RESEARCH PROJECT

CSCI6704 – Advanced Topics in Networks

Dhrumil Amish Shah (B00857606)
dh416386@dal.ca

Network Intrusion Detection for IoT Security Based on Learning Techniques

Introduction

The Internet of Things is a vast ever-evolving network of devices that are able to connect with each other to send and receive data over the internet through the help of computing devices embedded in everyday devices. The devices include laptops, mobiles, smartwatches and many more, all of these devices are able to communicate with each other through the Internet, Bluetooth and other techniques with the help of embedded sensors within these devices. The industry is rapidly evolving with companies trying to focus on the rapid commercialization of the sector. This approach is leaving the devices vulnerable to various kinds of external attacks aimed at obtaining confidential information. With regards to IoT, a web of devices makes up a complete eco-system consisting of Websites, Applications, Social Networks and Servers via controlled smart devices as a Robot Network(botnet). What this implies is that a single well place attack aimed at taking down a botnet will cripple the entire ecosystem and all the devices connected within. A priority task should be to analyze the types of attacks, classify them accordingly and try and develop countermeasures against such attacks in the future.[1]

Scope of Survey

The survey focuses on trying to identify the threats to IoT and trying to classify them into categories. It also aims to specify existing defensive strategies and to try and find out possible replacements for the older defense strategies with the help of emerging technologies such as Artificial Intelligence and Machine Learning. The protocols, standards and technologies that can be applied to IoT are vastly different to the ones that can be applied to Wireless Sensor Networks (WSN) and Cyber-Physical Network (CPN). Furthermore, the context to the development of these standards with respect to the different types of networks is also relevant to trying to develop a strategy to prevent attacks. The survey finds that the most popular strategy employed to detect attacks in a network is the Network Intrusion Detection System (NIDS). Unfortunately, it was observed during the survey that the traditional NIDS techniques may be inadequate to IoT systems due to characteristic changes like constrained resources, limited power, heterogeneity and connectivity. Due to IoT being heterogenous all the devices have their own IP addresses which is a huge trust issue and render the traditional NIDS inadequate with cases of false alarms, inability to detect unknown/zero-day attacks. Hence, researchers are trying to include machine learning algorithms with these IDS to improve system security. Their effectiveness has led researchers to deploy these learning algorithms among IDS to improve the chances of detection of cyber-attacks, anomalies and abnormal behaviors among IoTs.[1]

Methods

The survey focuses on trying to research IoT vulnerabilities based on intrusion detection techniques, NIDS in general, traditional NIDs architecture with comparisons and NIDS based on learning techniques. The survey begins with the classification of threats to IoT, then the traditional methods for security and concludes with the methods based on upcoming technologies.[1]

Classification of Threats

The survey finds that most of the threats to IoT can be classified under two categories based on architecture system and threats based on design challenges in the IoT system. The IoT architecture comprises of three layers the Perception Layer, The Network Layer and the Application Layer. The Perception layer is the hardware layer and so it is vulnerable to physical attacks, shortage of resources. The network layer is responsible for the transmission of signals between devices, and it is vulnerable to data exchange, unauthorized access. The application layer is the last layer and is also known as the software layer as it is responsible for providing an interface to users with which they can communicate through the systems. It is vulnerable to compromised applications, challenges with cryptography. Threats based on design challenges consist of ***spoofing*** an attack based on stealing credentials to gain unauthorized access. ***Routing attacks*** focus on the protocols to divert the traffic through unwanted places or to generate fictitious routing behaviors. ***Tampering*** attacks focus on either tampering with the device itself or tampering with the data. ***Repudiation*** attacks is about devices exhibiting malicious behavior and then denying it. ***Information disclosure*** attack deals with unauthorized information access. A ***DDOS*** attack is known as Distributed Denial of Service ad it focuses on denying service requests with the help of multiple compromised nodes across various geographical locations. ***Elevation of privilege*** focuses on falsely accessing information without the required level of access. ***MITM*** attack stands for Man in The Middle, which functions by eavesdropping in a private conversation by a third party. User privacy is similar to information disclosure**.** ***Cloning nodes*** focus on reintroducing compromised nodes in a network to obtain or falsify information, disable functions, etc. Based upon all these types of attacks the survey classified a list of design issues which were Heterogeneity and Inoperability, Connectivity, Mobility and Scalability, Addressing and Identification, Spatio-Temporal Services, Resource Constraints, Data Interchange, Resource and Service Discovery and Trust and Privacy.[1]

Traditional Defense Mechanisms

After discussing and describing the types of attacks the survey focused on the traditional defence mechanisms that are in place currently to try and prevent the attacks. They came up with the following[1]:

- Filter packets with firewalls and proxies.
- Adopt encryption with cryptographic protocols, data storage encryption or Virtual Private Networks(VPN).
- Employ robust password authentication schemes.
- Audit and log activities on database servers, web servers and application servers.
- Detect intrusions using IDS (Intrusion Detection System).
- Prevent intrusions with IPS (Intrusion Prevention System).

NIDS for IoT based on Learning Techniques

Big Data Analytics is the core to collecting data that will be used by Data Mining and intelligent algorithms to try and deduct previously undetected relations between data entities to predict and react to situations. Machine Learning is an artificial intelligence technique that is widely used in data mining. There are two types of ML algorithms:

- Supervised learning is based on learning from labelled training data which means that training data includes both the input and desired results.

- Unsupervised learning is based on clustering the input data in classes based on their statistical properties only.

The Machine Learning Algorithms used in these techniques range from decision trees (DT), support vector machines (SVM), naive bayes (NB), artificial neural networks (ANN), k-means clustering, fuzzy logic, genetic algorithm, stacked autoencoder (SAE). Initially, these algorithms have been used individually and later on were used in a combination of these algorithms to deeply understand the impacts on the results.[1]

In terms of NIDs based on learning techniques, the IDS was deployed either in a Distributed or Centralized way in most cases. The detection methodology for most cases was Anomaly-based. The datasets used to test these situations ranged from Simulations, Real IoT Devices, KDD99, NSL-KDD, Generated datasets and a combination of Simulation/Emulation in conjunction with NSL-KDD/KDD99. These learning techniques were used to treat threats ranging from but not limited to DDoS, Unauthorized Access, Botnet Attacks, and Sinkholes. A variety of Machine Learning algorithms were used in these tests that include Multi-Layer Perceptron, Logistic Regression vs SVM, Artificial Immune System (AIS), Supervised and Unsupervised Optimum Path Forest, Stacked AutoEncoder (SAE), Multi-Layer Deep Learning and Online Sequential Extreme Learning Machine (OS-ELM). Most of these techniques are useful to detect and prevent specific types of attacks but only a few of them are ready to prevent unknown attacks.[1]

Results and Discussion

The survey finds a lot of the traditional defense mechanisms used to protect the network from attacks to be incompatible with IoT simply due to its nature and complexity. An entirely new system of protocols combining multiple learning techniques, datasets, algorithms needs to be implemented in combination to support each other's shortcomings to design a comprehensive and precise Network Intrusion Detection System that is able to be scaled to accommodate the increasing number of devices capable of supporting IoT. Most issues regarding current techniques ranged from the datasets. Latest datasets need to be established in order to create systems that can react to any type of unknown attacks as well as manage the known type of attacks. Another aspect that needs to be taken into consideration is the size of the device and the intensiveness of the processes running on it, as highly intensive processes can be executed on large and powerful devices, but the opposite is true for smaller devices. Any solution that can be feasible needs to be a good combination of deployment, detection methodology, the datasets that are used and proper Machine Learning Algorithms.[1]

Open Research Challenges

The field of IoT is vast and ever evolving and so there are many challenges that need to be addressed in order to accommodate a large number of devices and the ability to protect the data in these devices. Some of these challenges include end-to-end security on devices, seamless scalability on either vertical or horizontal levels, design of low-cost terminals for IoT devices.[1]

- Issues in scalability depend upon vertical scalability which refers to adding computational resources to a node. Apart from that, other issues ranging from security and privacy to access control and data storage.
- Issues in security happen due to the lack of proper standards that can be enforced with wireless devices presenting an entirely new set of challenges.

- There is currently a transition occurring from IoT to the Internet of Everything (IoE) due to demands to make the devices and networks more proactive to enable a seamless user experience. The systems need to be able to proactively react to the changing environments.
- Another challenge is to develop Energy-Efficient IoT networks. Researchers have tried to combat this challenge by trying to develop wireless networks. Currently, the nodes in use are being overloaded with resources to adapt to the increasing functionalities being added to devices every day, but this leads to a compromise between fidelity and power efficiency.

Conclusion

The current lifestyle has become hugely dependent on the array of devices that we have designed and developed to help with our tasks and for entertainment purposes. Devices now range from Computers to Laptops, Mobiles, Smart Watches, Smart Homes and many more that are connected to the internet to create a seamless experience for users. However, this is a huge danger as well because this whole interconnected network of devices can be sabotaged to cause lasting damage to networks, Data and users. Because of its nature even one infected node in the network can be used to bring down the entire network. Another possible disadvantage is that the data being collected continuously from various devices can be used to Social Engineer people towards choices that are beneficial to the Highest Bidder; for example, people could be influenced to vote for a particular person in an election, insurance companies could increase the premiums based on the spending habits of customers and so on.[1]

Then there is the issue of security in the ever-expanding network of IoT devices. The use of Network Intrusion Detection Systems (NIDS) in conjunction with multiple machine learning techniques is one of the best solutions that can be used to combat the new emerging threats to this network.[1]

The future for these devices must include a dedicated dataset to improve network exchanges. There should be a clearly defined list of protocols that are able to adapt to the current devices and technology standards.[1]

The survey has been thorough in trying to go through its goals to identify the use of Machine Learning Algorithms in IoT devices. The comprehensive comparison of current standards and protocols and the research being carried out on the newer standards are able to properly demonstrate the importance of their premise. Further, the papers cited as references also contain veritable sources of data that support their survey.[1]

References

[1] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, thirdquarter 2019, doi: 10.1109/COMST.2019.2896380.