The Layer wise Security model in Internet of Things: A Novel Perspective

Feroz Khan A.B¹, Dr. G. Anandharaj², Dr. K. Arulanandam³, Dr. T. Balasubramanian⁴

Department of computer science¹,²,³,⁴, Adhiparasakthi College of arts and science¹,², Govt. Thirumagal Mills College³, Sri Vidya Mandir Arts & Science College⁴, Vellore¹,²,³, Krishnagiri⁴, Tamilnadu, India

ABSTRACT

IoT security is concerned with safeguarding the associated gadgets and systems in the Internet of things (IoT). The goal of this paper is that the conduct of various security related issues encompassing the internet of things and proposed countermeasure. In the next few years it is expecting that 50 billion of new devices are to be connected to the IoT. Hence the IoT network will face critical security risks because of this continuous growing network. In this work we plan on investigating some of these security issues as well as existing and proposed solutions for dealing with them. Also the various DDOS attacks are modeled in this work which gives the practical perspective of tasks that is implemented on the occurrence of the DDOS assault. The work proposed a new countermeasure called TBC (Threshold Based Countermeasure) for reply attack, which is considered as the most catastrophic attack. The result shows that the proposed mechanism TBC works well in the existence of reply attack with increased malicious node in the environment thereby by increasing the efficiency of energy and time delay.

Keywords: IoT, security attacks, preventive measures

This article has been retracted from International Journal of Communications and Networks per the request of authors. Please do not use it for any purposes.
I. INTRODUCTION

The Internet of Things (IoT) comprised of interrelated things such as computing gadgets, wearable devices, handheld devices, digital machines, mechanical devices, people, objects, or even animals that are provided with unique identifiers with the ability to send and receive data over a network without the need for human-to-human or human-to-computer interaction. A thing, in the Internet of Things can be anything on the planet, it can be a person with a Blood pressure monitor implant, a farm animal with a transponder, an automobile connected with sensors to make the driver alert when the pressure of tire is low—or any object that can be assigned an IP address and provided with the ability to transfer data over a network.

It is predicted that 50 billion devices will be associated with the Internet by 2020 and 500 billion by 2025 [14]. These associated gadgets—prominently known as the Internet of Things (IoT) that represent a great potential for the upgrade of social and business life and for market development. IoT devices helps for the extension of internet connection to anything apart from the day-day devices like computers, laptops, smartphones etc. From wellness trackers and self-driving autos to shrewd broilers, automated home lighting, and air-conditioning system, there are innumerable new developments and buzz about these interconnected devices and arrangements. Some of them have even progressed toward becoming a piece of shoppers' everyday life. Be that as it may, those are just a hint of a greater challenge. With this increase in accessibility, there is an increase in the need for strong security measures. Therefore, The IoT will likely be one of the most important technological advances of this century.

A. IoT Smart Home

The appearance of IoT devices at home can change our lifestyle providing smart technologies with the help of sensors that communicated and controlled remotely over the internet. The people with busy schedule can make their live easier just by connecting their home appliance to the IoT device. Thus machine-machine interaction is possible without human intervention. Cloudwash is one example of IoT Washing Machine. You can connect your washing machine to the IoT and you can control it anywhere from your phone. You can also set number of cycles required for washing through your phone. It is very helpful to the person who want to clean the laundry by the moment they come home from office. Another smart device is August Doorbell Cam, it is an attractive IoT invention. August Doorbell Cam can able to answer your door remotely. It continuously check your doors and it capture any motion changes at your doorstep. The next IoT is WeMo Light Switch, it is used to manage the lightings in the home through wall or mobile or through voice. It is connected to your existing internet for providing wire-free access to home lights. Nest Smoke Alarm is another kind of IoT device which is very useful to report any emergencies from your home. It is used to detect smoke, it talks to you and alert you for what’s going on in your home. There are so many smart devices available in the market today and the above list of smart devices are the top IoT devices in the world.

B. IoT at Workplace

Today’s workplaces have been converted to interconnected systems where people work together with technology. In workplace, the assigned jobs and duties are nowadays shared between employees and computer devices to achieve efficient productivity on business.

Most of the Internet of Things (IoT) devices introduced for the workplace are small devices to run the workplace more efficiently. For example programmable power strips is used in
the workplace for advanced power management via internet. It is used to switch on/off the electrical appliances from anywhere using the mobile phone or computer system. This will help the management to save the power resources by switch off all electrical appliance when not in use. Another device coming for market is that it sends notification to the sanitary workers to let them know which garbage bins are full. This allows them to ignore the places where bins are not filled or empty which reduce the time of the workers. Further this will save fuel/gas, and hence time and money.

It’s really a challenging task to implement IoT in the workplace IoT due to largely connected devices, employees and the devices have to be connected all the times and the privacy protection is the most critical issue than in other networks. However, the company can minimize the cost if it effectively implement IoT infrastructure. Wifi device connected via IoT is the important concern that no one talks about, if the companies provide high speed routers like wifi-6, it can be connected with multiple devices, and speed of the devices can be much faster even in a busier networks.

C. Future Considerations

Everyone, from consumers to industries, is adapting the changes provided by the revolution called the Internet of Things (IoT). It has changed the world brand new than we could imagine until a few years back. And these changes and advancements will be continued in future also. With the huge number of increased devices in the IoT connected environment, strong security need to be implemented to safeguard the IoT devices from the attacker. Homeowners need not concern about someone hacking into their refrigerator, but when home automation is implemented in their home, they will worry about if someone unlock the security system by hacking the Wi-Fi router where all devices are connected. Companies need to implement strong security to the Wi-Fi and they have to ensure that the devices are protected from outside access in order to safeguard the company databases. IoT infrastructure are also implemented in hospitals for tracking and monitoring the patients with the sensors attached in the patient’s body. Here the important goal is to make sure the safety and privacy of the patients by implementing strong security. IoT devices are also used in schools and universities for interaction between people and objects through various sensors and wearable technologies for providing smart class rooms, smart parking etc.

India is one of the countries where new invention is going for IoT across different technologies. The IoT ecosystem in India is mainly driven by 3 players: Government, Industry and Startups. There will be a lots of scope for IoT in India and Govt. has correctly recognized it and working towards its implementation. The government has initiated and drafted policies for developing IoT smart devices based on our country’s requirements. Government’s objective is to create an IoT industry in India of USD 15 billion by 2020. One of the key initiatives of the Government is to build smart cities across the country. Major aspects of a smart city being focused by the Government are:

- Smart parking
- Intelligent transport system
- Tele-care
- Woman Safety
- Smart grids
- Smart urban lighting
- Waste management
- Smart city maintenance
- Digital-signage
- Water Management
II. SECURITY

A. Security Attacks classification for IoT

When it comes to security we often think about physical security like locking our two wheeler or car or locking our home door. It is not guarantee that your bike cannot be stolen because you hold the key. Security is about protecting the things from malicious attacker by making the mechanism very hard to break or making it impossible. The purpose of internet security is to create rules and actions to protect against attacks over the internet [1].

<table>
<thead>
<tr>
<th>Layer</th>
<th>Possible Attacks</th>
<th>Security Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1</td>
<td>The two important attacks are jamming an eavesdropping.</td>
<td>This can be prevented by applying strong encryption techniques and hence confidentiality is preserved.</td>
</tr>
<tr>
<td>L2</td>
<td>Flooding the energy resources, denial of sleep are major attacks at L2</td>
<td>Encrypted tunnel have to be established for the communication over the network so that channels can be authenticated.</td>
</tr>
<tr>
<td>L3</td>
<td>Routing attacks, Sybil, DOS, DDOS attacks can be occurred at L3</td>
<td>Apply encryption algorithm for all the connected devices during communication.</td>
</tr>
<tr>
<td>L4</td>
<td>Traffic analysis, message modification and falsification of packet.</td>
<td>IDS can be implemented to detect this kind of attack so that it alert the system when data comes from unknown sources.</td>
</tr>
<tr>
<td>L5</td>
<td>Exploitation of Message integrity, non-repudiation, confidentiality.</td>
<td>S/MIME, SRTP can be used for security in application level.</td>
</tr>
</tbody>
</table>
The primary goal of internet security is to protect the confidential data. Before start to design the security system one must have the clearly specified requirements for what kind of security is required and what are the vulnerabilities that the system may exhibits. Then you must have the plant that will focus security from requirement gatherings to implementation with respect to SDLC to protect against identified attacks over the internet. The main object of this work is to classify the possible attacks in the IoT and proposed solution is constructed for DDOS attacks.

III. LAYER WISE SECURITY MODEL

A. Layered Model

Security for IoT is crucial that can be applied at various levels of internet security protocols. By using Layered model we can aggregate the technologies used in each layer. This layered model follows TCP/IP model which includes 5 layers (L1 to L5): application layer, transport layer, network layer, link layer and physical layer. The application layer is the upper layer that act as interface for the user application for IOT enabled devices. The network layer determines the optimal route to reach the destination node from the source node. In this layer IP address is uniquely assigned in order to communicate over the internet. The Transport Layer is used to transfer the data to the user application after obtaining IP-address from L3, here end-end communication is possible. The important functionality of link layer is placing the frames on the medium and making sure it is error-free. In L2 MAC address of the wireless devices are used for the communication. Physical layer happens to be the radio layer for wireless communication among IoT devices. FHSS/DSSS can be used for authorized communication among the network devices. Figure 2 shows the protocols involved in IoT layer model.

B. Physical-Layer Security

The two major attacks performed in physical layer are jamming and eavesdropping. Providing security at physical level involves the uses of spread spectrum technologies to avoid unauthorized interception. Hence this kind of security is used to prevent the existence of node in the communication to the interceptor but if the interceptor finds the details of the communication system then the network can be compromised. So spread spectrum cannot be considered as proven security system for physical security[4]. One of the crucial security issue in physical layer is pilot contamination. The recent effort made to state the secrecy of channel is MaMIMO (Massive Multiple Input Multiple Output) in pilot contamination. This is happening in BS under interference. Through pilot signals BS want to identify the user devices, these signals can be interfered and corrupted when received at BS level. This is very difficult to detect this interference. Recent research presented three variation of 2 N-PSK methods for the detection of this attack. To compare the performance of numerous physical layer security approaches, two important metrics, secret channel capacity and computational complexity can be used[6].

C. Encryption

Network applications often secure their data with encryption due to high risk of threats while transit. But encryption is not a solution for all types of assaults in network. Encryption can never be more secure without key and key management is still a challenging issue concerning security. Applications that are transmitted over the network can be encrypted either between two hosts called link encryption or between two applications called end-to-end encryption. In both form of encryption techniques, key distribution is always a critical issue. keys which are required to encrypt and decrypt must be
delivered to the sender and receiver in a secure path.

**i. Link Encryption**

In link encryption, data are encrypted just before the system places them on L1. Similarly, decryption will be done when the communication arrives at the receiving host. Figure 4 shows the working mechanism of Link encryption. Since encryption is performed in L1 message is exposed in all other layers of sender and receiver.

---

**Figure 2: IoT Protocol stack**

**Figure 3: Pilot Contamination [14]**
The message which is passed in intermediate hosts are also in clear because routing is performed only at higher layers. Hence intermediate hosts cannot be trustworthy. So this is suitable only with trustworthy hosts.

ii. End-to-End Encryption

As its name implies, end-to-end encryption provides security from one end to the other end. The encryption will be done at L7. With end-to-end encryption, messages sent through several hosts are protected. The data content of the message is still encrypted, as shown in Figure 5. Therefore, even when the message pass through potentially insecure nodes on the intermediate path between sender and receiver, the message is protected against disclosure while in transit.

D. Data Link Layer Security

The security for messages at L2 is more obscure than L1. The role of layer 1 is to place the input frames on the medium and ensure the error-free delivery of packets. The security is crucial because it expose all the MAC address of communication devices connected in the network. An example of L2 threat is Hello flooding attack. Routing protocol retains the connections of the node only if Hello message packets arrives periodically from the concerned node. Attacker use this packet and sends Hello packet repeatedly in order to flood the path. Several counter measures are available against Hello flood attack. In multi path data forwarding technique, sensor node will maintain different keys. BS will have control over particular group of nodes and there are common means of communication among BSs. Each base station stores all the secret keys shared by all sensors nodes. Whenever sensors approach the BS new will be assigned each time but computational overhead involved in this method makes the process slow. In the other method identify verification protocol, the nodes in either direction are verified based on the feedback message in encrypted form. This method is not efficient if any of the node is compromised. There are two major goals in performing link layer attack:

(I) flooding the resources in the network.
(II) Performance degradation of the service. Another interesting attack is denial of sleep, sleep mode is enabled in WSN when the node is in idle state to save the energy resources. To protect the network from this attack, strong authentication is required first. Secondly anti reply technique must be applied using protocols such as CARP.

E. Network Layer Security

IoT nodes can exchange data securely using IPSec

protocol suite in L3. IPSec is a part of IPv6 used for establishing secure communication between host – host or network – network or between gateway and host. IPSec is effectively used to prevent from reply attacks. IPSec is further broken in to multiple protocols

- ESP (encapsulated security payload)
- AH (authentication header)
- IKE (Internet Key Exchange)

The security services offered by AH are authentication and integrity services, ESP provides authentication, integrity and confidentiality. IKE provide key management services.

Confidentiality enables communicating nodes to encrypt messages and prevents eavesdropping from third parties.

Origin authentication and data integrity provides assurance that a received packet was actually transmitted by the source in the packet header and it confirms that the packet has not been altered otherwise. Key management allows secure exchange of keys between two parties.

![Fig.5. End to End Encryption](https://escipub.com/international-journal-of-communications-and-networks/)
AH
To avoid computational overhead AH only lets the receiver to verify that the message is intact and unaltered, it will not perform encryption on data. Figure 6 shows the AH in tunneling and transport mode.

IKE
AH and ESP require encryption and authentication Keys. IKE is responsible for creation of keys for AH and ESP and providing authentication during key establishment process. If the keys are sent over insecure channel, then it can be compromised, to overcome this IKE is divided in to 2 phases

Phase-1 (key selection)
In phase-1, it creates encrypted channel between two devices by using algorithm like D-H key Exchange, here two devices are authenticated by exchanging selected keys and the data is not exchanged here. Phase-2 (creation of encrypted tunnel)
In phase-2, two parties use the secured channel created in phase-1 and they use those keys for creating encrypted packets. Then the data can be exchanged.

Fig. 6. Authentication Header

The major issue that can be occurred in network layer is direct attack simply by altering the path of routing to the attackers’ own route and so the data can be diverted towards the attacker. Therefore strong authentication mechanism need to be implemented with the help IPSec protocols[9].
Alternate to IPSec is HIP (Host Identity Protocol), the primary goal of HIP is protect the host identifier and host locator from the attackers. HIP is introduced based on public key cryptography, Host identity is protected with pair of public/private keys where private key is kept at the host and public key is used as the host identifier. HIP also utilize ESP in IPSec for creating secure channel between pair of hosts. HIP also supports multipath routing and mobility for IoT based networks.

F. Transport Layer Security
In current IP infrastructure, exchange of data can be occurred securely in transport layer through TLS/SSL. TLS is the widely used security protocol in the IP environment for secure communication between applications. It provides data authentication services, integrity services and supports anti replay and confidentiality. DTLS is used in datagram services for the same security service for UDP. It is currently used in IoT environment because it uses UDP as transport protocol and DTLS is standardized as security protocol for CoAP. But still there are some issues in DLTS because of limited packet size supported by IEEE802.15.4
enabled devices. For this reason, DTLS experienced additional overhead during exchange and transport phase during fragmentation. This overhead can be minimized by using packet optimization and compression techniques with the help of 6LoWPAN. Although DTLS is standardized in IoT, it does not support multicasting only point-point communication is secured. Hence cluster key management should be introduced in IoT to support multicast communication.

G. Application Layer Security
Application layer supports end – end encryption in application level. This will simplify the needs for bottom layers and it reduced the computational overhead introduced with respect to packet size and data processing since encrypted data can be easily implemented in application domain. The main issue in application layer security is the poor reusability of codes that will introduce increased code size. This is because secure protocols are not well defined in application level.

To overcome this issue, S/MIME (Secure Multipurpose Internet Mail Extension) and SRTP (Secure Real-time Transport Protocol) can be helpful for providing services such as confidentiality, integrity, authentication and non-repudiation of source. MIME can be extended for any application data although it is developed for securing mail services. Similarly RTP is originally developed for real time data services to support real time data such as voice or video but it can be extended for any application scenario. However still more exploration is required to find out which is the suitable protocol for securing data at application level in IoT environment.

IV. Analysis of Different IoT attacks and Countermeasures
Security for IoT is critical due to various types of threats in the environment. All types of attacks are classified in to two: Active attacks and Passive attacks, former will damage the environment physically, later will be involved in eavesdropping or interception without making any physical damage to the network. Further these two types can be possible either internally or externally called internal attacks and external attacks. These kind of attacks can be prevented by using strong authorization and authentication mechanism. Although CoAP is introduced at L5 as in figure 2 for communication between smart devices and other internet devices, there is no mechanism for authentication and data protection, these should be implemented at application layer itself because depending lower layer security will not guaranteed the trust level without the support of higher layers. So end-end security is guaranteed only if security mechanism is implemented at L5/L3 in addition to PHY layer and MAC layer security.

When we consider communication layers such as physical layer, link layer for IEEE802.15.4 devices, these layers will use MTU for effective transmission of packets that will make the payload to be divided in to number of pieces called fragmentation that leads to higher overhead and delayed transmission. Also the energy consumption will be higher for the processing of large number of packets in the network which cannot be suitable in battery constraint devices. Even though end-end encryption at L3 and SSL at L4 guaranteed the security when combined, it leads to additional computational cost for setting up secure channel. So to combat these kinds of issues modern energy aware resources and compressed security protocols in all layers are required in order to reduce the computational overhead and to save the energy.

V. PROPOSED MECHANISM
The most important requirement in IoT is to achieve
low energy consumption along with minimum delay and maximum throughput. These required characteristics will increase the performance of IoT but the network suffers from security attacks
in different layers of IoT. The primary idea of this work is to model the behavior of DDOS attack [17, 18], a kind of the denial of service attack [4] which sends malicious traffic to the channel for the purpose of denying access to it. IoT is largely suffered by the various version of DDOS attacks at each layer. This paper primarily focused on DDOS attacks which can be occurred at two layers: PHY layer and MAC layer. Since the main responsibilities of these layers are allocating the resources, attacks here is more harmful to IoT. The several types of active and reply DDOS attack executed on IoT constraints based behavior, by raising the consumption of energy with maximized delay and minimized throughput which are the parameters for the Quality of service (QoS) of IoT. The several kinds of DDOS attacks are constant blocking, illusive blocking, random blocking and reply blocking. In this paper, we have identified many DDOS attack among which Reply attack is considered as the most important type which damage the network in its existence. The UML activity modelling for Reply attack is considered, it presents the required solution for minimizing the consequence of attack on IoT. The next important thing proposed in this paper is the analysis of different counteragents on DDOS attack.

Fig.7 Reply attack
Fig. 4 demonstrates the activity diagram of reply blocking. The series of steps involved during the occurrence of this attack are given below:

• The reply blocking assault is executed from the malicious node by attacking the non-malicious node in the network, then the victim node behave as a reply jammer, if attack is not success than the normal node will do its assigned operations.

• The noticeable characteristic of this assault is, it start executing if other node is busy sending the packets or the channel is unavailable.

• After ensuring that the channel is free, the normal node will try to send some packets to target node and it use the channel for sending data.

• The node act as a jammer will find if the channel is available, if so it goes to silent state, in this state the node will not be active, otherwise the jammer node starts activated and create the noise data repeatedly which leads to jamming in the network.

• The reply jammer will start working after finding that the channel is not free. So it is very hard to discover its presence in the network and it decrease the throughput of network.

The work done here introduces the threshold based blocking counteragent (TBC) to identify the DOS attack. The main goal of this algorithm is to improve the performance of IoT environment in the existence of reply blocking attack by safeguarding the IoT from the serious effects of reply blocking. TBC saves the network by storing threshold value in each node in the environment. The algorithm can accomplished it by having sending threshold which tells the maximum data that a node can transfer.

The points given below are considered in the simulation:

• To measure the effectiveness of the attack and the effectiveness of its counteragents, first we perform the simulation by moving traffic interval under various traffic situations. Traffic interval that we consider here ranges from 1 to 10. We consider traffic interval 1 as quick traffic and 10 as down. In this part we examine misbehavior nodes in the environment.

• Secondly different misbehavior nodes are included in the network. The misbehaving nodes in the network we considered are 1, 2, 4, 8 and 16. In this work we consider traffic interval 1 for fast traffic. To examine the impact of attack and its counteragents we have increased the malicious elements in the environment.

• Here we consider some practical conditions in the next set of simulation. Each node present in the environment will not send any data in the same time and the traffic interval consider here randomly differs from 1 to 10 since the traffic interval in random.

In the final part, the simulation is done with the inclusion of random mobility to each node in the environment. In this step we consider random traffic interval within 1 to 10 in a random fashion. It is also seen that mobility speed differs from 1 to 25 km/hr. We can see the actual behavior of the algorithm in this simulation from the analysis of random mobility and traffic interval.

Fig.8 and Fig.9 shows the computation of average energy consumption, time-delay and throughput when changing the traffic interval and time. The result gives that the TBC mechanism really enhance the energy utilization, time-delay, and throughput better under reply blocking attack. TBC detects the blocking attack after examining the network and it decrease the impact of blocking attack by isolating the blocking node from the environment.

VI. CONCLUSION

In this paper, the security requirements of IoT was explored by layer wise security model. The data security and user privacy has been identified as the important challenges in the IoT. The security issues and requirements at different layers are analyzed and countermeasures are suggested especially in
the area of IoT. The major security attacks in IoT are classified and countermeasures are discussed. Further we identified different attacks based on different layers form L1 to L5. Also we identified some challenging issues while investigating various security protocols, packet optimization and compression techniques are suggested together with DTLS to minimize computational overhead while performing fragmentation.

The performance of the TBC we introduce here is measured by considering with practical conditions where every node in the environment isn’t transmitting at the same time yet nodes are transmitting at various time case. The outcomes with various conditions demonstrate that TBC is great choice for reply blocking attack. The results from the simulated environment by considering mobility demonstrates TBC is adaptable when shifting the location of node in the network.

The future of IoT will grow as expected only if the user trust in the security and safety of connected devices are guaranteed.

Fig.8: Average energy consumption with time interval

Fig.9 Average energy consumption with time delay.
REFERENCES


