International Journal of Aquatic Science
ISSN: 2008-8019
Vol 12, Issue 02, 2021

Secured Wireless Connectivity With Machine Learning Optimized Flawless Iot

[1]Dr.A.M.Saravanan , [2]Dr.Monika Bhatnagar, [3]Ajay Kumar Chauhan, [4]Dr.G.Naga Rama Devi, [5] Dr.Kalaivani Ramanathan, [6]Purnendu Shekhar Pandey

[1]Assistant Professor , PG & Research Dept of Computer Science, Muthurangam Govt. Arts College (Autonomous), Otteri Road , Vellore - 632002. Vellore Dist. , Tamil Nadu , India.
[2]Associate Professor,Electronics and Communication Engineering, Galgotias College of Engineering & Technology,1,Knowledge Park Phase-II,Greater Noida-201310.
[3]Assistant Professor,Electronics and Communication Engineering,Indrapratha Engineering College, Ghaziabad-201010
[4]Professor, Computer Science and Engineering, CMR Institute of Technology, kandlakoya, Medchal,Hyderabad, 501401.
[5]Professor, Department of Electronics and Communication Engineering, Erode Sengunthar Engineering College, Perundurai, Erode, Tamilnadu, India – 638057.
[6]Associate Professor ,Department of Computer Science & Engineering,Koneru Lakshmaiah Education Foundation (KLEF),Greenfields, Vaddeswaram,Guntur-522502

Abstract: The advancement of the Internet of Things (IoT) model led to advancements in hardware and software, in connectivity, and convergence of digital technology, along with declining cost and efficiency. Several billion computers connecting to the Internet are part of IoT ecosystem. Besides, IoT devices are an integral part of ICT infrastructure which supports many day-to-day activities. In recent years, considerable attention has been paid to the protection of these IoT applications. The volume of data generated daily has sparked interest in technology like machine learning and artificial intelligence, another big recent development. In improving the safety of IoT systems, we explore the promise of machine learning techniques. The key emphasis is the use of supervised, unattended learning strategies and improving learning in the IoT context, both for host and network security solutions. Finally, we speak about some of the complexities of learning machinery that must be overcome to introduce and operate them successfully so that IoT devices can be properly secured.

Index: Internet of things, Machine learning, Security, Attack.

1. INTRODUCTION

In last twenty years, the real world and digital world have converged exponentially. Internet was at the first critical part of linking all worlds. As interconnected computers become smaller, versatile and cheaper, installed cost-effectively in many applications and systems and allow these applications available on the Internet from every platform, from anywhere and anywhere. These innovations have paved way for Internet of Things (IoT) to emerge. Several recent studies have shown that number of connected devices in the house has grown, and many IoT applications and technologies have now been introduced to different sectors including healthcare, shipping, smart home, manufacturing, etc. One report estimated, for

example, that by 2021 number of connected devices will be more than 30 per Australian household. Houses in broadband in the United States have 10 wired devices, like PC / Mac, mobile, tablet and in-home platforms including game consoles, Smart TV, video player streaming, Blu-ray player, DVR, and etc.

The ability of computer training technology to enhance IoT protection has recently been discussed with rising enthusiasm. This interest stems from an increase in intelligent adversaries generated by emergence in machine learning software and increasing big data, and from an inability to adjust signature defenses fast enough to zero-day threats. For e.g. some monitored models need high CPUs and memory during preparation but need less than unmonitored learning models once implemented. To enhance networking protection, machine learning techniques (e.g. laptops, routers etc.) are used on conventional networking hardware and are hence best suited to defending the IoT infrastructure.

2. RELATED WORK

Most IoT devices protection approaches rely on defensive interventions (such as encryption) on these devices (or use conventional network security control methods, such as intrusion prevention based on signatures). There has been little progress in discovering feasible network based machine learning defenses for IoT and host-based machine learning defense strategies for these applications. Moreover, we must take into account all the drawbacks associated with different types of machine learning when using machine learning-based security approaches for IoT applications [3]. Algorithms (supervised, unregulated and enhanced) and basic characteristics of certain IoT devices (for example, restricted processing and storage resources). We summarize as follows the key review papers:

- We shall shortly discuss the features and popular attacks on IoT computers.
- We provide taxonomy for networked and host-based machine learning methods that can enhance IoT security in practice (along with their strengths and weaknesses).
- We will address some key future issues to allow IoT protection for machine-learning methods to be better and more effective.

3. CONTEXT AND MACHINE LEARNING

Internet of Things: The Internet of Things makes the user easy to use Internet-connected gadgets and smooth networking that sustain our everyday cyber operation. The possible attack surface grows as more applications link to the IoT ecosystem. In consequence, the possibilities to intensify attacks are far higher provided the vast number of IoT devices linked in IoT settings. Cyberspace controlling IoT computers remains a big concern. For starters, millions of essential ports (e.g., ports 143 for Internet Message Control Protocol [8] or 445 for Microsoft Directory Services) been discovered by using instruments such as Shodan, an IoT computer search engine. Many of the gadgets use login credentials by default. In reality, vulnerable protocols like Telnet sometimes are used again due to the increasing proliferation of IoT. Also, many of Internet-enabled devices use wireless connectivity technology [7] that, unless properly safeguarded, make devices usable outside of conventional wired network region.

The recent data exhilaration by a casino-connected Aquarium Thermostat system is one example of this assault. The attackers used the system and moved multiple gigabytes of the data from the casino's high-roller database containing sensitive information from the network about their wealthiest high-roller visitors. The effect of infected IoT devices on the persons or organizations running these devices on their networks is not isolated. Compromised IoT computers can be used for botnet attacks [9] [10] on other platforms and networks on a wide scale, denial-of-service (DoS). A new study quantified the damage to organizations and society as a whole of such attacks. IoT hacks cost 13% of their annual sales to tiny US businesses [11].

In contrast with conventional information security, solid, cost-effective IoT security is more difficult to meet for several reasons including (a) the world in which these IoT devices work. Today, many IoT products have wireless networks that can be accessed beyond the organization's internal network border; (b) configuration fixes and vulnerability patching on existing IT systems are popular. This is not exactly case where user IoT security is not properly enforced, with automated firmware/software upgrades and patching processes. For IoT devices, user fixes or fixes are also not successful, (c) because of the small capacity, scale [12] and processing resources of many IoT devices it is challenging to use same security tests as are used on conventional computer systems.

Machine learning: Data from a large range of sources, including networks, computers, sensors, individuals, utilities and others, have been powered by an exponential increase in data in this period. Nowadays, a vast range of data-driven approaches is being used to achieve significant benefits such as value-added programs, resource management, new features, etc. Recently a strong revived interest has been seen in machine learning technologies in many applications. Cyber security has been one field in which we have seen development interests in the use of machine learning [13] [14]. Classification problems (e.g. assessment of reserves or detection of whether fruit is an apple or pear), as well as cluster problems, maybe resolve using machine learning algorithms [15] (e.g. distinguishing various classes of individuals based on their social backgrounds). Problems with classification (i.e., before analyzing data) are often resolved with supervised learning algorithms such as random forests [17] or neural networks. Unlabeled data clustering challenges are mostly resolved through unmonitored algorithms like the clustering of k -means and the use of DBSCAN [2]. In conclusion, enhanced learning is a different type of machine learning algorithm involving solution recognition, and is meant either to optimize or decrease a function (e.g. agent behaviors centered on a series of states that extend their contact with an opponent). This model uses a decision-making mechanism from Markov to model and iterate states and behavior to "read."

4. IOT CHARACTERISTICS AND COMMON ATTACKS

IoT systems often work in varying circumstances that are typically not the same as popular computer devices in their operating environments [1]. They also have specialized functions and targets and have their specific characteristics sponsored. IoT applications typically use conventional attack tactics to target the security flaws of their applications. We would then address some standard features and popular attacks on IoT computers.

Characteristics of IoT devices: We recognize certain special aspects of IoT systems.

a. Sensing: Various types of sensors can be used on IoT and multiple sensors can be mounted on a system in compliance with the application domain. These include body sensors, weather sensors, automobile sensors, etc. This sensor often leads; however, to error measurement rates or the loss of data (e.g., sensor misreads or reads not for a certain interval). The use of different mathematical approaches to rectify these anomalies is a well-known drawback of sensors [4] and tests.
b. Dynamic states: IoT systems work rather like any other machine network, as finite-state automatics at a device-level. Based on external shifts and the programming procedure, transfers between states (e.g. sleep, active) are predicted. These modifications often establish special requirements for the availability of data. For example, during the sleep of a system, a sensor [5] cannot read, resulting in missed information for that time. The lost data cannot be readily replaced by conventional methods (for example, the missing values use a regular average). An observer who watches a given computer instead will investigate whether the lack of data coincides with the system's condition and may mark the occurrence as a false positive. For automation of this process using machine learning algorithms, learning models need to integrate some network traffic activity unique to a system state (for example, when a computer is asleep, 80% fewer network packets are sent).

c. Connectivity: Wired network communication is also used for conventional networked computers. This is the case of industrial control systems. However, in these industrial control systems, wireless technology such as 802.11 networks, Zigbee and others are being used gradually. Many IoT systems now use Zigbee with low power consumption (so that battery life is extended). However, their performance (e.g. 250 Kbit / s) and a narrower range, these protocols appear to be much slower. The interruption caused by 802.11 connectivity, contributing to a spike in packet loss, also affects Zigbee communications.

d. Limited hardware resources: These machines tend to have minimal processing capacity to reduce expense of IoT devices and their power usage. The memory of certain IoT devices (those with as few kilo-octets) is by far the least available asset [18]. The availability of resources running on such platforms is often limited by CPU constraints. Both these hardware constraints explicitly impact the form of learning methods used to protect such IoT computers.
e. Heterogeneity: Another restricting property that also requires unique solutions for an IoT implementation is the wide variety of IoT configurations. Many applications, for example, use lightweight protocols such as MQTT [6], a publish-subscriber transportation protocol to transmit messages. MQTT provides better efficiency than HTTP and considerably less resource are required. However, we need a dedicated broker to gather the remainder of the IoT units, to use the MQTT. To gather sensor information, users enter the broker interface (instead of IoT devices).

Common attacks on IoT devices: We briefly explain several typical attacks on IoT devices to better understand advantages emanating from various machine learning security implementations. More thoroughly, but in the current literature, a discourse on attacks on IoT devices is beyond the scope of this article. Several popular attacks in the literature have been identified. DOS attacks disable IoT system to initiate other doS attacks by using a compromised computer. The first solution is to solve the simple contact medium used. The first solution is the second solution benefits from poor protection and servicing (for example, the IoT system vendor's default authorization keys will not be updated or the IoT device

owner will not upgrade periodically the firmware or functionality of the device, which also happens on many of these devices). DOS attacks will also lead to weak packets being generated to deactivate the system. E.g., to trigger a buffer overflow in the software system to manage this special exception, a field defined for a packet specifying a payload length may be replaced with an incorrect value. To interrupt network communications or operation of the system, an attacker may also replay previous packets in addition to falsely generating faulty packets. An assault requires the impersonation of actual computers in the IoT network, to reach or even set the stage for a potential man-in-the-middle assault. Man in the middle intrusion requires an intruder to wave in but also to change data sent via the medium of contact. In general, the attacker can impersonate the IoT gateway linking several IoT devices with a strong attack in this segment. An attack aims to obtain IoT channel information. Since detection is the first move in most attacks, readily available contact networks are also the attackers' prime target. For IoT messages, data shared locally or from afar are also not encrypted either because device administrators lack alternatives or negligence. Additional forms of attacks include the use of Trojans, worms and viruses to compromising, manipulating and obtain information from IoT devices.30,35 For example, a loophole on an IoT computer may be exploited by an assailant to mount a Trojan computer that provides him/her with access to the system.

5. MACHINE LEARNING: AN ABILITY TO IMPROVE IOT PROTECTION

The number of connected devices in different IoT environments (intelligent buildings, health care and critical infrastructure) is the, as we described above. Therefore, efficient security inspections are required, so that benign IoT data can be automaticity, evaluated and distinguished promptly. Receiving malicious traffic data and actions of machines operating in IoT environments, several academic activities have begun implementing machine learning techniques lately. Many drivers are responsible for this growth in the interests of machine learning strategies designed to improve IoT safety. This includes: (a) restricted capacity, computing power and network access of the resource-controlled design of IoT devices, which make these devices less manageable as compared with computers and networks. As a result, automating the processing of IoT data such that harmful and benevolent actions can be separated can be done employing machinery computing; (b) it is more difficult to implement machine learning methods [20] in conventional computer systems and networks than in IoT settings. The explanation is the regular disparities in traffic and activities of conventional network networks and equipment (such as bandwidth, length, delays and so on). Thus, in conventional network settings, it becomes more difficult to create a base line for "standard" traffic. IoT devices, by comparison, are usually programmed to perform unique and repetitive functions that stay the same throughout the IoT device's existence. This more predictable behavior simplifies the creation of a learning model for machines which uses IoT traffic data to discern benignly.

Machine-based solutions for security learning are feasible alternatives to conventional IoT security, which focuses primarily on access and encryption. However, such protections are bound to fail from a threat-centered defense perspective, and as such, an additional machine learning protection degree may be useful for improving safety. Machine apprenticeships are primarily classified into three major categories: supervised, unattended and improved. However, these solutions can be further separated into a network and host-based solutions

given the availability of network data. The same refers to regular network security protection strategies including network and host intrusion detection devices.

Figure 1 provides basic description of how machine learning techniques are applied at the host and network levels in the IoT context. Table 1 provides rundown algorithms for machine learning, their ability for networks and hosts, and several IoT-related problems. In the following pages, we discuss suitable methods of machine learning that are accessible on the host and the network levels. Our topic focuses on the effects of the relative characteristics of standard IoT devices (this involves technical limits, connectivity failure/latency resistance, lack of tolerance for data and dynamical state utilization). Based on their position, we also describe the strengths and shortcomings of these computer teachings.

6. NETWORK-BASED MACHINE LEARNING DEFENSE

In this group, machine learning methods allow for a range of approaches without computing capital limitations. The reach of encryption of network communications can, however, also restrict the potential to identify security events from network-dependent approaches. For starters, these network-based models won't read encrypted MQTT packets. Instead, the machine learning model must rely on network traffic efficiency observable metadata (e.g. IPs and ports) to better identify it. This method could theoretically be used to detect attacks by the middle man by network latency measurements through a regular machine learning system. For example, in Figure 1, a wireless router connecting IoT to the rest of the network can be imitated by an attacker, who would divert the traffic to the legal wireless router.

TABLE 1 Summary of machine learning approaches focused on influence of IoT system features

		Representative Algorithms	Computational Limitations	Communication Loss/Latency Tolerance	Missing Data Tolerance	Dynamic State Utilization
Network-based	Supervised	CNN, ADA	Low	Medium	High	-
	Unsupervised	DBSCAN	Low	Medium	High	-
	Reinforcement	SARSA, DQN	Medium	High	High	-
Host-based	Supervised	k-NN, SVM	High	High	Low	Available
	Unsupervised	k-Means, GGMs	High	High	Low	Available
	Reinforcement	Q-Learning	High	High	High	Available

Abbreviation: ADA, adaptive boosting; CNN, convolutional neural networks; DBSCAN, density-based spatial clustering of applications with noise; DQN, deep Q-network; GGM, Gaussian graphical model; k-NN, k-nearest neighbors; SARSA, state-action-reward-state-action; SVM, support vector machines.

This network topology transition can be detected by the calculation of disparities between input and outgoing packets during the round-trip time of the network-based computer learn IDS. If IoT devices and other LAN devices are on average talking frequently 100 meters, the additional node might theoretically boost the averaged latency by a few milliseconds above a standard deviation from the original network. The average latency over a given duration can be calculated as one attribute that can help detect these man-in-the-center attacks. This information is interpreted periodically by a learning machine model and a warning may be given if deviations are identified.

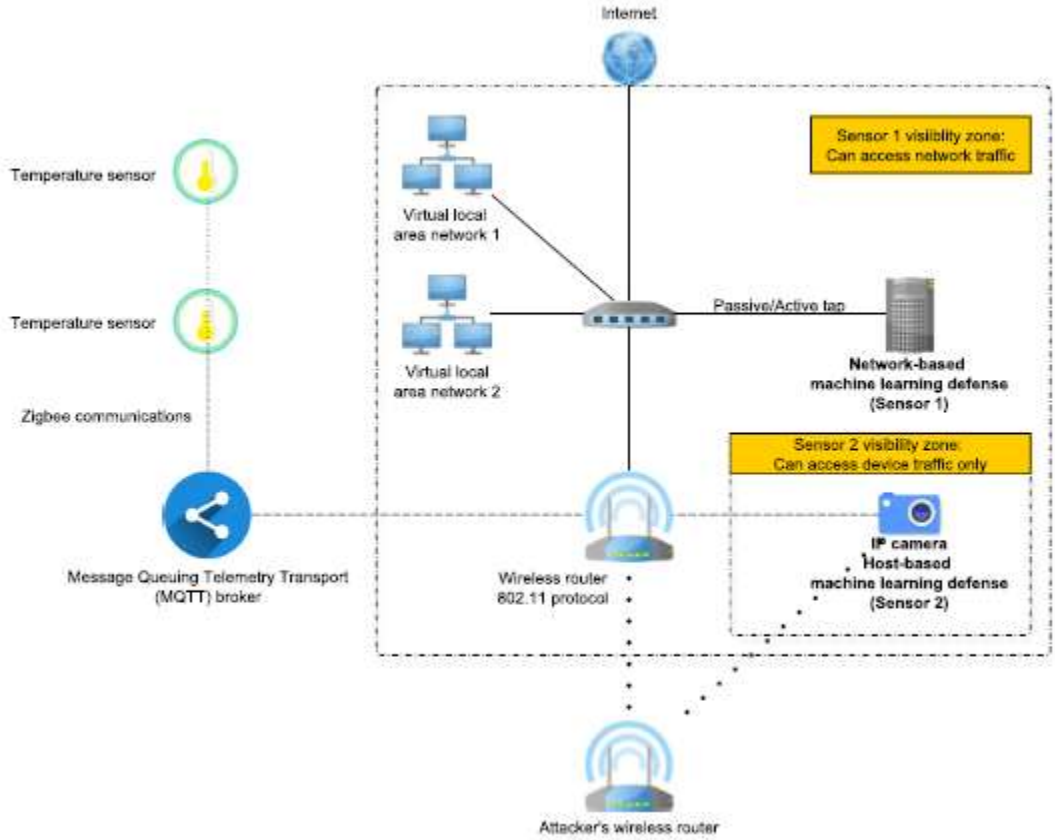

FIGURE 1 An example of an Internet of Things network (IoT) which uses different protocols of communication. MQTT is a protocol used for messages between IoT devices. MQTT is the protocol used with MQTT. The machine learning protections host and network are presented. Restrictions for tracking such interactions (for instance, temperature sensors for brokers) are often presented until other host-based methods are enforced. An example of aggression by a man in the middle is provided.

1. Supervised learning: Models supervised focus on recognizing recognized behaviors that differentiate benevolent and suspect behavior. From a network point of view, different attack styles that can generate network traffic (e.g. DOS and jamming) may be defined. To be able to define relevant data points (e.g. features), supervised models require setup in advance. As previously stated, IoT devices are very routine, simplified due to the utilities they provide and their one-purpose feature. Therefore, for supervised models, a finite number of usable data could be available that may preclude the need to use more high dimensional algorithms (such as deep learning) [16].

a. Resource requirements: Options such as vector support (SVM) or k-nearest neighbors (kNN), for network-based machine learning, can provide good outcomes when used in standard security analysis for the network. Also, SVM can also be computationally accurate and the same (once trained) model may be used to classify an adversary's malicious traffic. In kNN, the estimation in conjunction for each new data point (e.g. packet) allows the algorithm to be linked to a list of other data points already existing (training set). This means that there is no step of testing that generates a weight vector and the algorithm has to be republished each time against a training kit. Specifically, model-based approaches such as SVM,

regression or decision-making trees are more scalable across multiple networks whereas IoT applications are of the same type/vendor (i.e., network activities across networks are similar).
b. Missing data tolerance: IoT devices may encounter communication problems as well as data calculation errors that impair the analysis of network traffic. This makes it hard to distinguish between natural network behavior, which can confuse supervised learning models, and malicious network behavior. Large missing data sequences cannot, however, be effectively managed through supervised models due to connectivity issues. For instance, a failing communication or compromise could lead to lacking temperature reading by an IoT system for one hour. This lack of information must be supplemented by the preparation of a machine learning algorithm that contributes to several problems. The other problem with supervised models is that a forecast cannot be made where any data points are absent (unless the model is equipped in particular to recognize the importance of missed data). The lack of data traffic is natural or an irregular model, in other words, cannot be readily inferred.

c. Limited state information: IoT devices provide State information that network-based monitored models typically don't have access to, for example, an IoT won't broadcast when it goes to bed. Therefore, although hierarchical supervised learning models are possible (e.g. decision trees), they cannot be used successfully to learn different IoT behaviors in different states. These supervised models are not severely constrained, but cannot be used to their maximum capacity.

2. Unsupervised learning: Unattended preparation relies on the categorization (clustering) of data to differentiate between malicious and natural distribution behaviors. As a consequence, no simple fact (that is to say to the model, what malicious or benevolent traffic it looks like) is possible for the input. That means, however, that a person must perceive the output to see how malicious traffic is. As a consequence, approaches like hierarchical or clustering of k-means need more human intervention, since both are unattended learning algorithms. However, these techniques can identify night attacks; since unknown patterns can be grouped into the analysis of network traffic separately (depending on how machine learning functions are arranged in the model).

a. Resource requirements: Unattended preparation relies on the categorization (clustering) of data to differentiate between malicious and natural distribution behaviors. As a consequence, no simple fact (that is to say to the model, what malicious or benevolent traffic it looks like) is possible for the input. That means, however, that a person must perceive the output to see how malicious traffic is. As a consequence, approaches like hierarchical or clustering of k-means need more human intervention, since both are unattended learning algorithms. However, these techniques can identify night attacks; since unknown patterns can be grouped into the analysis of network traffic separately (depending on how machine learning functions are arranged in the model).

b. Missing data tolerance: If there is a lack of data generated by an IoT device or when the IoT device has been corrupted, the use of certain unattended algorithms is challenging. For starters, a full matrix with no missing data (e.g. null entries) is required to cluster k-means. This constraint can, however, be overcome by techniques such as k-POD (the form of k-mean clustering lack of data). In comparison, conventional unmonitored learning models make clear predictions about the normality of the knowledge and a standardized disparity between classes. The efficacy of unregulated learning algorithms would rely on noisy data generated

by IoT devices as a result of sensor measurement errors. Where noise data are usable, stronger methods such as Gaussian (GMM) or the spatial clustering of noise applications (DBSSCAN) based on hierarchical density [19] are needed. In contrast with others like ensemble methods, some computer models are not working well with noisy results. Compilation of methods aggregates prediction outcomes across several models (for example, the decision trees). The ensemble model, for example, would also identify traffic as malicious, if it had five decision trees and three of them categorized traffic also maliciously. So we can make sure we have chosen the right machine learning algorithm if the data are sound to ensure greater precision in the identification of malicious traffic.
c. Limited state information: These models do not otherwise provide knowledge about the State across the network compared to supervised learning. If state knowledge is available, it is also possible to use hierarchical clustering algorithms (for example a Ward method).

3. Reinforcement learning: The emphasis is on the setting up of environmental (state) and computer space. The algorithms in this category allow several simulations to be carried out based on behavior and state permutations leading to variable effects. These algorithms then follow winning strategies that are based on the environment. Implementing such algorithms at the network level is costly since the network has to be specified in several environmental states and behavior. E.g., in different locations in the network, a man-in-the-middle attack can be used and an arbitrary range of IoT devices may be used. In this case, although the compliance learning frameworks are not well-scale, the network security testing was successfully applied. It is thus possible to adapt these approaches to enhance network IoT stability.

4. Limited and dynamic state information: Since the status of a unique IoT system must be used in the enhancing learning model, the quality of detecting malicious network behavior is affected by the loss of data through the preparation or deployment of upgrades. This is particularly valid since IoT states and actions are all simulated while these models are educated. The monitoring of IoT states at the network level can be difficult in a particular scenario even though they are identified. For example, if an IoT system alerts you that it enters a sleeping state across the network because it is congested, it can lead the strengthening training model, since the sleeping situation is not transmitted on time, to perceive the traffic scarcity as a suspect. Owing to the poor efficiency of some IoT-devices networking protocols (e.g. Zigbee), improved learning on a network level can be difficult to enforce. Besides, the scale of the state space, as well as the way space shifts, are constrained by reinforming learning models. For example, it is difficult to ensure for most real-world situations that a strengthening education model makes the necessary choices at a cost. Increased learning, however, is restricted to the basic "scenarios" assault for large multi-state IoT networks.

7. HOST-BASED SECURITY MACHINE LEARNING

The use of machine learning security algorithms on IoT devices makes it impossible to detect threats from the traffic of networks alone. Figure 1, for instance, helps an intruder to subscribe to all channels posting messages using the MQTT protocol. In this attempt, the network communication would involve a computer and all messages must be transmitted to the MQTT broker. It is unlikely that this eavesdropping attack can be noticed or used using a network-based learning system (depending on the topology of the network), but such an

attack can be found with the MQTB broker software using machine learning. The framework used to test the system subscribing to all networks for the protective machine learning model is to confirm that the computer was previously approached by the broker and how long it was relative to other MQTT systems. The learning system will then use this knowledge to determine better the packages it should allow or mark as suspected after setting up a statistical profile. Then, when we are on the host for IoT computer protection, we study three types of machine-learning algorithms.

8. CONCLUSION

As more evidence points to enhanced decision-making, the Internet of Things devices are deeply integrated into organizations. Security problems, however, never take those resources into account. Besides, even though such steps are taken, there are distinct limitations on the guidelines and signatures for classifying potential opponents. We have looked at how we can boost IoT security through machine learning techniques at network and host levels in this post. We have also emphasized the strength and limitations of computer training algorithms given the unique features of IoT devices and their environment. Security scientists need to build advanced and cost-effective machine learning methods and apply existing machine learning strategies to help solve the device and environmental insecurity of the IoT ecosystem due to exponential growth.

9. REFERENCES

[1]. Weimin Qiu, Linxi Dong "Design of Intelligent Greenhouse Environment Monitoring System Based on ZigBee and embedded technology" IEEE International Conference on consumer Electronics-China, 9-13 April 2014.
[2]. Yun Du, Zengtao Xue, Quanmin Zhu, Xin Liu, Yuanzhuo Feng, and Suying Zhang "Design and Application of Intelligent Control System for Greenhouse Environment Based on CAN Bus" Proceedings of International Conference on Modeling, Identification & Control (lCMIC), 31 Aug.-2 Sept. 2013.
[3]. LIU Dan, CaoXin "Intelligent agriculture Greenhouse Environment Monitoring system based on IoT technology" International Conference on Intelligent Transportation, Big data and smart city(ICITBS), 19-20 Dec. 2015.
[4]. A.N. ARVIND, Keerathika D. "Experimental Investigation Of Remote Control Via Android Smart Phone Of Arduino Based Automated Irrigation System Using Moisture Sensor" 3rd International Conference on Electrical Energy Systems, 17-19 March 2016.
[5]. Izzatdin Abdul Aziz, Mohd Jimmy Ismail "Remote Monitoring Using Sensor in Greenhouse Agriculture" IT Sim 2008 Information Technology, 26-28 Aug. 2008.
[6]. Jorge E.Luzuriaga, Juan Carlos Cano. "Handling Mobility in IoT applications using the MQTT protocol "International Conference on Internet Technologies and Applications (ITA) - Wrexham, UK 8-11 Sept. 2015.
[7]. Urs Hunkeler & Hong Linh Truong, Andy Stanford Clark "MQTT-S – A Publish/Subscribe Protocol For Wireless Sensor Networks"3rd International Conference on Communication Systems Software and Middleware and Workshops – Bangalore India, 6-10 Jan. 2008.
[8]. Habibi J, Midi D, Mudgerikar A, Bertino E. Heimdall: mitigating the internet of insecure things. IEEE Int Things J. 2017; 4(4):968-978.

[9]. Bertino E, Islam N. Botnets and internet of things security. Computer. 2017; 50(2):76-79.
[10]. Gardner MT, Beard C, Medhi D. Using SEIRS Epidemic Models for IoT Botnets Attacks. In: Proceedings of the International Conference of Design of Reliable Communication Networks (DRCN '17). Munich, Germany; 2017:1-8.
[11]. Fong K, Hepler K, Raghavan R, Rowland P. IoT: quantifying consumer costs of insecure internet of things devices. Berkeley, CA: tech. rep., University of California, Berkeley, School of Information; 2018.
[12]. Help Net Security. The cost of IoT hacks up to 13% of revenue for smaller firms; 2017.
[13]. Munoz-Gonzalez L, Lupu EC. The secret of machine learning. IT NOW. 2018; 60(1):38-39.
[14]. Witten IH, Frank E, Hall MA. Data Mining: Practical Machine Learning Tools and Techniques. Burlington, MA: Morgan Kaufmann Publishers Inc.; 2011.
[15]. Chio C, Freeman D. Machine Learning and Security. Sebastopol, CA: O'Reilly Media, Inc.; 2018.
[16]. Shrestha A, Mahmood A. Review of deep learning algorithms and architectures. IEEE Access. 2019; 7:53040-53065.
[17]. Breiman L. Random forests. Machine Learning. 2001; 45(1):5-32.
[18]. Lloyd S. Least squares quantization in PCM. IEEE Trans Inf Theory. 1982; 28(2):129-137.
[19]. Ester M, Kriegel H-P, Sander J, Xu X. A density-based algorithm for discovering clusters a density-based algorithm for discovering clusters in large spatial databases with noise. In: Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (SIGKDD '96). Menlo Park, CA: AAAI Press; 1996:226-231.
[20]. Watkins CJCH, Dayan P. Q-Learning. Machine Learning. 1992; 8:279-292.