1. Survey recent IDS systems and methods for IoT networks based on ML

2. Analyze different aspects of study that should be taken into consideration during the design of an IDS for IoT

3. Propose an IDS taxonomy

4. Discuss open issues and research challenges with new security solutions.
Introduction

Challenges & Security issues in IoT networks

- Restricted device capabilities
- Presence of many standards
- Limited computing power
- High number of interconnected devices
- Presence of malware, spyware and eavesdroppers

Critical infrastructures, such as transportation, healthcare systems and household appliances can lead to dreadful consequences when subject to attacks

TAXONOMY AND CHALLENGES IN ML-BASED APPROACHES TO DETECT ATTACKS IN THE IOT
Traditional security approaches and countermeasures

These approaches may fail to defend IoT environments due to the mentioned challenges and vulnerabilities

Intrusion Detection Systems (IDSs) are proposed and designed to detect these attacks and protect IoT networks overcoming restrictions

Assisted by Machine Learning

Cryptography...

Intelligent Tool to deal with Big Data
3 Related Work

1. Some reviews have been conducted regarding intrusion detection in the fields of cloud computing, Wireless Sensor Networks (WSN) and traditional networks.

2. Few surveys are focused on intrusion detection methods in IoT environments.

3. Most of them overlook many aspects that are needed for studying an IDS.

4. These surveys are used to build our taxonomy & indicate missing aspects researchers must take into consideration while developing a new system.
Proposed taxonomy based on attributes used to design an IDS
Intrusion Detection in IoT

16 recent published papers from 2016 to 2019 were reviewed & classified, based on:

Two published papers as an example

<table>
<thead>
<tr>
<th>Ref</th>
<th>Method</th>
<th>Placement Strategy</th>
<th>Detection Method</th>
<th>Attack Type</th>
<th>IoT Scenario</th>
<th>Machine Learning</th>
<th>Study Methodology</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Ref</th>
<th>Detection Accuracy</th>
<th>Classification Accuracy</th>
<th>TPR</th>
<th>FPR</th>
<th>TNR</th>
<th>FNR</th>
<th>ROC curves</th>
<th>Processing time</th>
<th>Energy consumption</th>
<th>Computation overhead</th>
<th>Real-time detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>[43]</td>
<td>-</td>
<td>99%</td>
<td>99.4%</td>
<td>0.6%</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Offline</td>
</tr>
<tr>
<td>[44]</td>
<td>94.25%</td>
<td>85.05%</td>
<td>35.47%</td>
<td>5.74%</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Real-time</td>
</tr>
</tbody>
</table>
6 Open Issues and Research Challenges

Limitations of surveyed solutions

- Typical aspects
  - Carry out a detailed study on the advantages and disadvantages of the previously used aspects
  - Study methodology

- Attack detection
  - Study wide range of attack types rather than focusing on known ones

- Emerging technologies
  - IEEE802.15.4
  - BLE
  - WirelessHART
  - Z-wave
  - 6LoWPAN
  - CoAP, MQTT...

- Performance analysis
  - Energy and power of network nodes
  - Scalability, hardware limitations of nodes
  - Delay-sensitive services
  - ROC curves

TAXONOMY AND CHALLENGES IN ML-BASED APPROACHES TO DETECT ATTACKS IN THE IOT
Further lines for research

Requirements

• Taxonomy aspects are a must for the classification, categorization, improvement & analysis for the new developed methods

Generative Adversarial Network (GAN)

New Solution

• Evade and deceive any IDS
• Fool machine learning algorithms
Open Issues & Research Challenges

Further lines for research

New Solution  →  Challenge-response mechanisms

Watermarking

- Lightweight
- Less energy consumption
- Implement anomaly detection
- Solution for: data integrity, confidentiality, secure transmission, authentication, etc.
- No additional overhead on network communication and storage capacity of nodes
- Reduce end-to-end delay
Due to weak designs, low computational capabilities, and faulty protocol implementations found in IoT networks, traditional security techniques cannot be implemented.

Intrusion Detection Systems (IDSs) are designed to detect malicious activities to protect IoT networks.

Enormous quantity of data generated in these networks lead to the need of intelligent tools to assist IDSs (Machine Learning).

IDSs need to study detection rates, false positive rates, real-time detection, computation overhead and energy consumption in a combined manner.

Researchers must consider all aspects while designing and implementing a new IDS.
Conclusion & Recommendations

- More research should be conducted to cover all attack types and recent IoT technologies.
- Research efforts are needed to find the optimal placement strategies to compute machine learning-based detection that could benefit to the security of IoT networks.
- Watermarking algorithms are recommended to be deployed that are much lighter and require less power, storage and computational capabilities.