Introduction

Title: An adaptive intrusion detection and prevention system for Internet of Things

Researchers: Sheikh Tahir Bakhsh , Saleh Alghamdi, Rayan A Alsemmeari and Syed Raheel Hassan

Presentation: Prathyush Turaga

Professor: Dr. Tommy Dang

Overview

- What is an IoT
- Basic use cases of IoT -> Home based (Alexa), Edge devices (Farms), Power Stations, Water Supply systems (Dams) etc
- Need for Security of IoT
- Intrusion Detection and Prevention System for IoT (IDPIoT)
- Types of IDS systems -> Host-based, Network-based, Hybrid-based
- IDS Models -> Signature-based model, Anomaly detection model
- IoT Devices have limited memory, computation and processing power
- More than 360 IoTs platforms use 100 protocols

Related Works

- Snort -> Open-source, Cross-platform, network-based IDS, signature-based model, database containing rules & policies
- PAYL (Payload-based Anomaly detector) -> Train with normal application payload and compare it for detected intrusions
- HIDE (Hierarchal Intrusion Detection) -> network-based system, anomaly detection model, divide network traffic into zones and report it through agents and analyze it with neural networks.
- KMNP (K-means clustering based intrusion detection protocol) -> 2-phase technique (k-means Clustering and Naive Bayes classifying of malicious and non-malicious data)
- MINDS (Minnesota Intrusion Detection System) -> mining technique, detects through packet header information
- Graphics processor unit (GPU)-based hybrid multi-pattern algorithm (HMA) - process network traffic by supporting parallelism with GPU

Similar Applications & Current Limitations

- Many of current IDS systems focus on signature-based model while there is need for anomaly detection model.

Justification for Proposed Solution

Why do we need it

What's unique about it

How is it different

- Proposed IDPIoT (Intrusion Detection and Prevention System for IoT) is implemented in middle, between IoT devices and router installed in a gateway.
- Hybrid IDS (signature + anomaly model)
- Prevention System isolates affected IoT device in case of attack

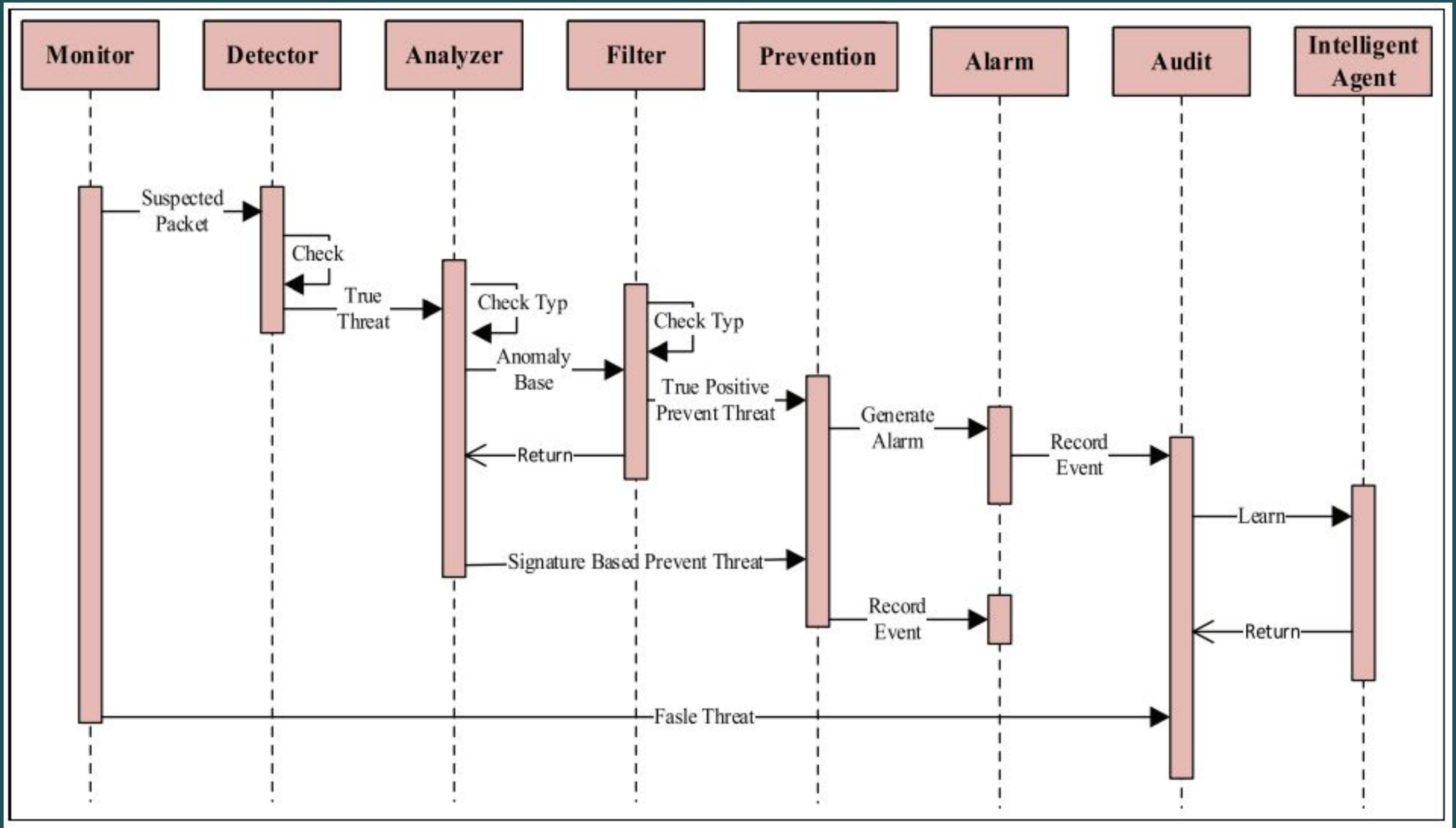
Proposed Solution. How does it work

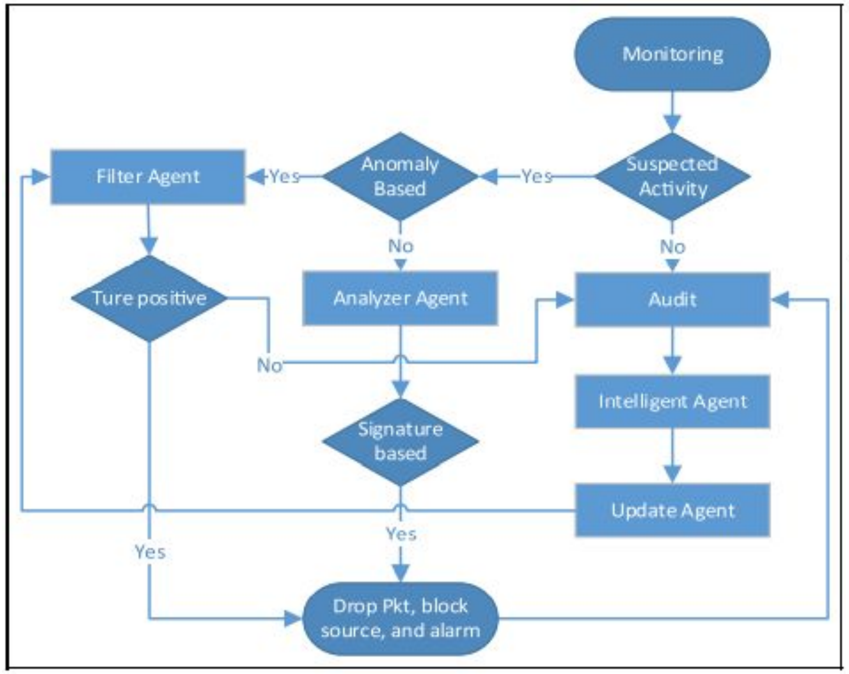
Stages of Intrusion detection and Prevention

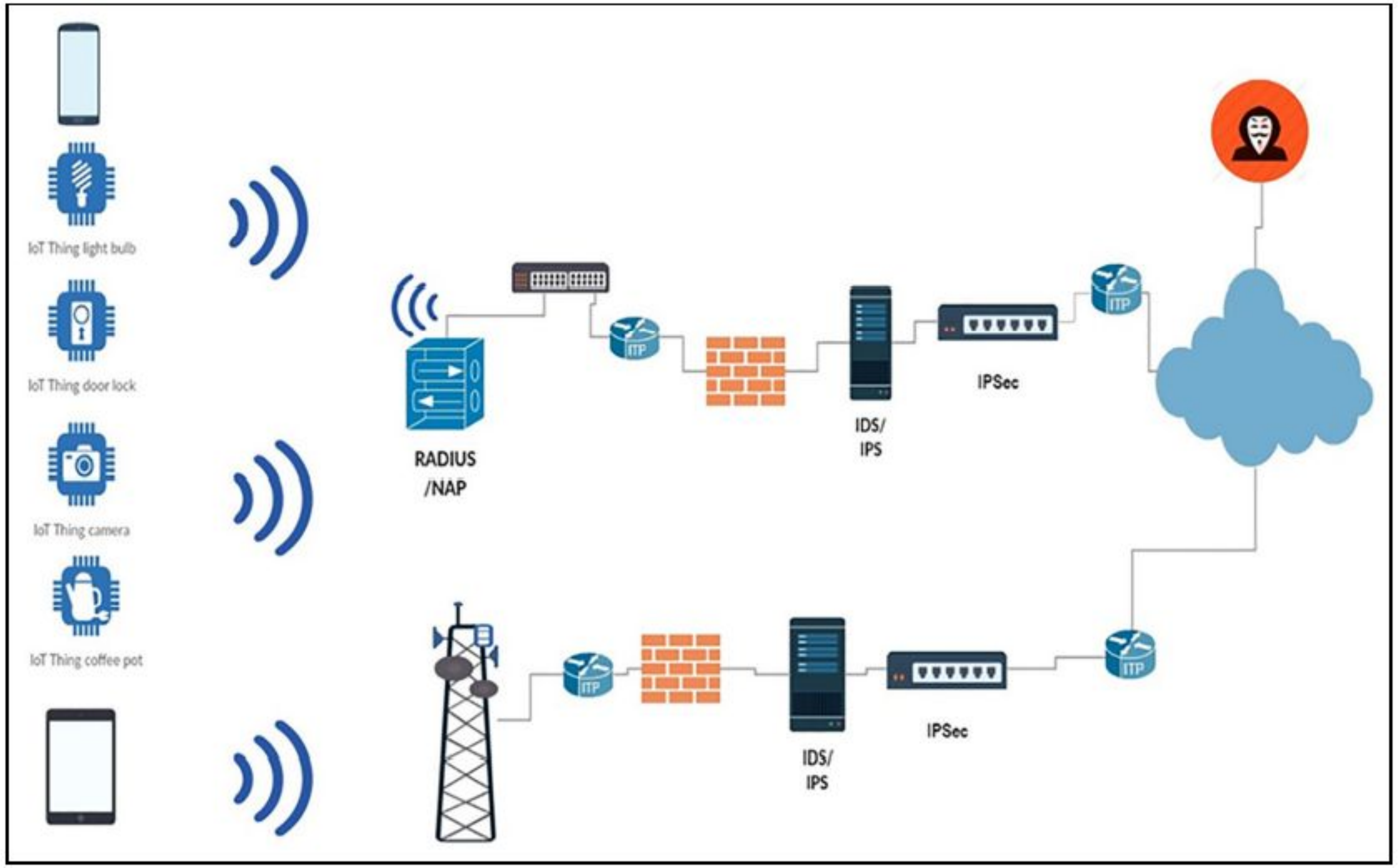
- Monitor (This agent checks network and sends suspected packet to Detector)
- Detector (This agent detects suspected activity and pass on to next)
- Analyzer (This agent analyzers through signature-based or anomaly-based and detects threat-based packets)
- Filter (This agent filters between false-positive & true-positive and generates an alarm)
- Prevention Manager (this protects IoT in case of DoS and sends signal to block intruder)
- Intelligent (This agent learns from the support and updates filter & analyzer rules and policies)
- Audit (This agent registers all events and actions to generate periodic reports)

Setup

- Proposed solution software is installed on IDP hardware that connects IoT devices and router.
- Alternatively, agent can be installed directly on IoT devices which connect directly to cloud. (like edge devices)
- For IoTs connected to cloud, a middleware(Firewall) is setup with Radius/NAP that authenticates IoT connections. (RADIUS/NAP -> Remote Authentication Dial-In Users Server/Service. Network access protection)


Monitor
Detector
Analyzer
Filter
Prevention
Alarm
Audit
Intelligent Agent
Suspected Packet
Check
True Threat
Check Typ
Check Typ
Anomaly Base
True Positive Prevent Threat
Generate Alarm
Record Event
Return
Learn
Signature Based Prevent Threat
Record Event
Return
Fasle Threat


Monitoring
Suspected Activity
Yes
Anomaly Based
Yes
Filter Agent
No
No
Ture positive
Analyzer Agent
Audit
No
Intelligent Agent
Signature based
Update Agent
Yes
Yes
Drop Pkt, block source, and alarm


IoT Thing light bulb
IoT Thing door lock
IoT Thing camera
IoT Thing coffee pot
RADIUS /NAP
ITP
IDS/ IPS
IPSec
ITP
ITP
IDS/ IPS
IPSec
ITP

Challenges, Limitations, Strengths, Weaknesses

(My Analysis)

- Research paper doesn't emphasize on scalability of the proposed solution.
- Strength lies in stages of IDP. Through circular model involving intelligent agent, system always learns and updates rules & policies.
- There could be a performance impact with additional layer of authentication for cloud connection & hardware dependency in case of on-premise model. This was not discussed in research paper.
- Through multiple stages of network scanning, will there be a delay in communication? Especially for time-sensitive projects looking for quick updates.

Future Works, Potential Applications, Possible Improvements

- As this technique looks efficient with wireless communication, and covers the most addressed problems like low memory, computing & processing power, this can be used for cell phones, Wi-Fi, & Bluetooth connections.
- Applicable to drones, remote control devices in large scale industries.

Conclusion

With increasing demand for IoT devices, there is a need to secure devices with IDP (Intrusion detection and Prevention) system to mitigate cyber security attacks. Unlike existing IDP systems that focus on signature-based model, proposed solution is a hybrid model which detects and prevents both signature-based and anomaly-based attacks. Through stages, it follows a loop through approach of self-learn and improve mechanism.

Thank You