Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-020-02769-3

ORIGINAL RESEARCH

Time dependent anomaly detection system for smart environment using probabilistic timed automaton

S. Venkatraman[1] · P. Muthusamy[2] · Bhanuchander Balusa[1] · T. Jayasankar[3] · G. Kavithaa[4] · K. R. Sekar[5] · C. Bharatiraja[6]

Received: 7 September 2020 / Accepted: 26 November 2020

Abstract
The wide-ranging implementation of the digital Internet of Things (IoT) system in recent years has contributed to the development of smart cities. In real-world time, smart cities are designed to encourage simplicity and quality of life in developed areas. A smart city's network traffic from loT networks is increasingly growing and posing new cybersecurity problems, because these loT devices are linked to sensors that are directly connected to large cloud servers. The researchers need to refine new methods for identifying compromised loT machines to prevent such cyberattacks. In the smart networks, traditional protection strategies are cumbersome to implement because of complexity in communication systems, vendor regulations, requirements, technology and location-specific resources. To address these difficulties, we used a Probabilistic Timed Automaton (PTA) to model the operating actions of smart devices and introduced novel Time Dependent Anomaly Detection Systems (TDADS) utilizing the operational behaviour of smart home environment. Simulations to test our concept are performed in real time. It is clear from the simulation findings that our TDADS achieves effective usage of resources and robust packet transport.

Keywords Anomaly detection · Probabilistic timed automata · Smart environment · Cyber attacks

1 Introduction

The IoT includes heterogeneous systems, products, and services. Low computing power and memory IoT devices are battery-powered and fitted with a radio interface and sensors/actuators. Recent studies in the wireless sector have primarily centred on rising data throughputs. However, environmental-specific applications such as smart home surveillance systems, factory controls, agricultural control systems, automotive networks, and medical systems involve poor data transfer speeds, short-range connectivity, limited IoT devices and affordable hardware. Typical protection and privacy measures cannot however be implemented explicitly in the IoT setting which is limited. But

✉ S. Venkatraman
venkats23@gmail.com

P. Muthusamy
muthu.namakkal@gmail.com

Bhanuchander Balusa
bhanuchander.balusa@vit.ac.in

T. Jayasankar
jayasankar27681@gmail.com

G. Kavithaa
kavi.dhanya@gmail.com

K. R. Sekar
sekar_kr@cse.sastra.edu

C. Bharatiraja
bharatiraja@gmail.com

[1] School of Computer Science and Engineering (SCOPE), Vellore Institute of Technology, Chennai, India

[2] School of Computing Science and Engineering, Galgotias University, NCR, Delhi, India

[3] Department of Electronics and Communication Engineering, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamilnadu, India

[4] Department of ECE, Government College of Engineering, Salem, Tamil Nadu, India

[5] School of Computing, SASTRA Deemed University, Thanjavur, India

[6] Department of Electrical and Electronics Engineering, SRM Institute of Science and Technology, Chennai, India

Published online: 01 January 2021

in application-specific IoT networks, stability and privacy are a big concern. It's being increasingly difficult to secure IoT-based smart home from an attacker. Intruders can not only attempt to capture confidential data from their home devices from a customer but may also attempt to manipulate it in an illegal way. Although device manufacturers release patches to fix software security issues, they are not easy to apply to casual users (Lee et al. 2017). Gartner et al. (2017) Estimates that in 2016 6.4 billion linked items were in usage worldwide and projects that by 2020 it will hit 20.8 billion. Consumers and companies mistakenly confide in useful data from IoT producers. Such details are therefore only protected from established threats and intrusions. Intrusions are described as a collection of actions that undermine safety objectives such as a system's functionality, security and honesty. Today, with the advancement of information technology and the increased availability and growth of hacking tools, there is a need for the protection of critical data in this age of globalisation. This could be supported by firewalls, but they never alert the administrator to any attacks. The solution to the above problem is a mandatory Intrusion Detection Device. It is identical to home or any organisation's burglar alarm device, which senses the existence of any unwelcome interference and warns the administrator of the system. The Anomaly Detection System (ADS) is an efficient and sensitive tool for identifying intruders when authentication of smart home networks becomes violated.

2 Literature review

Nevertheless, a vexing challenge lies at the heart of the tens of billions of linked devices that display and exchange data: cybersecurity. It's no secret that hackers and criminals hacked into baby controls, Internet cameras, bikes, lighting systems and medical equipment. While the number of devices attached to IoT continues to rise in the years ahead, the amount of malware and ransomware used to hack them will also increasing. Like the wireless sensor networks (WSNs), IoT is linked to the worldwide Internet, which, in response to cellular threats within an IoT network, opens it to global interference. Cryptographic and network protection technologies secure them, but they are susceptible to internal and external attacks.

Probably one of the most egregious risks IoT could have is the domestic invasion. Nowadays, in households and workplaces, IoT systems are used in vast numbers that have provided rise to home automation. The security of these IoT devices is of enormous concern as it can expose consumer IP address which can identify consumer residential address. Therefore, the usage of IoT technologies in public protection applications, so there is a risk that they might harm as well as leave the consumer house at a potentially huge hazard.

In October 2018, a 420 Gbps DDoS cyber-attack—the most popular IoT-specific malware—triggered a updated variant of Mirai botnet by the Bushido; unlike other botnets, usually comprised of servers, the Mirai botnet consisted primarily of one million IoT gadgets (video cameras, digital signage networks, consumer electronics, etc.) (Kupreev et al. 2019). IoT and Cyber Physical Systems (CPS) are evolving development platforms that allow keys to change conventional smart environments. Operations on the IoT network are normally tracked, organized, managed and incorporated with cyber infrastructure (Mohanty et al. 2016; Davahli et al. 2020). Intrusion detection in the IoT setting is a big problem for activities such as fault identification, real-time control and tracking systems, owing to the dynamicity of smart technology. Without adequate conceptual knowledge and prioritization of IoT devices' Organizational Intelligence (OI), conventional IDS has fewer effect in protecting intelligent environments. In the smart environment domain, the key research challenge (Venkatraman and Surendiran 2020; Park et al. 2020) is to integrate resources offered by the IoT devices surrounding them, so that the smart systems are not too smart but instead smart enough to be viable for years.

NIDS tracks and identifies Network flow anomalies. In general, NIDS is categorized into signature (a catalogue of documented attack signatures and device vulnerabilities) and anomaly-based (a deviation from standard or planned machine behaviour). Through defining the actions of the process (state transitions) and the consequences of that activity, OI typically offers a way to explain the dynamic existence of IoT systems in smart world. Therefore, by combining signature (packet header information) and anomaly (operational behavior) dependent NIDS techniques to improve intrusion detection accuracy with less false positives, the proposed Hybrid NIDS dependent on timed automaton is obtained.

Therefore, as seen in Table 1, our proposed hybrid NIDS will identify a number of intrusions triggered by frailty in smart environments. Like smartphones, most IoT systems don't have enough processors for memory and power. In addition to conventional network architectures, few newer protocols mentioned in Table 2 are organized and handled by low computing power IoT devices.

In (Verma and Ranga 2020) RPL is susceptible to many attacks that drain the resources of the node and reduce the efficiency of the network due to resource limited existence of nodes in the IoT. LPWAN is not a special approach for a particular collection of specifications but has a variety of functionality involving trade-offs and optimisation (Chaudhari et al. 2020). In (Venkatraman et al. 2019) hybrid network intrusion detection systems approach proposed to detect DDoS, atomic event attack, and radio jamming attacks in smart environments. Such design is useful for detecting documented risks and established assaults.

Table 1 Frailty in IoT centric smart networks

Sl. no.	Frailty	Cases
1	Vulnerable Firmware/Software	Without stable updating process and insecure upgrade service
2	Lack of Privacy and/or Accreditation	Absence of granular access regulation and accumulation of rights
3	Immature Internet API	Intra- and inter—site scripting risk, Limited reliable login recovery methods, SQL infusion, Suffer from poor of lock-out account
4	Minimal physical protection	Simple to disassemble unit, access apps via USB ports, and removable device drive
5	Transport Ignore Cryptographic/Credibility Test	Unencrypted application and accounts routing

Table 2 Protocols for IoT centric smart networks

Sl. no.	Segment	Protocols
1	Infrastructure	RPL, IPv4/IPv6, 6LowPAN
2	Identification	uCode, IPv6, EPC, URIs
3	Communications/Transport	LPWAN, Wifi, Bluetooth
4	Discovery	mDNS, Physical Web, DNS-SD
5	Data Protocols	AMQP, Node, CoAP, MQTT, Websocket
6	Device Management	OMA-DM, TR-069
7	Semantic	Web Thing Model, JSON-LD
8	Multi-layer Frameworks	Weave, Homekit, Alljoyn, IoTivity

3 Back ground

Intelligent home devices such as Smart TV, CCTV Camera, Microwave Ovens, Smart Door, Smart Lock, Washing Machines, Burglary Alarm, Smart Home Assistance, Dishwashing Machines, Smart Stove, and Smart Cooling Systems are Finite State Machine (FSM). Smart home with consumer electronic devices has a large range of sensor-intensive applications that deliver significant, continuously changing data. Detecting irregularities in streaming data in real time has realistic and important implications in many industries. The detector processes the data and make a judgment in real time, instead of making several passes across file batches. In anomaly detection systems of IoT ecosystems factors such as event ordering, real-time uploading, time dependency, and activity interaction are included. Hence, detecting an anomaly is repetitive, and a real-time testing method is needed to model the temporal dependencies of various events (tasks) in IoT Networks. In our proposal, therefore, timed automaton is used to describe how one specific operation will alter its actions over time, responding to events that are caused internally or externally.

A Probabilistic Timed Automaton (PTA) is a logical model of a time restricted computational system. PTA (Sproston et al. 2020) were adapted to represent the behaviour of the real-time control systems as a recognized model. A PTA embraces synchronized control signals-infinite sequences in which every signal is linked to a real-valued incident period. The specific instant arrangement of a IoT device is called states, and transitions are considered legal acts. This paper seeks to identify a reasonable trade-off between the operating model and the identification period for abnormalities. Operational Models focused on synchronized contact of the automaton between reasoning, and timing contribute to better performance.

4 Proposed system

Our proposed framework consists of two modules: (i) proposed device coordination design (ii) proposed TDADS utilizing a synchronized automaton. Those modules are discussed in the following parts. Connected devices interact through CoAP with the IoT gateway inside the smart home setting. CoAP is a lightweight coordination protocol for IoT devices which are low-power constraint (Shelby et al. 2017). From the literature review it is noted that the first solution is our suggested model TDADS, which senses intrusion depending on the IoT environment's organizational actions. environment.

4.1 Communication architecture of proposed system

CoAP is one of the new IETF-developed application layer protocol for IoT devices to link to the smart network (Chen 2014). Since several computers occur as components in

automobiles and buildings with resource limitations, it induces several differences in power processing, connectivity bandwidth, etc. IoT-enabled smart home devices are capable of storing and interacting, such as a sensor that translates measurements, or some other type of real environment knowledge surrounding us. The smart home system is a Low Power and Lossy network (LLN) that utilizes wireless networking protocols including IEEE 802.15.4. With IEEE 802.15.4 the maximum packet size is only 127 bytes. All the IP-based communication protocols presently accessible (HTTP, FTP, SOAP, etc.) would not be ideal for 802.15.4-based networks. Thus, the CoAP lightweight protocol is meant to be used and regarded as a substitute for HTTP as a protocol for IoT device layers. Figure 1 reveals RESTful web service, an architectural design and collaboration method commonly used in the creation of IoT-based web service. Messages are sent to the smart network in tiny data units called IP packets. Any IP packet with CoAP will carry precisely one activity in a home automation IoT setting. Objects are exploited using a defined series of four operations to create, update, read, delete: PUT, GET, POST, and DELETE.

CoAP communicates asynchronously as opposed to HTTP and accepts multicast demands. CoAP works over UDP and needs limited communications overhead. This also facilitates quicker wake-up times and periods of activity, tiny packet sizes and longer sleepy phases. Default IEEE 802.15.4 embraces basic tools that use limited power and usually run in specific event space (home automation) with a 10 m or less star topology. For instance, in home automation, certain peripherals and digital home appliances need 250 kb/s, a lower data rate of 20 kb/s may satisfy the needs of many other perceived applications such as smart tags, sensors, and consumer electronics.

4.2 Proposed time dependent ADS using probabilistic timed automata

The design approach of a PTA based automata controller strategy for ADS in this segment identifies operational malicious activities within the IoT system is illustrated in Fig. 2. PTA incorporates operational actions of resource limited IoT system. Normally IoT systems execute an all-defined, limited series of operations. Those activity sets establish the IoT devices' normal behavior when building their PTA. The PTA functions as an IoT device's event—driven operator, and the automata controller/monitor functions as the context aware engine to define dynamic interactions between basic PTAs incidents. The Proposed Time Dependent ADS senses trends of deviation in serial occurrence activity. In our idea the synchronized automatons hold the time period for each legitimately conceivable pair of IoT system cases. In an IoT environment, event orchestration is a process in which a new service or activity is extracted from the execution, discovery, and integration of atomic events created by IoT devices. When detecting intrusions, it can generate high energy consumption and high overhead computing, and it provides fresh anomalies and policy breaches in smart environments. Our suggested solution is to efficiently orchestrate various patterns of intrusion detection that are functionally similar to safety and protection policies to resolve such IoT vulnerabilities.

4.2.1 Construction of various probabilistic timed automatons for smart environment

In our scenario, we took IoT enabled washing machine consisting of nine states {OFF, ON, LOADTYPE, COTTON, SYNTHETIC, MIXED, SPIN, RINSE, DRY} and five input

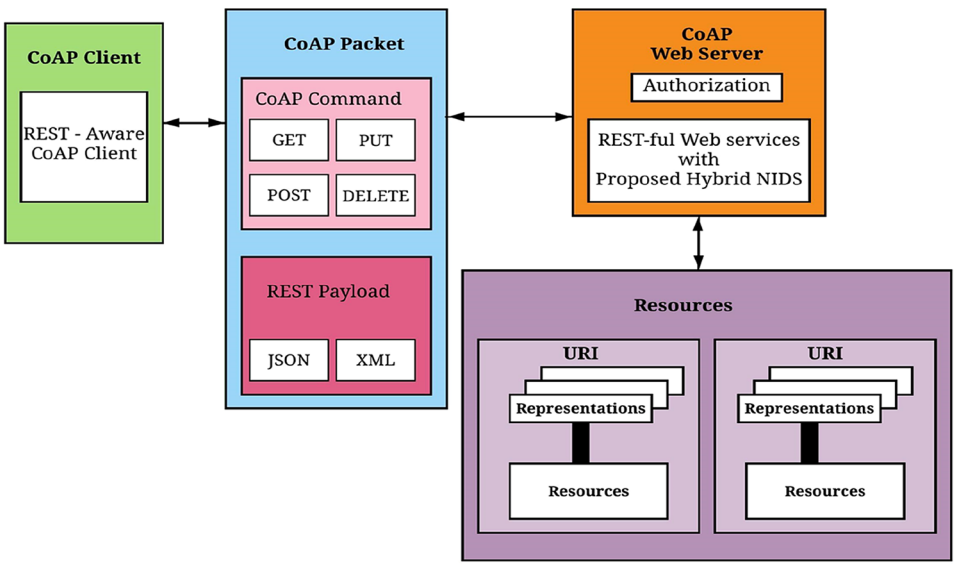

Fig. 1 Communication architecture of proposed system

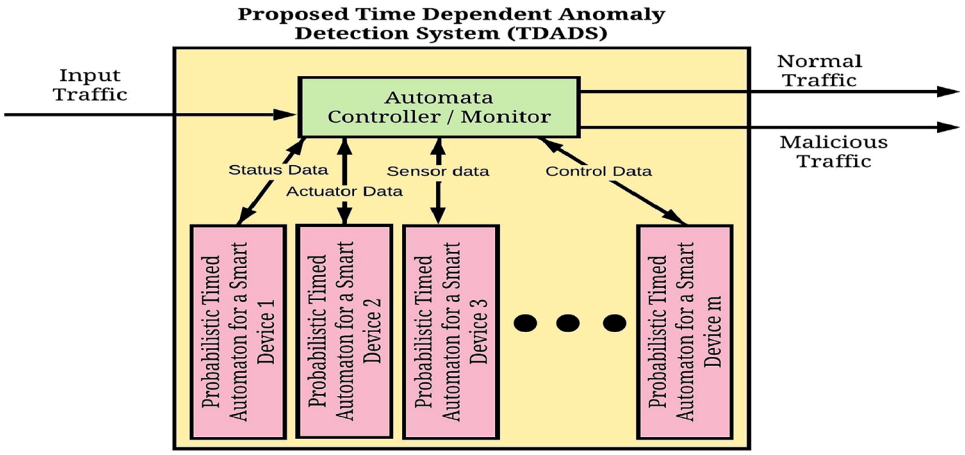

Fig. 2 Proposed TDADS

signals On, Off, C, S, M, W {where On and Off for device turned on and tuned off respectively, C to Cotton-type clothing, S to Synthetic-type clothing, M to Mixed-type clothing and W to Wash}. Used in this representation "ON" and "OFF" to indicate machine state on and off. In "OFF" we only have one "on" user input option and the machine goes to "ON" status, and the probability (P) is 1. If the machine receives any other input signal in the "OFF" state it will result in anomaly. Now in the state machine "ON" has two choices, if the clock value X is greater than 30 s and less than 60 s ($30 <= X <= 60$) with probability $P = 0.9$, the first alternative is to "LOADTYPE". The second choice, if the clock value ($30 <= X <= 60$) with likelihood $P = 0.1$, is to switch to "OFF" mode. In the state of "LOADTYPE," the machine can receive input from the 3 different input signals {C, S, M}. The probabilities of getting cotton, synthetic, and mixed-type clothing are 0.3, 0.2, and 0.5. If the washing machine received this input signal from the user with a time limit of $30 <= X <= 60$, the legal event is otherwise considered to be anomaly. When the machine is in anyone of the following states "COTTON," "SYNTHETIC," and "MIXED" it is capable of receiving "w" input from the user to wash, within the time limit ($30\ s <= X <= 60\ s$) after that machine moves to "SPIN" state with $P = 1$. Depending on the type of load in the "SPIN" state, the machine may remain in the "SPIN" state by time limit ($900\ s <= X <= 1500\ s$). Further machine moves to state "RINSE," in that state machine has two possibilities, it can go to state "DRY" or it can get to state "OFF." The state machine switches from "DRY" to "OFF" when the clock (X) value is greater than 600 s and less than 1200 s, so the likelihood (P) is 1 here since there is no other alternative left in "DRY" mode (Fig. 3).

State transition (Current State, Input, Clock value(X) or Guard, Probability) → Next State.

Example: (COTTON, W, $30\ s <= X <= 60\ s$, 1) → SPIN. {Where COTTON and SPIN are states, W is for Washing event (input signal from user), $30\ s <= X <= 60\ s$ clock value for that transition, and 1 indicates the probability of such transmission}.

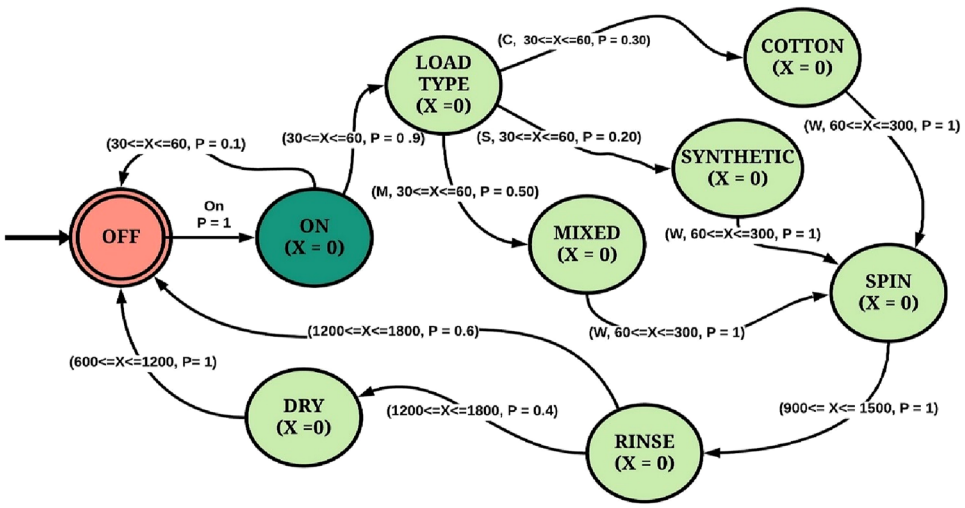

Fig. 3 Probabilistic timed automaton for smart washing machine

If an IoT device is defined using "n" states and "m" input signals, then we can generate $n^{((n+m))}$ different activity sequences. With our washing machine model 9 states and 6 input signals, we can verify 9^{15} possible operation sequences in that only 6 operational sequences are valid, the remaining $(9^{15} - 6)$ sequences are anomaly activity sequences. Smart Door having three States {Closed, OpenfromOutside, OpenfromInside} and four inputs or acceptable control events {ClosedInside, ClosedOutside, OpenInside, OpenOutside}. From this representation, we are able to get $3^7 = 2187$ possible event sequences in Smart Door device alone.

Similarly, Smart Bulb having 4 states {ON, OFF, DIMLIGHT, BRIGHTLIGHT} and 4 acceptable control events {On, Off, Dim, Bright} it leads to $4^8 = 65{,}536$ possible event sequences. When both smart devices rely on their legal control activities, then it yields 2187 * 65,536 = 143,327,232 potential legal sequences. We proposed semantic rule sets in automated controller to represent state dependence information between different IoT devices to overcome state exhaustive issue. To fix scalability problems, rule sets are constructed dynamically using a few major dependence situations in a regulation articulated between distinct IoT appliances in the smart home network. By applying forward reasoning in rule sets, automata controller automatically predicts and track the legal instances (states) of an IoT device.

4.3 Simulation assessment

A prototype of an IoT-based smart home configuration is being modelled by using NetSim emulator to validate the proposed TDADS. In Fig. 4 a connected home comprising of multiple (internal and external) IoT network nodes (CoAP device), portal and authentication system (CoAP server) with the suggested TDADS. Our proposed system consists of two units where the first unit scrutinizes payloads regarding the PTAs and categorizes the packet as valid and malevolent. The second unit utilizes the automata controller to recognize the status information of reliant IoT devices, which consists of semantic rule sets. Semantic rule sets are used to verify any specific case to validate an IoT device's operating activity with other IoT devices. The automata controller is used to accept packets, and packets are only collected while CoAP is the application protocol.

The whole intelligent home surroundings is made accessible internally or remotely via a wireless IoT gateway by legitimate end-users. Few authorized clients and two malevolent client end devices were being used for generating regular and malevolent traffic in the virtual smart environment shown in Table 3. Those kinds of malevolent clients transmit information which interrupt the operation of the network. Furthermore, certain legal programs create harmful behaviors like replaying, adding, and altering. Accuracy is determined depending upon the cumulative amount of correctly defined valid and fraudulent packets.

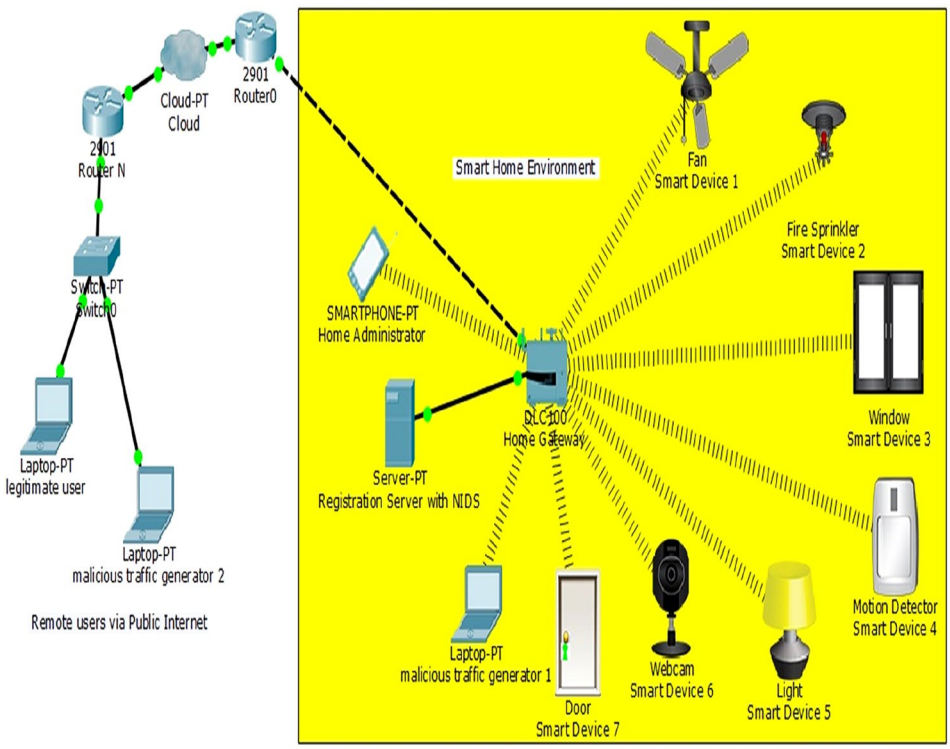

Fig. 4 Modelled connected home surroundings dependent on IoT

Table 3 Test case attributes

Sample size of IoT-Network nodes	Legal incidents	Anomaly incidents	Overall incidents	Anomaly incidents ratio (%)
15	4500	700	5200	13.46
25	11,500	2300	13,800	16.67
35	18,000	4150	22,150	18.73

$$\text{Accuracy} = (\text{TN} + \text{TP} \,/\, (\text{TN} + \text{FP} + \text{TP} + \text{FN})) * 100$$

In which True Positive (TP) and True Negative (TN) are just the number of packets accurately marked, respectively, as valid traffic and deceptive traffic. False Positive (FP) and False Negative (FN) represent the numbers of packets that misidentify deceptive packets as legitimate traffic and valid traffic that were mislabelled as fraudulent traffic, respectively. Tables 4, 5, respectively, provide a description of the collection of abnormalities and how such abnormalities are observed, and a distinction between current anomaly detection systems and our proposed TDADS. Through contrasting the current IoT anomaly detector approaches in a literature review, our model findings indicate that the new TDADS will identify a broader spectrum of abnormalities through checking the IoT devices' working behavior.

5 Detection of DDoS attack through our proposed TDADS

Figure 5 shows how numerous packets reach smart home gateways from various sources and go to the automata controller via Web Server. Further, our suggested TDADS is activated by submitting valid packets to the smart home system based on the current state of the IoT device detected by PTA's next qualifying occurrence, and all harmful packets are discarded.Our proposed TDADS is currently built on a web server that connects to the IoT gateway. In a specific case, the PTA representation of IoT devices in TDADS helps in detecting the present situation of the IoT system and all appropriate input incidents in that state. The overhead of this TDADS system is negligible in terms of response time and state change delay in the evaluation due to the automatic controller.

6 Conclusion

Modern vulnerabilities of security in Smart networks have rendered IoT network security one of the most important problems. Several protection measures have been suggested in the literature to protect against intrusion attacks. They can compete with some threats but can't cover other vital security attacks like the masquerade attack. We have proposed a new ADS called TDADS to remedy this problem, which extracts clock skews from intervals of messages, probabilities between events and models their operational behaviours using PTA. The suggested PTA-based TDADS is deployed to defend IoT networks from Playback, DDoS, Zero-day, Mischievous series assaults, Hijacking, and Spoofing-Jamming assaults. Since our proposed TDADS operates in a smart home setting on an IoT gateway, it overwhelms resource limitation issues and has ample capacity to identify new, irregular and complicated scenarios for attack.

Table 4 Anomaly detection scenario for various attacks

Sl. No.	Attack name	Detection scenarios
1	Playback and DDoS attacks	Keeps dropping the packet by analysing the current status time restriction in the associated PTA
2	Zero-day attacks and Mischievous attack sequence	Notifies if legal position is not met in the respective PTA
3	Hijacking attack	Restricts the number of modifications in the state during a specified period
4	Mischievous atomic attack	Compares the valid PTA events to the input event in their current state
5	Spoofing-Jamming attack	Checks on an IoT device's power consumption periodically

Table 5 Comparison between existing ADS with proposed TDADS in IoT network

NIDS	Techniques	Approach	Deployment environment	Type	Data set	Accuracy claimed	Detecting attacks
Venkatraman et al. (2019)	Timed Automata	Operational Behavior	Smart City	Hybrid	Simulated Traffic	99.17	DDoS, radio jamming attacks
Habibi et al. (2017)	Heimdall Defense Technique	Profile Learning and Enforcement	IoT	Hybrid Based	Private Real Traffic	Not mentioned	DDoS attacks
Wang et al. (2015)	Markov Chain Monte Carlo Learning	Dynamics Network and Service Structures	Smart City	Anomaly based	Private Real Traffic	Not mentioned	Routing attacks
Misra et al. (2009)	Learning Automata (LA)	Sampling Path and Budgets	WSN	Anomaly based	Private Real Traffic	96%	Malicious atomic events
Fu et al. (2017)	Finite Automata	Event Database	IoT Networks	Hybrid Based	Radius Simulated Traffic	Not mentioned	Jamming, Replay attacks
Sedjelmaci et al. (2017)	Back Propagation Network	Nash Equilibrium	WSN	Hybrid based	TOSSIM (Simulated Traffic)	93%	Attacks caused by energy consumption
Mrugala (et al. 2017)	Genetic Algorithm	Gilbert–Elliott Model	WSN	Anomaly based	Simulator Traffic	95%	Cache poisoning attacks
Proposed TDADS	Timed Automata Controller	Operational Behavior	Smart Home	Hybrid Based	Private Real and Simulated Traffic	Above 90% in more cases	Atomic event attacks, Malicious sequential event attacks, DoS attacks, Replay attacks, Jamming Attacks, Zero Day attacks

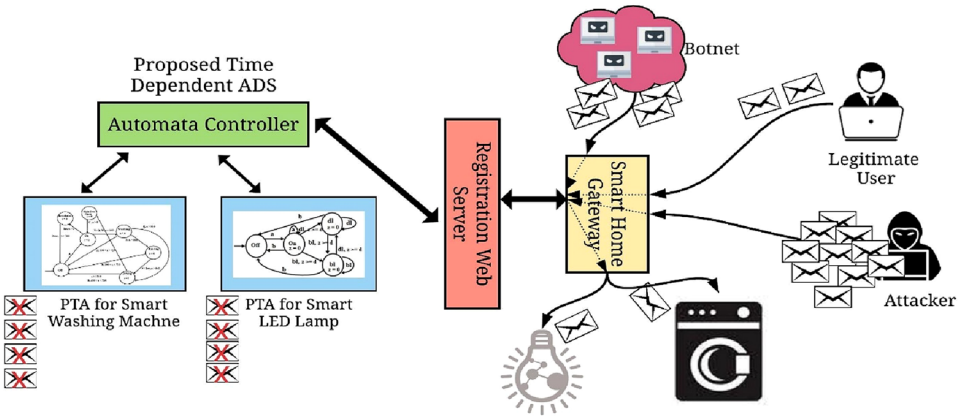

Fig. 5 DDoS attack detection scenario in smart home environment

References

Chaudhari BS, Zennaro M, Borkar S (2020) LPWAN Technologies: Emerging Application Characteristics, Requirements, and Design considerations. Future Internet 12(3):46–71

Chen X (2014) Constrained Application Protocol for Internet of Things, April 2014, [online]. http:/www.cse.wustl.edu/jain/cse574 14/ftp/coap/index.html.

Davahli A, Shamsi M, Abaei G (2020) Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-020-01919-x

Fu Y, Yan Z, Cao J, Cao X (2017) An automata based intrusion detection method for internet of things. Mobile Inf Syst, vol 2017, Article ID 1750637, pp 1–13

Gartner (2017) Forecast alert: internet of things—endpoints and associated services, worldwide, 2016. In: The Gartner Catalyst Conference, San Diego

Habibi J, Midi D, Mudgerikar A, Bertino E (2017) Heimdall: mitigating the internet of insecure things. IEEE Internet Things J 4(4):968–978

Kupreev O, Badovskaya E, Gutnikov A (2019) DDoS attacks in Q4 2018, DDoS reports. Accessed July Online. https://securelist.com/ddos-attacks-in-q4-2018/89565/

Lee J, Kim H (2017) Security and privacy challenges in the internet of things [security and privacy matters]. IEEE Consum Electron Mag 6(3):134–136. https://doi.org/10.1109/MCE.2017.2685019

Misra S, Abraham KI, Obaidat MS, Krishna PV (2009) LAID: a learning automata-based scheme for intrusion detection in wireless sensor networks. Secury Commun Netw 2:105–115. https://doi.org/10.1002/sec.74

Mohanty SP, Choppali U, Kougianos E (2016) Everything you wanted to know about smart cities: the internet of things is the backbone. IEEE Consum Electron Mag 5(3):60–70. https://doi.org/10.1109/MCE.2016.2556879

Mrugala K, Tuptuk N, Hailes S (2017) Evolving attackers against wireless sensor networks using genetic programming. IET Wirel Sens Syst 7(4):113–122

Park S, LiG HJ (2020) A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning. J Ambient Intell Human Comput 11:1405–1412. https://doi.org/10.1007/s12652-018-0998-6

Sedjelmaci H, SenouciS M, Taleb T (2017) An accurate security game for low-resource IoT devices. IEEE Trans Veh Technol 66(10):9381–9393. https://doi.org/10.1109/TVT.2017.2701551

Shelby Z, Frank B, Sturek D (2017) Constrained Application Protocol (CoAP)

Sproston J (2020) Probabilistic timed automata with one clock and initialised clock-dependent probabilities. In: Gotsman A, Sokolova A (eds) Formal techniques for distributed objects, components, and systems. FORTE 2020. Lecture notes in computer science, vol 12136. Springer, Cham. https://doi.org/10.1007/978-3-030-50086-3_9

Venkatraman S, Surendiran B (2020) Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems. Multimed Tools Appl. https://doi.org/10.1007/s11042-019-7495-6

Venkatraman S, Surendiran B, ArunRajKumar P (2019) Hybrid network intrusion detection system for smart environments based on internet of things. Comput J OUP 62(12):1822–1839

Verma A, Ranga V (2020) Security of RPL based 6LoWPAN networks in the internet of things: a review. IEEE Sens J 20(11):5666–5690. https://doi.org/10.1109/JSEN.2020.2973677

Wang J, Kuang Q, Duan S (2015) A new online anomaly learning and detection for large-scale service of internet of thing. Pers Ubiquit Comput 19:1021–1031