179	S446	D1106	S176	S290	S175	S369	D903	S176	S290	S179	S253	D626	S179	S446	D1106	S179
9:	S179	S440	D1100	S179	S448	D1106	S176	S290	S175	S369	D903	S172	S233	D551	S176	S290	S179	S253	D626	S179
10:	S179	S159	D345	S179	S440	D1100	S179	S446	D1106	S175	S369	D903	S176	S290	S176	S290	S179	S253	D626	S179

Fig. 7. Extraction of the first 20 packet sizes from each of the ten physical-triggered cleaning events in the Oslo environment. The strict signature we identified is highlighted in grey.

Analysis Results and Identified Signatures (5/7)

- **App engagement**
  - For our analysis, we activated and interacted with the iRobot application, without focusing on any specific action.
  - No DNS packets were observed during the event.
  - A consistent pattern: five packet sizes [S140, S174, S176, D333, D151]
  - We also found another less strict signature: [S140, S174, S176, D333]

1:	D209	D315	D288	S298	D408	S176	S1053	D1514	D1514	D1084	D1514	D1514	D1111	S174	S140	D333	S175	S1514	S569	D1514
2:	D208	D316	D289	S176	S187	D409	S176	S1052	D1514	D1514	D1112	D1514	D1514	D1085	S174	S140	D333	S175	S1514	S570
3:	D208	D537	S176	S186	D408	S176	S1052	D1514	D1514	D1085	D1514	D1514	D1112	S174	S140	D333	S175	S1514	S570	D1514
4:	S179	S160	D346	D208	D289	D316	S176	S187	D409	S176	D1052	D1514	D1514	D1111	D1514	D1514	D1084	S174	S140	D333
5:	D209	D315	D288	S176	S186	D408	S176	S1053	D1514	D1514	D1085	D1514	D1514	D1112	S174	S140	D333	S175	S1514	S570
6:	D205	D289	D316	S176	S1046	S176	S187	D409	D1514	D1514	D1112	D1514	D1514	D1085	S174	S140	D333	S175	S1514	S570
7:	D207	D315	D288	S176	S186	D408	S176	S1051	D1514	D1514	D1085	D1514	D1514	D1112	S174	S140	D333	S175	S1514	S570
8:	S179	S159	D345	D207	D289	D316	S176	S187	D409	S176	S1051	D1514	D1514	D1514	D1514	D1514	D654	S174	S140	D333
9:	D207	D508	S176	S1050	S176	S186	D408	D1514	D1514	D1112	D1514	D1514	D1085	S174	S140	D333	S175	S1514	S570	D1514
10:	D208	D316	D289	S176	S1052	S176	S187	D409	S172	S219	D505	D1514	D1514	D1085	D1514	D1514	D1112	S174	S140	D333

Fig. 8. Extraction of the first 20 packet sizes from the ten App engagement events in the Oslo environment. The strict signature we identified is highlighted in grey.

Analysis Results and Identified Signatures (6/7)

- **Bin removal**
  - A consistent pattern: two packet sizes [S186, D410].
  - Given that the signature consists only two packet sizes, we did not pursue any less strict signatures for this event.

1: D208	D288	D315	S176	S186	D408	S176	S1052	S179	S450	D1110	S179	S186	D410	S179	S450	D1110	S179	S185	D409
2: S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S186	D410								
3: S179	S160	D346	S172	S233	D551	S179	S450	D1110	S179	S187	D411	S179	S450	D1110	S179	S450	D1110	S179	S450
4: S179	S492	D1222	S179	S450	D1110	S179	S186	D410											
5: S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S186	D410								
6: S603	D1220	S179	S448	D1108	S179	S186	D410												
7: S179	S490	D1220	S179	S448	D1108	S179	S186	D410											
8: S325	D505	S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S186	D410	S172	S179	D392			
9: S179	S490	D1220	S179	S448	D1108	S179	S186	D410											
10: S179	S490	D1220	S179	S448	D1108	S179	S448	D1108	S179	S448	D1108	S179	S186	D410					

Fig. 9. The first few packet sizes extracted from the ten bin removal events in the Oslo environment. The identified signature is highlighted in grey.

Analysis Results and Identified Signatures (7/7)

- **Summary**
  - Based on our analysis, the following two DNS responses were consistently found in all cleaning events, but not in other events.
    - A DNS response for “0550315.ingest.sentry.io”.
    - A DNS response for “s3.amazonaws.com”.
  - Therefore, while these DNS responses can indicate if a cleaning event occurs, they cannot distinguish between different types of cleaning events.
  - Each strict signature is unique to its corresponding event
    - even though there is some slight overlapping between different event.

Table 2. All identified signatures for each event.

Event	Identified signatures
Automated cleaning	Strict: [S175, S176, S179, S446, D1100, D1106] Less strict: none
App-triggered cleaning	Strict: [S176, S179, D1239] Less strict: [S176, D1239] or [S179, D1239]
Scheduled cleaning	Strict: [S176, S179, S253, S448, D626, D1108] Less strict: none
Physical-triggered cleaning	Strict: [S175, S176, S179, D626, D903, S253, S290, S369, D1106] Less strict: none
App engagement	Strict: [S140, S174, S176, D333, D1514] Less strict: [S140, S174, S176, D333]
Bin removal	Strict: [S186, D410] Less strict: none

Evaluation – Test environment

- We conducted a series of tests in another smart environment located in Drammen, Norway.
- Similar to the Oslo environment, we established a wired and wireless network infrastructure, Internet connection, set up the Raspberry Pi device for traffic eavesdropping, etc.
- This setup allowed us to conduct traffic eavesdropping from this environment.

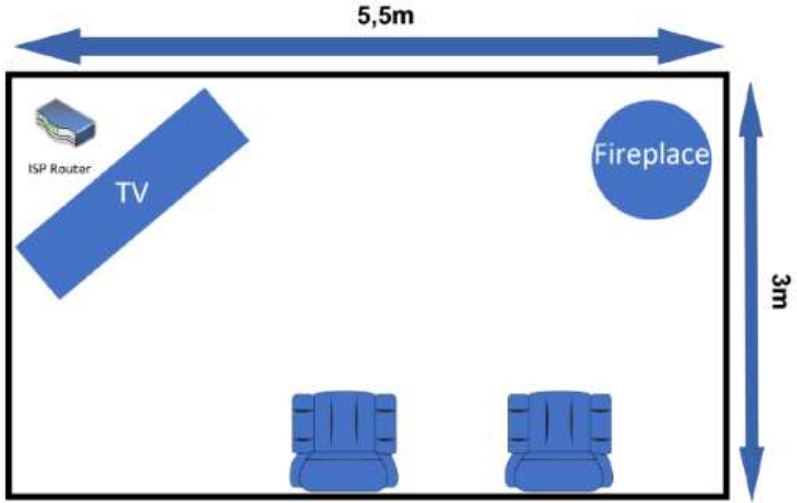


Fig. 10. The smart environment in Drammen, Norway.

Evaluation – Packet size sequences

Automated cleaning

1:	D315	D288	S176	S186	D408	D404	S175	S425	D982	S179	S439	D1099	S179	S445	D1105	S176	S474	S176	S615	S179
2:	D289	D316	S176	S187	D409	D404	S175	S449	D1046	S179	S440	D1100	S179	S446	D1106	S176	S475	S179	S253	D626
3:	S172	S288	D714	D316	D289	S176	S187	D409	D404	S175	S425	D982	S179	S439	D1099	S179	S445	D1105	S176	S474
4:	D315	D288	S176	S186	D408	D404	S179	S439	D1099	S175	S425	D982	S179	S445	D1105	S176	S615	S179	S253	D626
5:	D289	D316	S176	S187	D409	D404	S175	S410	D936	S179	S446	D1106	S176	S475	S176	S616	S179	S253	D626	S179
6:	D289	D316	D316	S176	S187	D409	D404	S175	S449	D1046	S179	S440	D1100	S179	S446	D1106	S176	S475	S176	S616
7:	D288	D315	S176	S186	D408	D404	S175	S449	D1046	S179	S440	D1100	S179	S446	D1106	S176	S475	S176	S616	S179
8:	D289	D316	S297	D409	D404	S179	S440	D1100	S175	S449	D1046	S179	S446	D1106	S176	S475	S176	S616	S179	S253
9:	S172	S233	D551	D315	D288	S176	S186	D408	D404	S175	S449	D1046	S179	S440	D1100	S179	S446	D1106	S176	S475
10:	D289	D316	S176	S187	D409	D404	S179	S440	D1100	S175	S449	D1046	S179	S446	D1106	S176	S475	S176	S616	S179

App-triggered cleaning

1:	D209	D315	D288	S176	S186	D408	S176	S949	D503	S175	S540	D1200	S179	S440	D1100	S179	S446	D1106	S176	S715
2:	D208	D289	D316	S176	S187	D409	S176	S1514	S227	D503	S175	S509	D1106	S179	S440	D1100	S179	S446	D1106	S574
3:	D209	D316	D289	S176	S187	D409	S176	S1514	S1514	S787	D503	D503	S175	S524	D1152	S179	S440	D1100	S179	S446
4:	D209	D288	D315	S176	S1085	S176	S186	D408	D503	S175	S524	D1152	S179	S440	D1100	S179	S446	D1106	S176	S574
5:	S179	S160	D346	D209	D316	D289	S176	S1514	S256	S176	S187	D409	D503	S175	S540	D1200	S179	S440	D1100	S179
6:	S172	S179	D392	D208	D315	D288	S176	S186	D408	S176	S1359	D503	S175	S509	D1106	S179	S440	D1100	S179	S446
7:	D207	D289	D316	S176	S187	D409	S176	S1514	S1514	S1514	S1514	S1514	S205	D318	S175	S398	D869	S179	S440	D1100
8:	D207	D315	D288	S176	S186	D408	S176	S1514	S1514	S926	D318	S175	S398	D869	S179	S440	D1100	S179	S446	D1106
9:	D208	D315	D288	S176	S985	S176	S186	D408	D208	S176	D316	D289	S985	S176	S187	D409	D503	S175	S509	D1106
10:	D208	D315	D288	S176	S186	D408	S176	S1514	S255	D503	S175	S509	D1106	S179	S440	D1100	S179	S446	D1106	S176

Scheduled cleaning

1:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S477	S179	S253	D626	S179	S448	D1108	S179	S448	D1108
2:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S618	S179	S253	D626	S176	S835	S179	S448	D1108	S179
3:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S477	S176	S618	S179	S253	D626	S176	S835	S179	S448
4:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S477	S176	S618	S179	S253	D626	S179	S448	D1108	S176
5:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S618	S179	S253	D626	S179	S448	D1108	S176	S835	S179
6:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S477	S176	S618	S179	S253	D626	S176	S835	S179	S448
7:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S477	S176	S618	S179	S253	D626	S179	S448	D1108	S179
8:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S477	S176	S618	S179	S253	D626	S179	S448	D1108	S179
9:	S172	S234	D552	S175	S466	D1094	S179	S448	D1108	S176	S477	S176	S618	S179	S253	D626	S179	S448	D1108	S179
10:	S175	S466	D1094	S179	S442	D1102	S179	S448	D1108	S176	S618	S179	S253	D626	S176	S835	S179	S448	D1108	S179

Physical-triggered cleaning

1:	S175	S314	D745	S179	S447	D1107	S179	S447	D1107	S179	S445	D1105	S179	S253	D626	S179	S445	D1105	S179	S445
2:	S179	S446	D1106	S176	S290	S175	S338	D809	S176	S290	S179	S253	D626	S179	S446	D1106	S179	S446	D1106	S176
3:	S179	S440	D1100	S179	S446	D1106	S176	S290	S175	S338	D809	S176	S290	S179	S253	D626	S179	S446	D1106	S179
4:	S179	S159	D345	S179	S440	D1100	S179	S446	D1106	S175	S338	D809	S176	S290	S176	S290	S179	S253	D626	S179
5:	S179	S439	D1099	S179	S445	D1105	S175	S314	D745	S176	S289	S176	S289	S179	S253	D626	S179	S445	D1105	S179
6:	S179	S439	D1099	S179	S445	D1105	S175	S314	D745	S176	S430	S179	S253	D626	S179	S445	D1105	S179	S445	D1105
7:	S179	S160	D346	S179	S439	D1099	S179	S445	D1105	S175	S314	D745	S176	S289	S176	S289	S179	S253	D626	S179
8:	S172	S233	D551	S179	S439	D1099	S179	S445	D1105	S175	S314	D745	S176	S289	S176	S289	S179	S253	D626	S179
9:	S179	S440	D1100	S179	S446	D1106	S175	S338	D809	S176	S574	S176	S431	S179	S253	D626	S176	S648	S179	S446
10:	S179	S440	D1100	S179	S446	D1106	S175	S338	D809	S176	S290	S176	S290	S179	S253	D626	S179	S446	D1106	S179

App engagement

1:	D209	D288	D315	S296	D408	S176	S1514	S376	D879	D852	S174	S140	D333	S175	S469	D904	S175	S346	D848	
2:	D209	D289	D316	S176	S187	D409	S176	S1514	S131	D852	D879	S174	S140	D333	S175	S469	D904	S175	S346	D848
3:	D209	D315	D288	S176	S186	D408	S176	S1514	S131	D879	D852	S174	S140	D333	S175	S469	D904	S175	S346	D848
4:	D209	D289	D316	S176	S1514	S159	S176	S187	D409	D852	S174	D879	S140	D333	S175	S469	D904	S175	S346	D848
5:	S172	S179	D392	D208	D315	D288	S176	S186	D408	S176	S987	D825	D852	S174	S140	D333	S175	S466	D877	S175
6:	D208	D289	D316	S176	S187	D409	S176	S1514	S158	D852	D825	S174	S140	D333	S175	S466	D877	S175	S346	D848
7:	D208	D288	D315	S176	S1361	S176	S186	D408	D852	D825	S174	S140	D333	S175	S466	D877	S175			
8:	D208	D289	D316	S176	S187	D409	S176	S1514	S98	D851	D824	S174	S140	D333	S175	S465	D876	S175	S346	D848
9:	D208	D288	D315	S176	S1514	S126	S176	S186	D408	D825	D852	S174	S140	D333	S175	S466	D877	S175	S346	D848
10:	D208	D289	D316	S176	S187	D409	S176	D1389	D825	D852	S174	D852	S140	D333	S175	S466	D877	S175	S346	D848

Bin removal

1:	S179	S448	D1108	S179	S187	D411														
2:	S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S186	D410								
3:	S172	S293	D861	S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S186	D410					
4:	S179	S448	D1108	S179	S187	D411	S172	S179	D392	S179	S448	D1108	S179	S186	D410					
5:	S172	S219	D505	S179	S448	D1108	S179	S187	D411	S172	S234	D552								
6:	S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S448	D1108	S179	S489	D1219					
7:	S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S186	D410								
8:	S561	D1108	S179	S187	D411	S179	S448	D1108	S179	S448	D1108	S179	S448	D1108	S179	S186	D410			
9:	S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S448	D1108	S179	S448	D1108	S179	S186	D410		
10:	S179	S448	D1108	S179	S187	D411	S179	S448	D1108	S179	S186	D410								

Fig. 11. The first few packet sizes extracted from each of the 60 events triggered in the Drammen environment.

Evaluation - Metrics

- True positive (*TP*)
- False positive (*FP*)
- False negative (*FN*)

- Precision = $\frac{TP}{TP+FP}$
- Recall = $\frac{TP}{TP+FN}$
- F1 = $2\times\frac{P\times R}{P+R}$

Evaluation – Event Identification Results (1/3)

Table 3. The *TP*, *FP*, and *FN* results of each signature.

Signature	Associated event	*TP*	*FP*	*FN*
[S175, S176, S179, S446, D1100, D1106]	Automated cleaning	6	10	4
[S176, S179, D1239]	App-triggered cleaning	0	0	10
[S176, D1239]	App-triggered cleaning	0	0	10
[S179, D1239]	App-triggered cleaning	0	0	10
[S176, S179, S253, S448, D626, D1108]	Scheduled cleaning	10	0	0
[S175, S176, S179, D626, D903, S253, S290, S369, D1106]	Physical-triggered	0	0	10
[S140, S174, S176, D333, D1514]	App engagement	0	0	10
[S140, S174, S176, D333]	App engagement	10	0	0
[S186, D410]	Bin removal	7	0	3

Evaluation – Event Identification Results (2/3)

- 5 out of the 9 identified signatures failed to accurately recognize their associated events within the Drammen environment, yielding a Precision of 0 and a recall of 0.
  - 3 signatures are associated with the App-triggered cleaning event, indicating that none of these signatures can serve as a reliable indicator for recognizing the app-triggered cleaning event.
  - The only signature identified for the physical-triggered cleaning could not recognize any physical-triggered cleaning event occurring in the Drammen environment, making it an unreliable indicator.

Table 4. The event identification results of each signature.

Signature	Associated event	P	R	$F1$
[S175, S176, S179, S446, D1100, D1106]	Automated cleaning	0.375	0.6	0.462
[S176, S179, D1239]	App-triggered cleaning	0	0	undefined
[S176, D1239]	App-triggered cleaning	0	0	undefined
[S179, D1239]	App-triggered cleaning	0	0	undefined
[S176, S179, S253, S448, D626, D1108]	Scheduled cleaning	1	1	1
[S175, S176, S179, D626, D903, S253, S290, S369, D1106]	Physical-triggered	0	0	undefined
[S140, S174, S176, D333, D1514]	App engagement	0	0	undefined
[S140, S174, S176, D333]	App engagement	1	1	1
[S186, D410]	Bin removal	1	0.7	0.824

Evaluation – Event Identification Results (3/3)

- Although the App engagement event could not be identified using the strict signature [S140, S174, S176, D333, D1514], it was successfully identified using the less strict signature [S140, S174, S176, D333], achieving an F1-score of 1 without introducing any false positives or false negatives.
-
- If any malicious individuals are aware of these reliable signatures, they could determine when a household schedules a cleaning, when a user interacts with their iRobot application on their smartphones, and whether the user is present in their homes to remove the bin from their iRobot Roomba i7.

Table 4. The event identification results of each signature.

Signature	Associated event	P	R	$F1$
[S175, S176, S179, S446, D1100, D1106]	Automated cleaning	0.375	0.6	0.462
[S176, S179, D1239]	App-triggered cleaning	0	0	undefined
[S176, D1239]	App-triggered cleaning	0	0	undefined
[S179, D1239]	App-triggered cleaning	0	0	undefined
[S176, S179, S253, S448, D626, D1108]	Scheduled cleaning	1	1	1
[S175, S176, S179, D626, D903, S253, S290, S369, D1106]	Physical-triggered	0	0	undefined
[S140, S174, S176, D333, D1514]	App engagement	0	0	undefined
[S140, S174, S176, D333]	App engagement	1	1	1
[S186, D410]	Bin removal	1	0.7	0.824

Conclusions and Future Work

- According to our analysis, certain identified signatures can accurately recognize events.
  - Examples: scheduled cleaning, application engagement, and bin removal.
  - This capability implies that malicious individuals could exploit these signatures to further infer user habits and routines.

- Our study highlights the urgent need for enhanced measures to protect user privacy and advocates for a comprehensive approach to secure robot vacuum cleaners.

- In our future work, we aim to develop efficient solutions to protect robot vacuum cleaners from passive eavesdropping attacks and to create advanced traffic analysis methods to assess potential privacy risks.

Acknowledgement

- The authors thank the anonymous reviewers for their reviews and valuable suggestions to this paper.

- This work has received funding from the Research Council of Norway through the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) project no. 310105.

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

Thank you very much for your attention

Any questions?