Multimedia Tools and Applications (2020) 79:3993–4010
https://doi.org/10.1007/s11042-019-7495-6

Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems

S. Venkatraman [1] · B. Surendiran [2]

Received: 31 October 2018 / Revised: 1 March 2019 / Accepted: 18 March 2019 /
Published online: 4 May 2019

Abstract
The rapidly increasing volume of lightweight devices in Internet of Things (IoT) environment needs a strong Intrusion Detection System (IDS). Conventional IDS cannot be applied directly in IoT networks due to various communication architectures, standards, technologies, and environment specific services. The main problem with current IDS and handling techniques is that they can't adapt to service changes in real-time. To overcome this open challenge, adaptive hybrid IDS based on timed automata controller approach is proposed in this paper. Proposed Hybrid IDS have additional knowledge in relation to frequent multimedia file formats and use this knowledge to carry out a comprehensive analysis of packets carrying multimedia files. Crowd sourcing online repository for signature based malicious pattern set generation is designed and self-tuning timed automaton is developed to detect the intruder in IoT networks. From the experimental results, it is evident that our proposed method, an adaptive hybrid IDS suit smart city applications and are accurate (99.06%) in detecting Denial of Service (DoS) attacks, control hijacking attacks, zero day attacks, and replay attacks in IoT environments.

Keywords Attacks · Control hijacking · Internet of things · Intrusion detection · Automata controller

1 Introduction

The Internet of Things (IoT) covers an enormous range of smart heterogeneous multimedia technologies, products, and services. With rapid technology growth and digitalization, IoT made every single thing manageable from the Internet and facilitates multimedia based

✉ S. Venkatraman
venkats23@gmail.com

B. Surendiran
surendiran@nitpy.ac.in

[1] Research Scholar (CSE), National Institute of Technology Puducherry, Karaikal, India

[2] Depatment of CSE, National Institute of Technology Puducherry, Karaikal, India

services and applications that are globally available to the users. Due to increasing volume and variety of IoT constrained devices, traditional security and privacy policies cannot be applied directly. Therefore, security and privacy are a major concern in real-time multimedia application specific IoT networks. Intrusions are defined as set of actions that compromise the security goals such as confidentiality, availability, and integrity of a system [11]. According to cloud security service provider Qualys report [32], it is found that 55,000 Heating, Ventilation and Air Conditioning (HVAC) systems connected to the Internet in two years span to have flaws that may be easily exploited by hackers. The breach at U.S. retailer Target [21] resulted in the theft of at least 40 million customer records containing financial data such as debit and credit card information. The data theft was caused by the installation of malware on the firm's point of sale machines. It is emerging as one of the biggest ever breaches, which originated in malware introduced in point of sale machine and other IoT services. In October 2016, the largest DDoS cyber-attack strength of 1.2 Tbps caused by Mirai botnet brought down the servers of DYN, a company that controls much of the Internet's Domain Name System (DNS) infrastructure. Unlike other botnets, which are typically made up of computers, the Mirai botnet is largely made up of one million IoT devices (digital cameras, DVR players, etc.)[8]. In [13], Banks in India prompt users to change the authentication codes (PIN) of the 3.2 million debit cards to ensure the security of the customers.

Consider smart city, which consist of a set of smart homes equipped with wireless multimedia based surveillance and monitoring system. The multimedia devices can be cameras, harvesting the multimedia information from the smart home environment and reporting to home users and administrators. The connected devices are communicating through Constrained Application Protocol (CoAP). CoAP is a major suitable lightweight protocol for multimedia constraint devices for data communication [7].

Manufacturers are rapidly producing smart devices to meet consumer and market demand, which creates a shortened time-to-market in manufacturing. The level of security in the product development life cycle becomes questionable, as well as production standards [31]. Most of the IoT manufacturers often produce insecure products simply because it is cheaper to do so. Unlike smart phones, which have adequate memory and controlling processors might not be available in many of the IoT devices. Hence, IDS may be deployed in the gateway. IDS in IoT gateway of smart home monitors incoming and outgoing traffic of all the IoT devices that exist on the local network.

Intrusion Detection System (IDS) monitors networks or system logs to identify the intruders. However, IDS fail if the authorised users violate the security policies. Building IDS for IoT networks remains a major challenge due to its heterogeneous nature. Generally, IDS is classified into Signature-based (database of known attack signatures and system vulnerabilities) and Anomaly-based (deviation from normal or expected behaviour of the system) [19].

Importance and the need of IDS in multimedia IoT based surveillance and monitoring system.

i) Application of IoT devices is restricted by the scalability of human interaction. It represents the need to design system for IoT devices to provide security in an automated manner.
ii) Because of huge variety of versions in IoT devices, implementing patches for software vulnerabilities are more difficult to deploy.
iii) There are more possibility to control any IoT device by another IoT devices on network.
iv) Authentication and authorization for user requests might not be possible in most of the IoT devices.
v) Most of the IoT devices are vulnerable as it is developed by start-up companies or manufactured without rigorous testing or using Do It Yourself (DIY) technology.

In our proposal, crowdsourcing system is used to acquire various instance of signature based malicious behaviour from different IoT networks. Crowd sourcing improves the IDS capability by comparing the input stream of packets with malicious instances.

Our paper is organized as follows: Section II analyse the existing intrusion detection systems in IoT networks. Section III deals with the background concepts of Crowd sourcing and Timed automata. Section IV describes the formal construction of proposed timed automata. Experimental results are discussed in section V. Finally, section VI concludes the paper.

2 Related work

Protocols that are used in IoT networks (not employed in existing conventional network architectures) are as follows: IPv6 Routing Protocol for Low power and lossy networks (RPL), IEEE802.15.4, and IPv6 over Low power Wireless Personal Area Networks (6LowPAN)[34]. Thus, these protocols result in unique vulnerabilities and demands for comprehensive IDS. The existing IDS for IoT environment is summarized in Table 1 (Signature based) and Table 2 (Anomaly based) with the following features: IDS detection approach, techniques, handling security issues, deployment environment, data set, detection accuracy, and limitations. The drawback of signature based IDS is, detection of only known intrusion pattern through predefined pattern set and detecting very limited attacks. In [28], a deep packet intrusion detection approach was proposed for resource constrained IoT devices. Further, to strengthen the detection, n-grams pattern matching is preferred for the payloads that are highly similar. The drawback in [28] is high false positive rates for DDoS attacks. To improve the intrusion detection rate, watchdog nodes based IDS was suggested in [20] which monitors the traffic of their neighbors within its radio range. In their communication architecture, there is no association among the watchdog nodes. There is a research gap in the area of collaborative IDS [30]. Distributed and decentralized collaborative IDS allow mounting to large networks, but are still in primary stages of development. These are restricted to very limited attacks and do not provide high accuracy similar to centralized IDS. Intrusion detection rate strongly depends on the knowledge of the IoT network administrator in [3]. Mismatch in malicious pattern selection may cause high false negatives, high false positives, and high risk in IoT networks.

From the Table 1 and Table 2, the existing IDS for IoT are incomprehensive and imperfect to detect intrusion in different environment specific applications of IoT networks. It is evident that current IDS methods are not intended for low power constrained devices and remains a significant challenge. And no event based IDS is designed for the IPv6 (Network protocol) and CoAP (Application protocol) in IoT environment. Because the existing IDS methodologies are either tailored for WSNs or for the traditional Internet. To address these challenges, we propose a timed automata controller approach in network IDS for crowd sourced IoT networks.

3 Background

3.1 Crowd sourced intrusion detection system for IoT

Crowd sourcing is a model in which internet users provide needed services or ideas to achieve security in networks. Introducing crowdsourcing strategy in IDS will enhance the chances to prevent attacks, increase network security, and minimize the damages in IoT environment. And

Table 1 Signature based intrusion detection system

Author	Detection Approach	Techniques	Handling Security Issues	Deployment Environment	Data set	Accuracy	Limitations
C. V. Zhou et al. [35]	Collaborative	Pattern Lattice	DDoS Attacks	IoT Networks	Private Real Traffic	93.1%	Limited to very specific attacks
C. Jun& *C. chi* [15]	Event Modelling	Complex Event Processor Mechanism (CEPM)	Event Streaming with Temporal and Spatial Constraints	IoT Enabled Enterprise Applications	Private Real Traffic	92%	Suffer from single point of failure.
A. Sforzin et.al [25]	Plug & Protect	Raspberry Pi equipped with Snort	Hardware Resource Consumption	IoT Enabled Smart Home	Snort	Not given	Difficult to update rule pattern
Bastille [5]	Post-Event Forensic Analysis	Radio Spectrum	Detection of Radio Frequency Attacks	IoT Enabled Corporates	Private Real Traffic	100% (unauthorized RF usage detection)	Detect limited attacks
P. Kasinathan et.al [16]	Ebbits Framework	Physical World Adaptation Layer	DoS Attacks	6LoWPAN, Real-World IoT Scenarios.	Metasploit	100% (flooding attacks)	Detect Limited attacks

Table 2 Anomaly based intrusion detection system

Author	Detection Approach	Techniques	Handling Security Issues	Deployment Environment	Malicious Pattern Set	Accuracy	Limitations
B. Sun et al. [29]	Markov Chain-Based Approach	Hotelling's T-squared Test	Link change rate	Mobile Ad-Hoc Networks	Private Pattern using GloMoSim	Not given	Detecting anomalies in network level not application Level.
E. Hodo et al.[12]	Evolutionary	Artificial Neural Network	DDoS/DoS attacks.	IoT Enabled Monitoring System	Private Real Traffic	99.4%	It is a type of offline IDS
Pajouh et al. [10]	Two-tier Classification	Naïve Bayes and Certainty Factor version of K-Nearest Neighbor	User to Root and Remote to Local attacks	WSN	NSL-KDD	84.86%	Not designed for IP-based WSNs.
F. Bao et.al [4]	Cluster-Based Hierarchical	Trust-Based Geographic Routing	Good and Bad mouthing attacks.	WSN	Social Networks	90%	Not designed for IP-based WSNs.
A. Alghuried [1]	Clustering	C4.5 decision tree algorithm	temperature and humidity	IoT Enabled Climate Monitoring	Modified version of Intel Lab IoT pattern set	97%	Model will not be able to deal with textual data.
S. Raza et.al [23]	Decentralized	6Mapper	Routing attacks	6LoWPAN Networks	Private Real Traffic	90% in smaller networks	Detect very limited Attacks
S. Misra et.al [18]	Adaptive	Learning Automata (LA)	Malicious Packets	WSN	Private Real Traffic	96%	Difficult to detect passive attack
Y. Fu et.al [9]	Labelled Transition Systems	Finite Automata	Jam- attacks, Replay attacks	IoT Networks	Radius	Not given	Limited attacks
J. Krimmling& Peter [17]	Clustering	Neural Networks	Man in Middle attacks	IoT Smart Public Transport	OMNeT++	Not given	Simulated framework
G. Wang et.al [33]	Machine Learning	Decision Trees and SVM	Crowdturfing	Internet	Sina Weibo Pattern set	98%	Uses simplifying assumptions
M. Shatnawi & M. Hefeeda [26]	Cluster Approach	Operational Multimedia Service	Reduction of Unwarranted Alerts	IoT	Private Real Traffic	89.2%	Designed based on SLA violations.
H. Bosman et al. [6]	Neighborhood Based Approach	Distributed Data Fusion	Spatial & Temporal Correlations	IoT	Private Real Traffic	Not given	Not Suitable for Constrained IoT Devices.

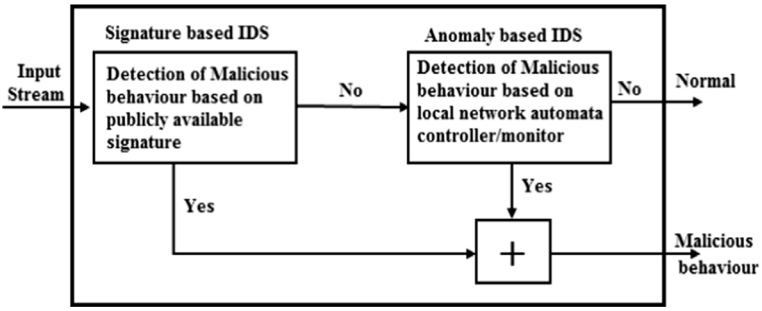

Fig. 1 Proposed Hybrid IDS

also it has positive impact on resilience, self-configuration, and interoperability features of IDS in IoT environment. For example, Crowdroid is an anomaly based IDS for smartphones that uses collected information (various system call operation counts) from a crowd to detect malware [26]. According to FBI report [14], the IoT users and manufacturers are aware of the probable threats and an instance of an attacker may seek to remotely exploit vulnerabilities in the future. Survey [27] confirmed that researchers might gain significant control over IoT device functions remotely by manipulating wireless communications vulnerabilities. Through crowdsourcing it is possible to collect customer experience on various vulnerabilities of application specific IoT networks. And the power of crowd is becoming a significant benchmark for security researchers and IoT device manufacturer. Further, existing network infrastructure afford tiny information to recognize the effect of intrusion through malicious events on IoT services. To address the need of smart society, we proposed crowd sourced framework to build online repository for malicious pattern set of IoT networks as shown in Fig. 1.

3.2 Timed automaton for IoT device

A timed automaton is a mathematical representation of a computing machine with time constraints. Timed finite automaton [2] were adapted as a recognised model to represent the behaviour of real-time control systems.

Mathematical representation of a location invariant timed automaton for IoT devices with 5 tuples is as follows:

- Q is a finite set of possible states in IoT device,
- Q0 ∈ Q is a set of start states,

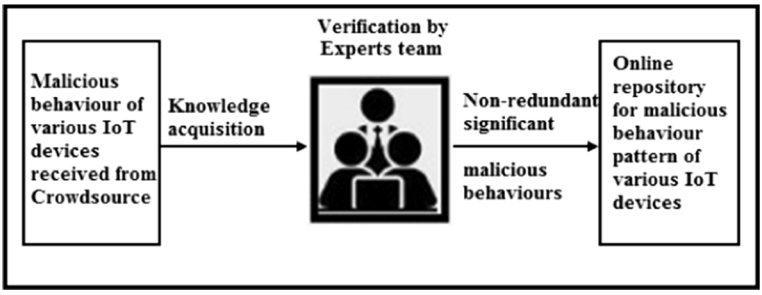

Fig. 2 Proposed framework for online signature based malicious pattern repository construction for IoT environments

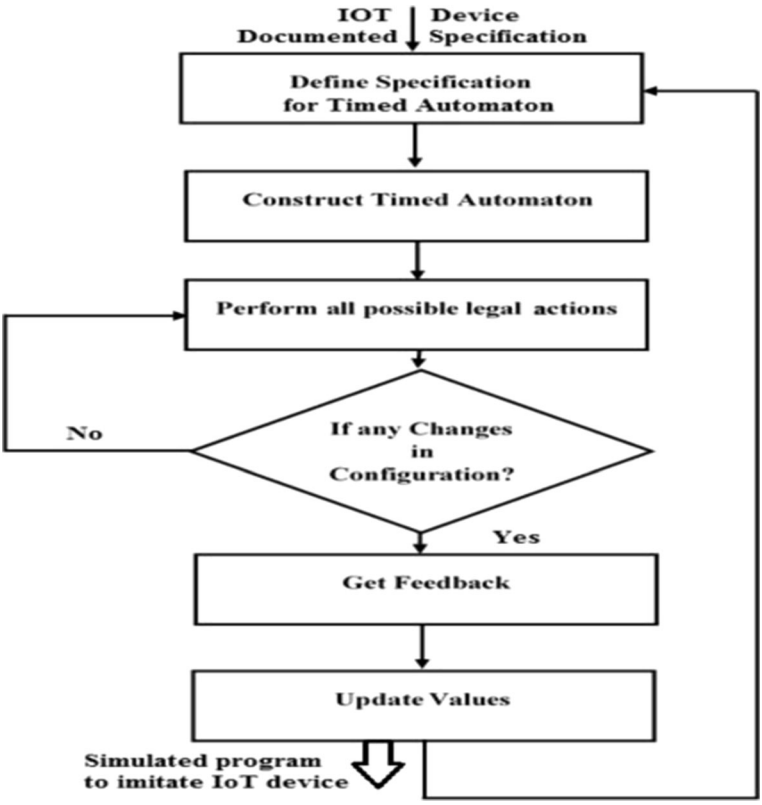

Fig. 3 Construction of self-tuning Timed Automaton

- C is a finite set of real-valued clocks,
- $\sum$ is a finite set of legal control signals acceptable by an IoT device, and
- -∂ (Q, Q, $\sum$, 2^C, Φ(C)) is a set of all possible legal control transition functions of an IoT device over timed constraints. An instantaneous state transition of an IoT device is∂ (q, $q,^1$ a, α, β) which represents a transition from state q to state q^1 on control signal a. The set $\alpha \epsilon C$ provides the clocks to be reset with this transition and β is clock constraints called as guard over C.

4 Proposed controller approach in hybrid intrusion detection system

Our proposed hybrid IDS consist of two modules i) Signature based IDS and ii) Anomaly based IDS. We discuss these modules in following subsections IV.A and IV.B respectively. Fig.2 shows the arrangement of two modules in our proposed hybrid IDS that is deployed in IoT Gateway. From the literature survey, it is found that our proposed Hybrid IDS is the first approach that detects intrusion based on operational behaviour of IoT environment.

4.1 Signature based IDS

In first module, signature dataset for malicious behaviour in IoT network is included along with collection of few standard malicious rule set from Snort [24]. Stateful Packet Inspection (SPI) is

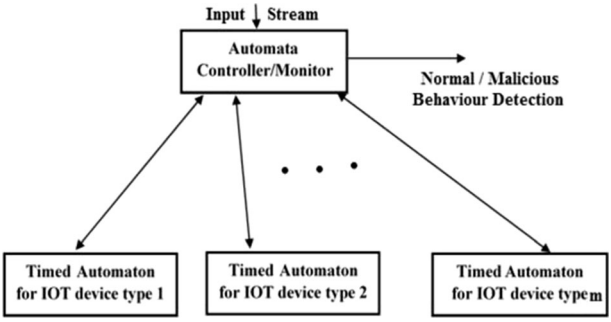

Fig. 4 Malicious behaviour Detection in Smart Home using automata controller

implemented to check the header detail of the captured packet and detects whether it is malicious or legitimate traffic in local network. Updating signature data set for malicious behaviour is proposed in crowd sourced framework as shown in Fig. 2. The steps are as follows:

i) Knowledge acquisition: It collect various malicious behaviour addressed in application and environment specific IoT networks through crowdsourcing.
ii) Human interaction: Expert group collect malicious behaviour instance from different source, identify the non-redundant malicious instance and construct malicious pattern set for various version of IoT devices.
iii) Open repository generation: The constructed malicious pattern set is placed in the open repository for public access.

4.2 Anomaly based IDS

In this subsection, we describe conceptual design of self-tuning timed automata controller approach for Anomaly based IDS to detect internal malicious behaviours on IoT network. Operational behaviour of resource constraint IoT devices is implemented by Timed Automaton (TA). TA act as Event Processing Agent (EPA) and automata controller act as Event Processing Engine (EPE) to detect intrusion in IoT Smart Home environment. The use of timed automaton in our proposal is to maintain the time interval between any legally possible pair of events of IoT device. This feature helps proposed IDS prevent from event flooding attacks which is a type of DoS attacks. Proposed anomaly based IDS works in two modes Initialization / Learning and Testing. The event orchestration or event composition in an IoT environment is a process in which a new service or activity is derived by executing, discovering, and integrating the atomic events produced by IoT devices. It may produce high-energy consumption and high computation overhead, while detecting intrusions and it offers new anomalies and policy violations in smart environments. Our proposed approach with effective orchestration of different intrusion detection patterns, which are functionally equivalent with respect to the safety and security policies to overcome the certain vulnerabilities in IoT environment.

4.2.1 Initialization /learning

In this mode IDS works in offline mode to monitor the behaviour of each and every IOT enabled devices, which exist in the smart home network based on its baseline specification. The activities of

various IoT devices are configured by the administrator of the smart home. Administrator classifies the activities into normal and malicious based on need of the Internal IoT environment. Fig. 3 shows Learning process of an adaptive timed automaton.

4.2.2 Testing

In this mode proposed Anomaly based IDS works in real time based on rule set generated during learning mode. Automata controller is a program to monitor the behaviour of each and every IoT device present in the smart home network. Collaborative operations of automata controller (shown in Fig. 4) system is described in following steps:

i) The payloads are extracted from the input stream of captured packets.
ii) The payload contents are classified based on the type of IoT device recognition.
iii) Classified content is sent to simulated program to imitate an IoT device in the smart home network.
iv) Payload contents are verified in simulated program with the use of timed automaton state transition functions.

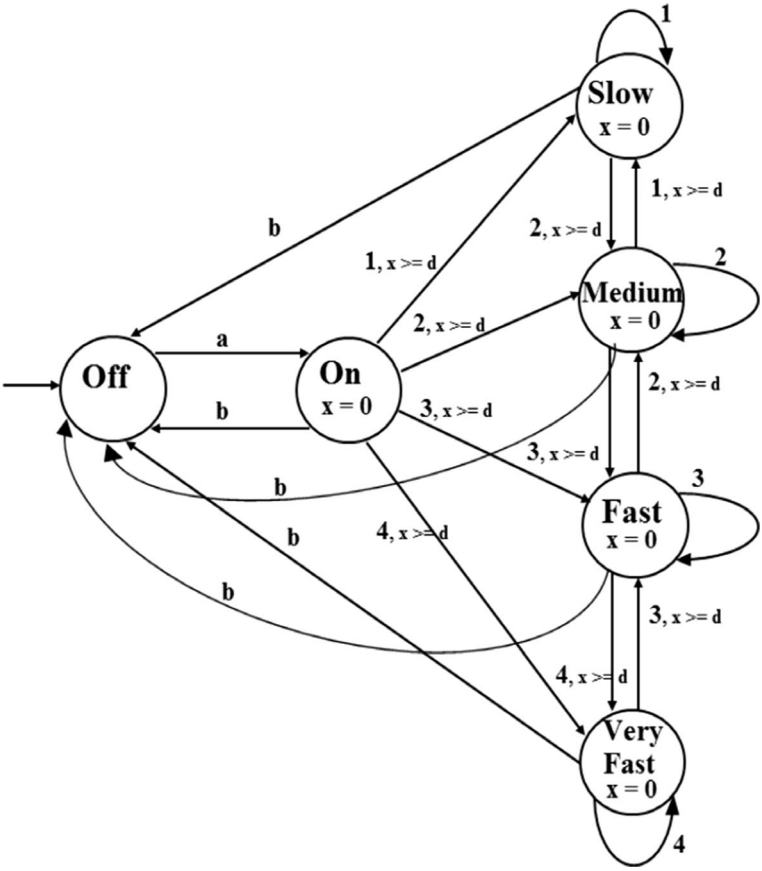

Fig. 5 Timed Automaton for IoT enabled FAN

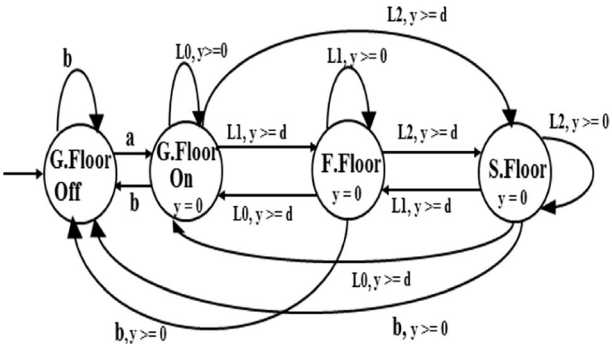

Fig. 6 Timed automaton for IoT enabled Lift machine for G + 2 floors

v) If payload content reach legal state with timed constraints, then the packet is considered as normal traffic. Otherwise malicious traffic.
vi) Based on the feedback of the automata controller, decision is taken to allow or discard the packets.

Input control signals = {1, 2, 3, 4, a, b}, Clock = {x}, Guard = {x >= d} where each control signal represents information. 1, 2, 3, 4 represents slow, medium fast, fast, and very fast respectively. 'a' represents value between 200 V to 240 V. b = 0 V represents switch operations, x represent clock signal, x = 0 represents clock initialization or clock reset and x >= d denotes time constraint or guard. i.e., particular state transition will happen after some 'd' duration. Fig. 5 isstate transition diagram with timed constraints of IoT enabled Fan. Through guard or time constraints, replay, control hijacking and DDoS attacks in IoT devices are detected. Instantaneous definition for an example transition function is ∂(On, Fast, 3, x = 0, x >= d) which means IoT device moves from "On" state to "Fast" state for an input control signal 3 when clock x real value is greater than d and reset the clock x = 0 in state "Fast".

Input control signals = {L0, L1, L2, a, b}, Clock = {y}, Guard = {y >=d, y >=0} where 200v < a < 240v, b = 0v, L0 represents Ground floor, L1 represents first floor, L2 represents second floor are the Lift operations and this machine works with clock y. Initially, lift machine begins from the ground floor in "OFF" state. In that state it receives 'a' control signal and causes the machine to move "ON" state in ground floor without time constraint. Then in "ON" state it is possible to move to first and second floor based on input control signals "L1" and "L2" with time constraint "y >=d" respectively. Transitions are initiated by the input control signals which are received from packets. The state transition diagram shown in Fig. 6 indicates that in "OFF" state, machine can't move to first and second floor without getting control signal "a".

Table 3 Simulation parameters of network traffic for testing

Number of nodes in IoT Network	Legitimate Events	Malicious Events	Total Events	Malicious Events Ratio
10	4000	450	4450	10.11%
20	8000	1000	9000	11.11%
30	15,000	3000	18,000	16.66%

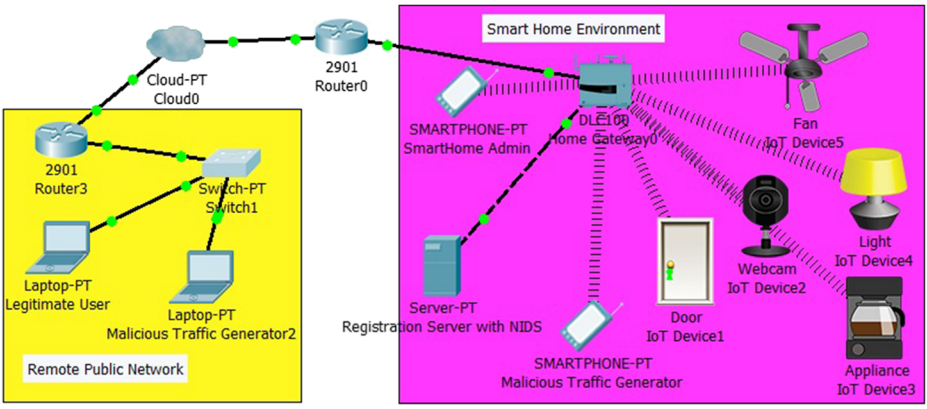

Fig. 7 Experimental design of IoT based Smart Home architecture

Our proposed Hybrid IDS, provide secure Smart home IoT device communication and protect from event control hijacking, DoS (Event flooding) attacks, Event replay attacks and Zero day attacks (vulnerability cause by embedding third party software for internet connectivity in IoT devices). The proposed approach in an IoT environment achieves high speed and high intrusion detection accuracy for malicious patterns such as atomic events and sequential interaction of events. Proposed timed automaton used to understand the complex nature of IoT devices in smart environment by identifying the operational behavior and effects of that behavior.

5 Experimental evaluation

5.1 Experimental design

Communication between IoT devices and IoT gateway is done through IPV6 network protocol and CoAP application protocol. Messages on the smart home are transmitted in small data units called packets. The use of CoAP that runs on most of the IoT devices uses UDP as a transport layer protocol. Each Lightweight packet contains a header and an unencrypted payload. We extract the payload of each packet and feed it to our proposed Hybrid IDS. We implement and evaluate our Hybrid IDS with smart home application in simulated Wi-Fi lab environment. IoT gateways capture the packets that pass through, and the payload is extracted as in CoAP protocol. To test the performance of our Hybrid IDS, IoT network is created with the parameters and test bed as shown in Table 3 and Fig. 7. In our proposal, there is tradeoff between the processing speed

Table 4 Various attacks percentage in malicious pattern (MP) sets

	Event Replay Attacks	Malicious Atomic Events	Malicious Sequential Events	Event Control Hijacking Attacks	DoS (Event Flooding) Attacks
MP Set 1	40%	10%	30%	10%	10%
MP Set 2	20%	50%	10%	10%	10%
MP Set 3	15%	15%	10%	15%	45%
MP Set 4	20%	20%	20%	20%	20%

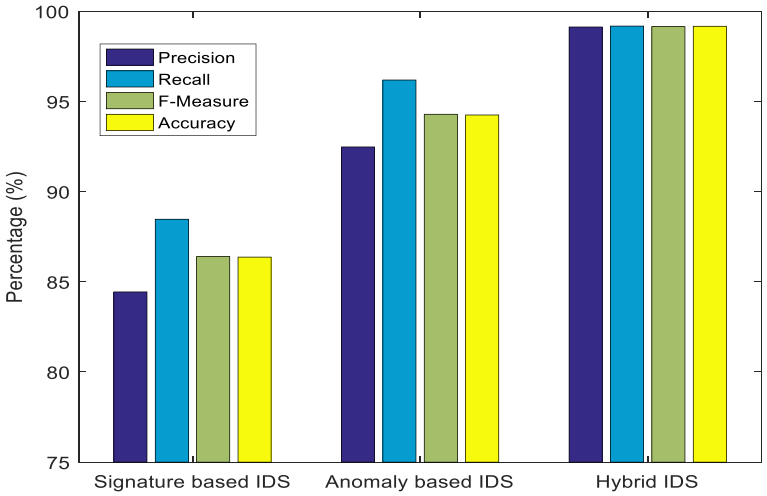

Fig. 8 Precision, Recall, F-Measure and Accuracy of proposed system with N = 10

of IDS and the payload content in CoaP. High speed IDS detection is achieved with fewer amount of IP packet payload.

In order to verify the proposed IDS system, an experimental IoT based architecture has been designed as shown in Fig. 7. As evident from the Fig. 7, a smart home environment has been simulated, which consisting of various client nodes and an IDS programmed registration server (Automata controller). This smart home environment can be accessed by legitimate end users internally or remotely or both at a time via a wireless home gateway. This remote public network is just the simulation of publicly available internet. The client nodes in the smart home environment simulate the operational behaviour of various IoT devices with their own state transitions. Furthermore, two malicious client nodes have been included in both, the smart home environment and the remote public network for generating different types of malicious traffic. If our proposed IDS system detects a malicious behaviour, it stops processing and communicating with that IoT device, and produce alerts and reports to the Smart home administrators. The intention of generating the malicious traffic is to test and evaluate the performance and security of IDS in IoT enabled smart home. Actually, our proposed hybrid IDS is installed in web server, which connect with IoT gateway. Timed automaton representation of IoT devices in hybrid IDS helps to detect actual state of the IoT device and all acceptable input's events of that state in a particular situation. In the evaluation, because of the automata controller, the overheads of this IDS system, in terms of response time and state transition delay are negligible. Proposed approach increases the removal of unwanted packets in IoT environment that automatically decreases energy consumption in constrained IoT terminals.

Table 5 Comparison of different combinations of our proposed algorithms at $N = 10$

Proposed Intrusion Detection Algorithm	Precision (%)	Recall (%)	F-measure (%)	Accuracy (%)
Signature based IDS	84.44	88.47	86.4	86.37
Anomaly based IDS	92.48	96.19	94.29	94.25
Hybrid IDS	99.13	99.18	99.15	99.17

Table 6 Accuracy of proposed algorithms in different malicious pattern sets

Pattern sets	No. of IoT devices in smart network	Signature based IDS	Anomaly based IDS	Hybrid based IDS
Malicious pattern set 1	10	86.37	94.25	99.06
	20	86.2	93.9	99.02
	30	85.8	93.8	99.02
Malicious pattern set 2	10	75.6	89.5	98.6
	20	75.4	87.1	98.7
	30	75.3	87	98.6
Malicious pattern set 3	10	85.4	94.3	98.23
	20	85.3	94.5	98.21
	30	85.6	94.3	98.21
Malicious pattern set 4	10	79.3	93.7	98.18
	20	79.3	93.4	98.29
	30	78.9	93.4	98.24

5.2 Evaluation measures

Our outcomes are assessed by performance metrics such as malicious behaviour precision, malicious behaviour recall, F-Measure and accuracy. According to [22], the malicious precision, malicious recall and accuracy are defined as follows:

$$\text{Precision} = (\text{True Positive (TP)}/(\text{TP} + \text{False Positive (FP)}))^{*} 100 \tag{1}$$

$$\text{Recall} = (\text{TP}/(\text{TP} + \text{False Negative (FN)}))^{*} 100 \tag{2}$$

$$\text{F-Measure} = 2^{*} \frac{\text{Precision}^{*} \text{Recall}}{\text{Precision} + \text{Recall}} \tag{3}$$

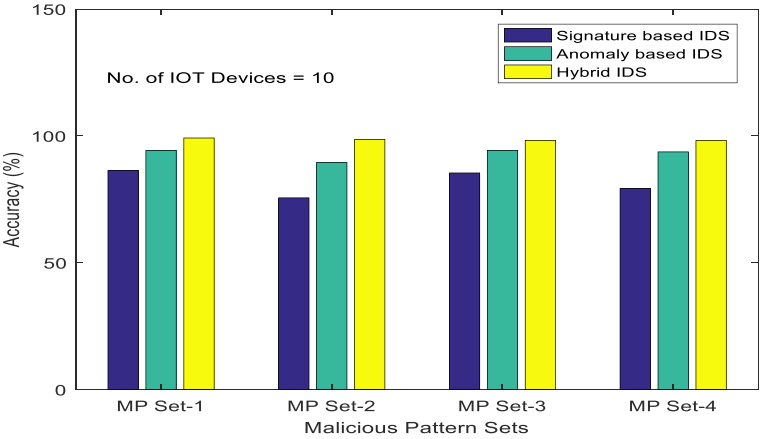

Fig. 9 Malicious Events Detection accuracy of our proposed system with $N = 10$

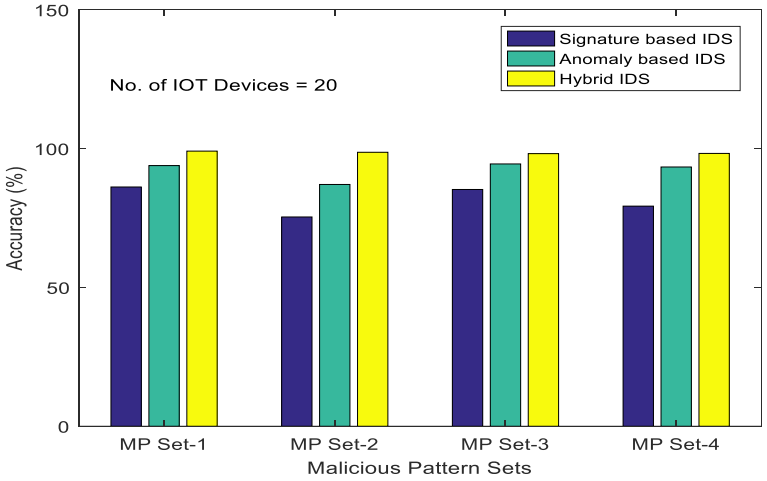

Fig. 10 Malicious Event Detections accuracy of a proposed system with $N = 20$

$$\text{Accuracy} = \frac{\text{TN} + \text{TP}}{(\text{TN} + \text{False Positive}\ (\ \text{FP})) + (\text{TP} + \text{FN})} * 100 \tag{4}$$

Where TP (True Positive), TN (True Negative),FN (False Negative) and FP (False Positive).

5.3 Experiment results and analysis

Table 4 shows percentages of various attack patterns in different malicious pattern sets. Table 5 shows classification performance with different combinations of our proposed algorithm at $N = 10$ (where N is number of IoT devices in the smart home network) and with the malicious pattern set 1. Fig. 8 reflects the Table 5 in bar chart and indicates our Hybrid IDS having high precision and accuracy value in detection of malicious traffic in IoT environment compared to signature and anomaly based IDS.

Table 6 represents the cumulative view of detection accuracy of our proposed system with different test cases. For performance analysis, various test cases were generated based on MP set by varying the ratio of different class of malicious attacks. In Fig. 9, signature based IDS accuracy is changed with respect to the different malicious pattern set in the same network. It indicates that signature based IDS is not stable to detect dynamic malicious behaviour in IoT networks. From Fig. 9 and Fig. 10 it is evident that anomaly based IDS malicious traffic detection accuracy is decreased when increasing the size of IoT network. Fig.9, Fig. 10, and Fig. 11 show our Hybrid IDS is very stable and produces 98% detection accuracy in all test cases. From these experimental analyses, our proposed Hybrid IDS is capable of detect malicious traffic with high accuracy. Due to state-space explosion problem and dynamicity of the IoT environment, our proposed system consumes more time to detect anomaly behavior in complex (interleaved or concurrent) event interactions between different IoT devices.

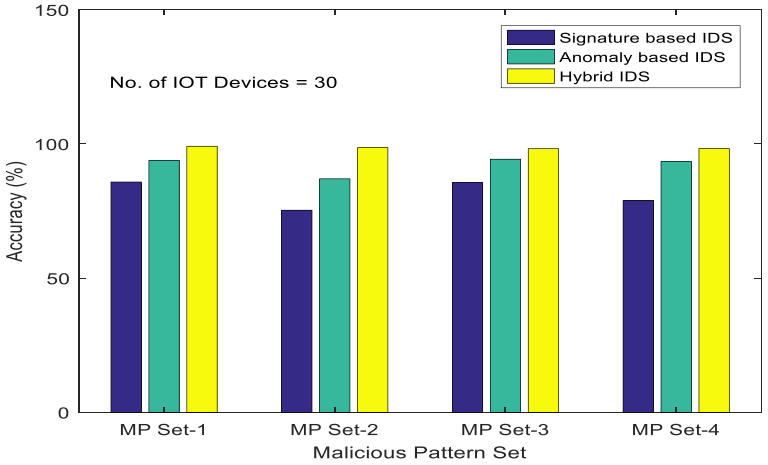

Fig. 11 Malicious Event Detection accuracy of our proposed system with $N = 30$

6 Conclusion

IoT networks are vulnerable to malicious attacks such as DoS, control hijacking, replay attacks, zero day attacks, etc. It may compromise IoT network security and increase damages in existing internet architecture. Adaptive Hybrid IDS based on the timed automaton, and crowd sourced approach is proposed and implemented to secure IoT networks from DoS, control hijacking, replay, and zero day attacks. Further, our crowdsourcing framework helps to detect new attack's scenario in IoT environment and the impact automata controller in Hybrid IDS achieves high detection accuracy of 99.06%. Finally, the performance of our proposed method is verified through experimental analysis. And it has a significant influence to produce sustainability of the cyberspace and to our smart society.

Compliance with ethical standards

Conflict of interest The Authors and Co-Authors have no conflict of interest. The paper is not submitted to any other journals.

References

1. Alghuried A (2017) A model for anomalies detection in internet of things (IoT) using inverse weight clustering and decision tree. Dublin Institute of Technology. https://doi.org/10.21427/d7wk7s
2. Alur R, Dill DL (1994) Fundamental study a theory of timed automata. Theor Comput Sci 126(2):183–235
3. Amaral J, Oliveira L, Rodrigues J, Han G, Shu L (2014) Policy and network based intrusion detection system for IPv6-enabled wireless sensor networks. In: 2014 IEEE International Conference on Communications (ICC), pp 1796–1801
4. Bao F, Chen I-R, Chang M, Cho J-H (2012) Hierarchical Trust Management for Wireless Sensor Networks and its applications to trust-based routing and intrusion detection. IEEE Trans Netw Serv Manag 9(2):169–183

5. Bastille Security for the Internet of Radios. Retrieved Jun 2017 from Bastille Networks: https://www.bastille.net/research/mission/. Accessed 5 June 2017
6. Bosman H, Iacca G, Tejada A, Wörtche HJ, Liotta A (2017) Spatial anomaly detection in sensor networks using neighborhood information. Information Fusion 33:41–56
7. Constrained Application Protocol (CoAP) (2017). https://tools.ietf.org/id/draft-ietf-core-coap-03.html. Accessed 5 June 2017
8. DDoS attack that disrupted internet was largest of its kind in history, experts say, 2016. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botne. Accessed 8 Dec 2016
9. Fu Y, Yan Z, Cao J, Kone O, Cao X (2017) An automata based intrusion detection method for internet of things. Mob Inf Syst 2017(1750637):13. https://doi.org/10.1155/2017/1750637
10. Haddad Pajouh H, Javadian R, Khayami R, Dehghantanha A, Choo R (2016) A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks, IEEE Transactions on Emerging Topics in Computing, (in Press)
11. Heady R, Luger G, Maccabe A, Servilla M (1990) The architecture of network level intrusion detection system. In: Technical report, Department of Computer Science, University of new Mexico
12. Hodo E, Bellekens X, Hamilton A, Dubouilh PL (2016) Threat analysis of IoT networks using artificial neural network intrusion detection system. In: International Symposium on Networks, Computers and Communications (ISNCC) pp 1–6
13. http://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow /54945561.cms. Accessed 26 Dec 2017
14. http://www.securityweek.com/fbi-reminds-cars-are-increasingly-vulnerable-remote-exploits. March 2016
15. Jun C, Chi C (2014) Design of complex event processing IDS in internet of things. In: Sixth International Conference on Measuring Technology and Mechatronics Automation, pp 226–229
16. Kasinathan P, Pastrone C, Spirito MA, Vinkovits M (2013) Denial-of-Service detection in 6LoWPAN based Internet of Things. In: IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp 600–607
17. Krimmling J, Peter S (2014) Integration and evaluation of intrusion detection for CoAP in smart city applications. In: IEEE Conference on Communications and Network Security (CNS'14), pp 73–78
18. Misra S, Abraham KI, Obaidat MS, Krishna PV (2009) LAID: a learning automata-based scheme for intrusion detection in wireless sensor networks. Security Comm Networks 2:105–115. https://doi.org/10.1002/sec.74
19. Mutz D, Valeur F, Vigna G, Kruegel C (2006) Anomalous system call detection. ACM Trans Inf Syst Secur 9(1):61–93
20. Onat I, Miri A (2005) An intrusion detection system for wireless sensor networks. In: Proceeding of the IEEE International Conference on Wireless and Mobile Com- puting, Networking and Communications, Montreal, Canada, August 2005, vol 3, pp 253–259
21. Osborne C 2014 How hackers stole millions of credit card records from target, http://www.zdnet.com/article/how-hackers-stole-millions-of-credit-card-records-from-target/. Accessed 23 Mar 2018
22. Provost F, Fawcett T (2001) Robust classification for imprecise environments, machine learning, vol 42/3, pp 203-231
23. Raza S, Wallgren L, Voigt T (2013) SVELTE: real-time intrusion detection in the internet of things. Ad Hoc Netw 11(8):2661–2674
24. Roesch M (1999) Snort – lightweight intrusion detection for networks. In: Proceedings of the 13th USENIX Conference on System Administration Seattle, Washington, pp 229–238
25. Sforzin A, Marmol FG, Conti M, Bohli JM (2016) RPiDS: Raspberry Pi IDS - A Fruitful Intrusion Detection System for IoT, Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congres, pp 440–448
26. Shatnawi M, Hefeeda M (2018) Dynamic Input Anomaly Detection in Interactive Multimedia Services. In: 9th ACM International Conference on Multimedia System, Amsterdam, Netherlands, June 12–15
27. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A (2015) Security, privacy and trust in internet of things: the road ahead. Comput Netw 76:146–164
28. Summerville DH, Zach KM, Chen Y (2015) Ultra-lightweight deep packet anomaly detection for Internet of Things devices. In: IEEE 34th International Performance Computing and Communications Conference (IPCCC), IEEE, pp 1–8
29. Sun B, Wu K, Xiao Y, Wang R (2007) Integration of mobility and intrusion detection for wireless ad hoc networks. Wiley's International Journal of Communication Systems 20(6):695–721
30. Vasilomanolakis E, Karuppayah S, Fischer M (2015) 55 taxonomy and survey of collaborative intrusion detection. ACM Comput Surv 47(4):1–33

31. Venkatraman S, Arun Raj Kumar P (2018) Improving Adhoc wireless sensor networks security using distributed automaton. Clust Comput. https://doi.org/10.1007/s10586-018-2352-3
32. Vijayan J (2014) Target attack shows danger of remotely accessible HVAC systems. http://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html. Accessed 23 Mar 2018
33. Wang G, Barbara S, Wang T, Barbara S, Zheng H, Zhao BY (2014) Man vs. Machine : Practical Adversarial Detection of Malicious Crowdsourcing Workers. In: Proceedings of the 23rd USENIX Security Symposium, pp 239-254
34. Xiao Y, Shen XS, Du DZ (2007) Wireless Network Security, Springer Science + Business Media, LLC, USA. E-ISBN-10 0-387-33112-3
35. Zhou CV, Leckie C, Karunasekera S (2009) Decentralized multi-dimensional alert correlation for collaborative intrusion detection. J Netw Comput Appl 32(5):1106–1123

Venkatraman S. received B.E. degree in Computer Science and Engineering (CSE) from Bharathidasan University, Tiruchirappalli, India in 2001 and the M.E. degree in software engineering from Anna University, Chennai, India in 2004. His research interests include Cybernetics, Network Security, Internet of Things, and Machine Learning. Currently, he is pursuing his Ph.D. degree in the CSE Dept. at NIT Puducherry, India.

Surendiran B. received B.E. degree in CSE from Sona College of Engineering, Salem, Tamil Nadu, India and the M.E., degree in CSE from VIT University and Ph.D. degrees in Computer Science and Engineering from National Institute of Technology, Tiruchirappalli, India. His research interests include Network Security, Image and Video Processing, Machine Learning, and Data Mining. Currently, he is working as an Assistant Professor in the Dept. of CSE at National Institute of Technology Puducherry, India.