A Critical Review of Practices & Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems

Benkhelifa E., Welsh T., Hamouda W.

Presented by Gilbert Owusu-Amonoo Gyamfi

Outline

- Introduction
- Brief Overview of IoT
- Summary of Related Surveys
- IoT Security Threats & Practices
- Intrusion Detection in IoT Systems
- Proposed IoT-IDS Architecture
- Conclusion

Introduction

- IoT is a novel paradigm concerned with building a pervasive environment of smart devices, seeking to enhance everyday life by ubiquitous connectivity.
- This is achieved by interconnectivity of sensors and actuators, to gather and analyze a wealth of data and facilitate the making of smart decisions.
- It is also forseen that the future IoT platform would be through M2M communications, allowing devices to directly communicate with each other to share vital information and to inform optimal decision making.

Introduction

- With IoT basically evolving from using passive unintelligent RFID tagged objects to interactive, cooperative and smart devices, the wealth of data that can be gathered from a number of such devices is immense.
- Coupled with the use of wireless computing networks, the capability of producing wide scale sensor networks can be achieved easily.
- However, with this interconnectivity and the mass collection and analysis of data, security then becomes a critical issue that needs to be addressed.

Overview of IoT

- The term IoT merely describes the idea of global interconnectivity among smart devices, but does not specifically define the way these devices should communicate.
- It can thus be described as an umbrella term encompassing a variety of technologies and standards, both hardware and software and doesn't denote any particular standardization.
- IoT networks typically consists of heterogenous, communicating devices and their networks.

Overview of IoT

- IoT networks are usually driven by and built upon wireless networking specifications.
  - Low power wireless specifications: NFC, WSNs, RFID, Zigbee etc.
  - Wide Area Protocols: GPRS, 3G, 4G, WiMax etc.

- These protocols are not specifically designed for IoT, but their integration and potential use does require consideration in terms of security.

- IoT can also be thought of as a 3-layer model
  - Perception stage: Comprises sensing technologies and short range transmission protocols
  - Transportation stage: Consists of longer range communication
  - Application stage: Consists of platforms such as cloud architectures for data management and actuators

Overview of IoT

TABLE I
A NON-EXHAUSTIVE LIST OF STANDARDS AND PROTOCOLS USED IN IOT

Name	Layer	Description
COAP	Application	Constrained Application Protocol
HTTP	Application	HyperText Transport Protocol
MQTT	Application	MQ Telemetry Transport
XMPP	Application	Extensible Messaging and Presence Protocol
REST	Application	Representational State Transfer
IPV4/6	Network	Internet Protocol 4 / 6
RPL	Network	Routing Protocol for Low power and Lossy Networks
6Lowpan	Network	IPv6 over Low power Wireless Personal Area Networks
802.15.x	Link / Physical	IEEE Wireless Personal Network Standards
802.11	Link / Physical	IEEE Wireless Local Area Network Standards
802.3	Link / Physical	IEEE Local Area Network Standards
2G/3G/4G/5G	Link / Physical	2nd-5th Generation Mobile Telephony Standards
RFID	Link / Physical	Radio-frequency identification
NFC	Link / Physical	Near Field Communication
WiMax	Link / Physical	Broadband Wireless Metropolitan Area Networks
ZigBee	Link / Physical	High-level Wireless Personal Area Network Standard
GPS	Other	Global Positioning System

Overview of IoT

- The lack of standardization however creates security problems especially in the attempt to develop generalized research solutions to determine exactly what needs to be secured.

- Therefore security solutions specifically developed for various IoT technologies need to be considered to pick out the best combination of solutions to make the IoT network security more robust.

Summary of Related Surveys

- Various studies have been done on Intrusion Detection Systems for predominantly wired networks, but tend to focus on a particular type of IDS.
- Due to the wide array of data available, machine learning and data mining techniques are often leveraged for intrusion detection systems.
- Most studies for IDS with respect to wireless networks are done with WSNs due to their resource constrained nature which makes their security quite difficult.
- Some of the shortcomings of IDS for WSNs include poor energy consumption optimization, a lack of universal attack detection, failure to account for Internet-enabled attacks such as DDoS attacks

Summary of Related Surveys

- Some studies have advocated the application of Mobile Ad-hoc Network (MANET) IDS to WSNs, considered IDSs for Cyber Physical Systems, with at least one paper focusing on an Intrusion Detection System for IoT.

- The key points drawn from all the studies are that:
  - Implementation and Detection methods for IDSs depend on the particular technology and tend to cover just one technology type, and detect specific attacks
  - A successful IDS for IoT needs to cover all the service layers
  - Most solutions cannot be properly validated with current IDS systems

IoT Security: Threats & Practices

- Since IoT deals with heavy data collection and processing, it is really necessary to ensure data security (Availability, Integrity and Confidentiality)
- Attacks on data can be considered as passive or active
  - Passive attacks are concerned about data theft or privacy subversion
  - Active attacks are concerned with data subversion or destruction within the network
- Inherent characteristics of IoT cause security issues to be prevalent and varied from conventional security issues
- This is from to the perception layer, and the constrained nature of the devices in the network.
- The constrained nature makes the large amount of resources needed for effective information security difficult to obtain.

IoT Security: Threats & Practices

- Sometimes the data can also been seen as too trivial for concern about its security, but this data can reveal a lot when leaked e.g data obtained from Smart Meters.
- The architectural features in the perception layer ensure the efficient and reliable operation of the networks, but would also make them vulnerable to a variety of attacks due to inherent security issues mentioned in previous slides.
- Most of the attacks on the IoT network may originate from the physical layer so solutions need to be found to ensure security, however the constrained nature makes many of the proposed solutions flawed.

IoT Security: Threats & Practices

TABLE II
NETWORK LAYER INSECURITIES

Networking Layer	Attack Facilitating Features
Physical	External deployment, open wireless medium, embedded design, constrained resources
Link-Layer	Contention based access / collision avoidance
Network	Multi-hop routing, decentralization, broadcast transmissions
Application	Insecure-lower levels, lack of encryption

TABLE III
PERCEPTION LEVEL IOT ATTACK SUSCEPTIBILITY

Attack	Facilitated by IoT Feature	Result of attack	Type	Examples
Device Jamming [33]	Open wireless medium, embedded design,	Denial of service	Active	Random, reactive, constant, Deceptive
Network sniffing [34]	Open wireless medium, insecure routing, decentralization	Data disclosure, Privacy Invasion	Passive	-
Battery exhaustion [35]	Embedded design, open wireless medium	Denial of service	Active	Traffic flooding,
Device Cloning [36]	External deployment, open wireless medium	Denial of service, data disclosure	Active /Passive	-
Side-channel Analysis [37]	External deployment, embedded design	Data disclosure, advanced cryptographic attacks	Passive	-
Routing Attacks [38]	Multi-hop networking, decentralization	Denial of service, data misdirection, data subversion	Active	Selective forwarding, packet alteration, sinkhole
Cryptographic attacks [39]	Open wireless medium, constrained resources	Secured data disclosure,	Active/Passive	Brute force

IoT Security: Threats & Practices

- The physical layer thus needs the strongest focus when it comes to securing the IoT network.
- In the transportation layer, charcteristics of networking protocols used such as broadcast routing, open network medium, decentralized architecture etc create multi-layer insecurities.
- This can be solved using traditional computer security solutions such as firewalls and IDS
- Because of the resource constraint, these protocols are often applied further away from the perception devices to make the network more secure, such as using IPSec for end-to-end authentication and integration encryption in IPv4/6

IoT Security: Threats & Practices

- In the IoT Application layer, since this deals with the service itself with message passing and covers all aspects of the network, the security solutions implemented would have to reflect that fact accordingly.

- Encryption can be easily deployed on the back-end or the end-user devices, but less on the perception devices. IDS are also more easily supported.

- Protection at this layer would need to span all the networking layers, with interoperability amongst the layers cited as a key issue for IoT security

State of the Art Intrusion Detection in IoT & Analysis

- Intrusion Detection Systems are:
  - Widely established networking security components
  - A form of detection, not protection
  - Very useful in wireless networking as preventative security measures are difficult to implement

- IDS can be either host-based or network-based
  - Host-based IDS monitors activity on the system itself(Disk activity, memory usage etc.)
  - Network-based IDS monitors network activity and communications

- IDS monitors behaviour (either host activity or network traffic) for signs of attack, assuming that nominal behavior and malicious behavior are distinct

State of the Art Intrusion Detection in IoT & Analysis

- IDS efficacy is measured with two prominent metrics i.e. False positives and False negatives
  - False positives occur with legitimate traffic being flagged as illegitimate
  - False negatives occur when illegitimate activity is not detected at all

- Due to sparse availability of data sets for IDS, however, there is contention about the efficacy of measuring the performance

- Detection techniques employed in IDS can be classified as:
  - Misuse
  - Anomaly
  - Specification
  - Hybrid

State of the Art Intrusion Detection in IoT & Analysis

- Misuse Detection techniques employ a database of known attacks in which activities such as network traffic or system-level actions are compared to signatures in the database
- If there is a match, then the activity is flagged as suspicious
- Misuse detection is good at detecting known attacks (low false positives)
- However, due to the lack of signature for novel attacks, they are poor at detecting unknown attacks (high false negatives)
- Also storing and updating databases of signatures are impractical for resource constrained devices

State of the Art Intrusion Detection in IoT & Analysis

- Anomaly detection techniques build a model of typical activity to which current activity is compared and any discrepancies are flagged as suspicious
- These detection techniques are good at detecting illegitimate activity that misuse detection techniques fail to pick up.
- But they tend to suffer from high rate of false positives if the model is not periodically updated. Also the varying nature of wireless communications may cause false positives, and is also resource intensive

State of the Art Intrusion Detection in IoT & Analysis

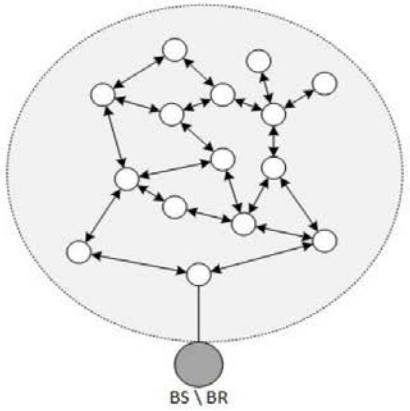
- Specification based techniques combine attributes of anomaly and misuse detection.
- Anomalous activity is also detected by comparison to a pre-defined model, but needs confirmation as malicious from a human participant.
- This technique has the advantage of having increased accuracy, but introduces a delay in the signature creation due to the human interaction which makes it relatively slow.
- Hybrid detection techniques involve any combination of the three types, where issues from one technique are mitigated by the strengths of another.

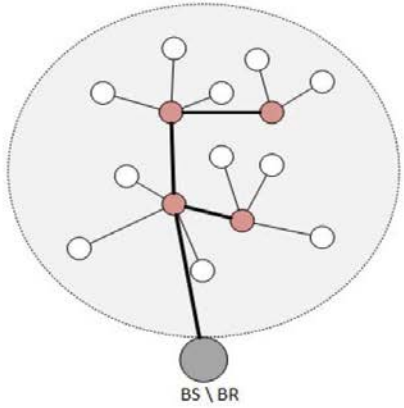
State of the Art Intrusion Detection in IoT & Analysis

- IDS can also be classified according to the architecture into four groups
- Centralised Architectures place the entire IDS in a central location, either remote or host-based
- Distributed Architectures have the IDS placed among multiple or all the nodes within a network with responsibility shared amongst them.
- Hierarchical Architectures may be stand-alone or a combination with another architecture in which some nodes have greater responsibility than others for intrusion detection. Decentralized architectures are considered in this group
- Hybrid architectures involve any combination of the above-mentioned types, and are found in tandem with multiple detection types

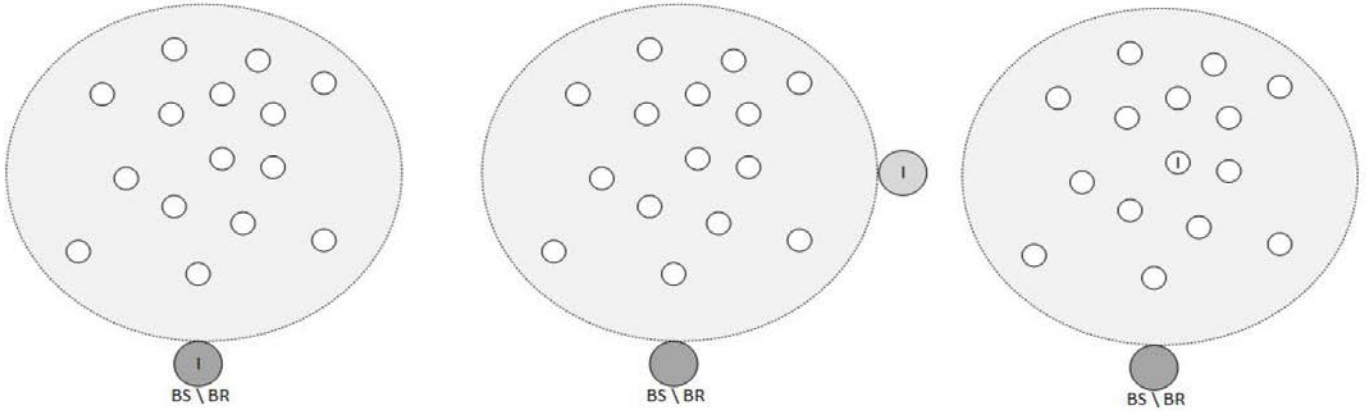
State of the Art Intrusion Detection in IoT & Analysis (Architecture)

Distributed





Hierarchical



Centralized with different node placements

State of the Art Intrusion Detection in IoT & Analysis

TABLE IV
OVERVIEW OF SURVEYED IDS FOR IOT LITERATURE

Reference	Architecture	Tech Focus	Detection Method	Type
[48]	Centralised	Bluetooth	Misuse	NIDS
[35]	Centralised	Mobile devices	Anomaly	HIDS
[45]	Centralised	Mobile devices	Anomaly	HIDS
[51]	Centralised	6LoWPAN	Hybrid	NIDS
[49]	Centralised	Bluetooth	misuse	NIDS
[52]	Centralised	Mobile devices	Anomaly	HIDS
[46]	Centralised	IP Wifi	misuse	NIDS
[47]	Centralised	IP application	anomaly	NDIS
[50]	Centralised with probe	6LoWPAN	misuse	NIDS
[72]	Distributed	WSNs	anomaly	HIDS
[59]	Distributed	WSNs	anomaly	NIDS
[73]	Distributed	WSNs	hybrid	NIDS
[56]	Distributed	Multi-Layer	specification	NDIS
[57]	Distributed	wireless protocols	hybrid	hybrid
[60]	Distributed	WSNs	signature	NDIS
[58]	Distributed	RPL	specification	hybrid
[53]	Distributed watchdog	WSNs	Anomaly	NIDS
[54]	Distributed watchdog	WSNs	Anomaly	HIDS, NIDS
[55]	Distributed watchdog	WSNs	Hybrid	NIDS
[70]	Hierarchichal	WSNs	Anomaly	HIDS, NIDS
[3]	Hierarchichal	802.15.4, 802.11, wired ethernet	Anomaly	HIDS,WIDS,NIDS
[66]	Hierarchichal	RPL	anomaly	NIDS
[65]	Hierarchichal	RPL based 6LoWPAN	anomaly	NDIS
[68]	Hierarchichal	WSN	anomaly	NIDS
[71]	Hierarchichal	WSNs	anomaly	NIDS
[69]	Hierarchichal	WSNs	hybrid	NIDS
[64]	Hierarchichal	6LoWPAN	hybrid	NDIS
[63]	Hierarchichal watchdog	Ipv6 wsn	specification	NIDS
[10]	Hybrid	RPL based 6LoWPAN	Hybrid	NIDS
[74]	Hybrid	RPL	specification	NIDS
[67]	Hybrid	RPL	anomaly	NIDS

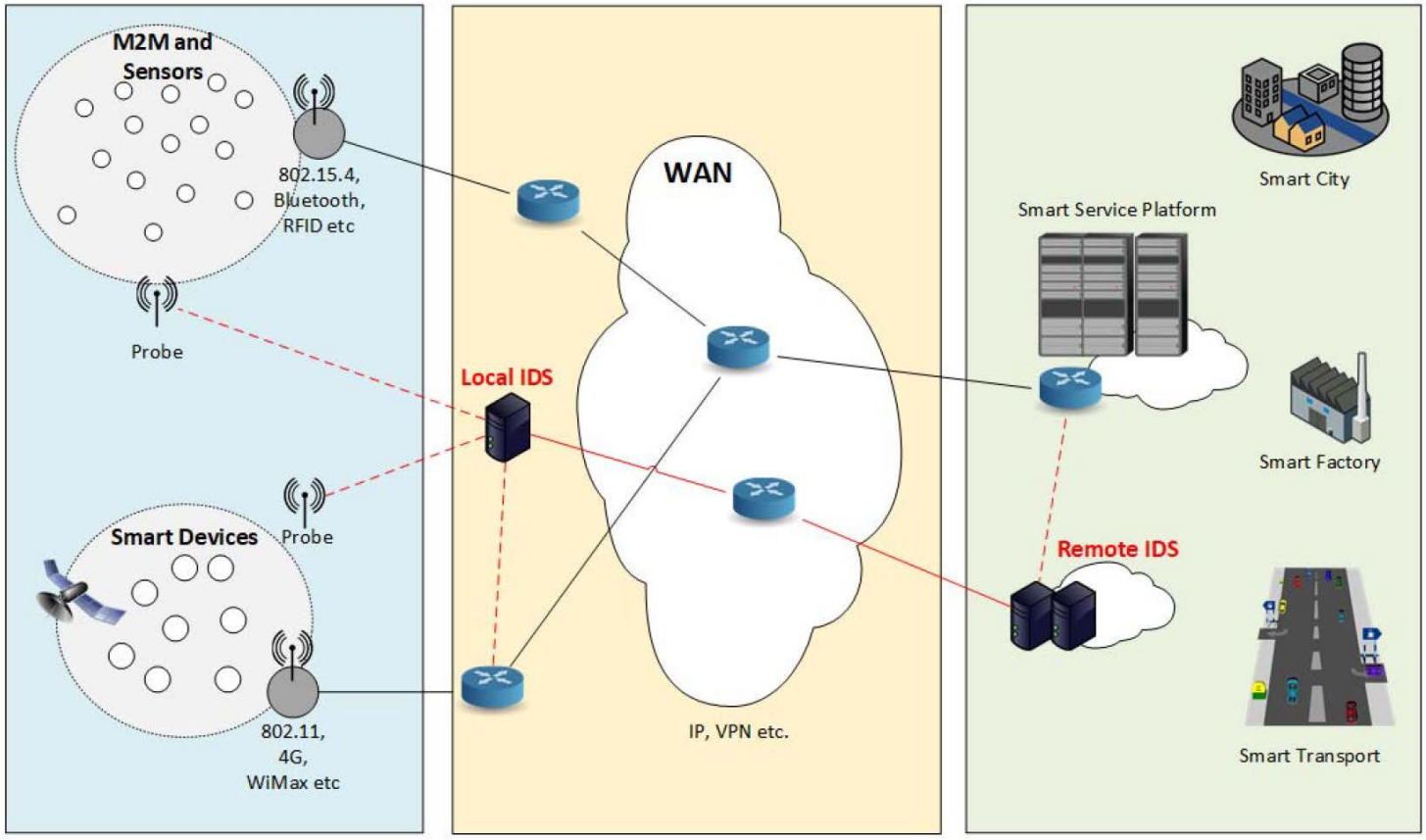
Proposed IoT-IDS Architecture

- From previous slides, we can see that for typical IoT networks:
  - The wide variety of technology types employed in IoT makes any solution implemented for security have a poor coverage in all three IoT layers
  - Due to the variability of wireless communications and the limited amount of resources available for data capture and processing, most detection techniques are not able to cover all attack types with good accuracy
  - The distributed nature of IoT networks makes distributed or hierarchical IDS quite prominent, but are difficult to implement due to resource constraints
  - The constrained nature of IoT devices leaves them liable to subversion at the physical layer, and cannot be trusted security services

Proposed IoT-IDS Architecture

- As such it is proposed that the most effective and secure IDS solution would involve the use of probes to passively monitor the network
- This gives the advantage of being adaptable to various IoT technologies and attack scenarios
- Secure point-to-point or hard wired links can be used to connect probes to an external site, with these being modular in nature
- A cloud based system can provide the back-end system which can be used for a number of modular detection methods and potentially provide unlimited processing power to facilitate any data analysis required.

Proposed IoT-IDS Architecture



IoT Layers

Proposed IoT-IDS Architecture

- The proposed architecture has the following advantages:
  - Ability to process data externally and thus conduct resource intensive detection methods and comprehensive attack detection
  - Ability to detect attacks on the physical layer and above, providing monitoring for the entire network.
  - Facilitating monitoring of various node types through a universal modular monitoring solution
  - Ensure more security by moving the IDS to a different layer than that being monitored.
- However the architecture has some negative aspects for review:
  - Ensuring a secure connection between the sniffer nodes/probes
  - Cost of additional hardware
  - Incurred cost of monitoring multiple RF frequencies
  - Security of an external monitoring platform
  - Lack of full coverage of a site, and obtaining an incomplete picture of the network traffic

Conclusion

- As interest in IoT increases, more data sensitive projects would be involved and as such ensuring its security is a top priority
- Intrusion Detection Systems are a type of defence mechanism employed to achieve that aim.
- Due to the architectural implementation of existing systems, they are not able to defend from all types of attacks
- New approaches need to be taken to secure IoT networks with heterogenous device types, such as cloud processing, usage of probes for data collection and secure transportation
- Correct security solutions need to be found before the wide-scale adoption of insecure processes which widely assist modern society

THANK YOU!!