ORIGINAL ARTICLE

Multi-layer Security Model for DDos Detection in the Internet of Things

Feroz Khan A. B*, Anandharaj G

PG and Research Department of Computer Science, Adhiparasakthi College of Arts & Science, India

*Corresponding author abferozkhan@gmail.com

Received: 14th February 2020
Accepted: 26th March 2021

OPEN ACCESS

Abstract: IoT security is concerned with safeguarding the associated gadgets and systems on 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 new devices are to be connected to the IoT. Hence the Internet of Things will encounter highly security risks because of this continuing 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 classified in a multilayer approach and the reply attack is modeled which is the variation of DDoS attack that 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) which detects the jamming in the communication environment and protects the network from the reply blocking attack, which is considered as the most catastrophic attack among all DDoS attacks. The proposed countermeasure is examined by considering the increasing number of blocking nodes in the network. The result shows that the proposed mechanism TBC works well in the existence of a reply attack with the increased malicious node in the environment thereby increasing the efficiency of energy and time delay.

Keywords: IoT, Layered model, TBC (Threshold Based Countermeasures), security attacks

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 market development. With this increase in accessibility as shown in fig.1, there is an increase in the need for strong security measures. The main reason that the performance of the network lower because it requires large energy consumption due to its minimal battery power. Therefore, the important requirement to achieve QoS in the IoT environment is to reduce the energy consumption. This important requirement is mainly affected by various security assaults happening in different layers of the network. The main objective of the paper is to obtain the effective security mechanism for jamming attack. We proposed a new security mechanism called TBC against a reply jamming attack. This TBC uses threshold value in each node connected in the environment to discover the attack. First, the mechanism proposed will permit the attack inside the network then blocks it after detecting the attack. All the nodes maintain some threshold value. The

TBC starts working by comparing the threshold value maintained in each node with the current transmission. If the threshold value exceeds the limit then it means that the attack has occurred and the information is sent to all the connected devices to isolate the malicious node from the network. The proposed work is simulated using NS-2 considering the realistic condition. The result shows that the algorithm works well in the presence of reply blocking attack by adding number of malicious nodes in the simulation environment.

Figure 1. IoT Model

Organization of the paper is given here. In Section 2, we discuss the related works in multilayer security approach for the IoT environment. In Sections 3, the issues and challenges identified from each layer of the OSI model are discussed. In Section4, we discuss the security analysis and in sections 5, 6 we propose our algorithm TBC with relevant work for countermeasures. In section 7 we introduce the TBC algorithm to identify the DDoS attack and in section 8, the simulation of the proposed mechanism is presented. Finally, we conclude the work in Section 9.

Related Work

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 guaranteed that your bike cannot be stolen because you hold the key. Security is about protecting the things from the 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].

The primary goal of internet security is to protect confidential data. Basically, the security of any system needs to satisfy the three principles CIA. In a typical network environment, CIA (Confidentiality, Integrity, Availability) are ensured through encryption and decryption methods. But embedded devices cannot cope up with these cryptographic methods due to the energy constraints of the embedded devices. So CIA has to be implemented at each layer of IoT to ensure the safety of embedded devices in the IoT environment. Before starting to design the security system one must have clearly specified the requirements for what kind of security is required and what are the vulnerabilities that the system may exhibits are. Then you must have the plan that will focus security from requirement gatherings to implementation with concerning SDLC to protect against identified attacks over the internet.

This section discusses the requirements of the security mechanism in the IoT environment and IoT security related issues with recent studies.

In [5], M.Daniel suggested some techniques to safeguard the IoT environment from cyber-attacks such as protecting the identification details using cryptographic keys, automatic intrusion alert, and the frequent updating of the system to save the network from hidden threats. Al-Gburi et.al [6] describe the IoT reference model with the classification of threats in each layer of the IoT model and the layer wise security threats are identified. They also suggest the security guidelines to protect the IoT environment from various threats classified in their work. B. Payne et.al [7] investigated the threats in hyper connectivity and IoT and the cause of threats during data transmission. They suggested to implementing strong security policies while deploying the network to the outside world. They discuss the various security standards and policies for IoT networks.

Shruti et.al [8] proposed a security framework for IoT networks. Several challenges were identified by applying their framework with the case study of the Remote patient monitoring system. They conclude the work with the need for device specific security algorithms. In [9], Shainika et.al gave some recommendations to protect the WSN network from security risks. The work proposed CMKM, a cluster based key management scheme for cluster based mobile environment. This improves the scalability in the mobile environment and lowers the energy consumption. Here ECDSA encryption method is used to lower the energy consumption but the hash function used here is more complex to create digital signature which increases the computational overheads.

Maryam et.al [10] suggested some of the ways to improve the energy efficiency of IoT devices in its environment. They proposed a decentralized hierarchical clustering algorithm for energy aware wsn. They focused on hardware specifications of the smart devices and the comparative analysis of different commercially used IoT hardware devices was done with parameters such as size, cost, and energy consumption.

Pavithra et.al [11] proposed a cluster based algorithm using HACOPSO. This improves the performance of the network but it increases the computational overhead when the mobiles are in different cluster.

The main objective of this work is to classify the possible attacks in the IoT, then layer wise security analysis is done and the proposed solution is constructed for DDoS attacks. Among all the attacks in the IoT environment, DDoS attack is considered as the catastrophic attack. There are various types of DDoS attack all perform jamming of the network. Here we consider reply blocking attack and solution to this attack is proposed with the new TBC (Threshold Based Countermeasure) technique.

Table 1. Layer wise attacks and security guidelines

Layers	Possible Attacks	Security guidelines	Layers	Possible Attacks
L1	The two important attacks are jamming and eavesdropping.	This can be prevented by applying strong encryption techniques and hence confidentiality is preserved.	L1	The two important attacks are jamming and eavesdropping.
L2	Flooding the energy resources, denial of sleep are major attacks at L2.	The encrypted tunnel has to be established for the communication over the network so that channels can be authenticated.	L2	Flooding the energy resources, denial of sleep are major attacks at L2.
L3	Routing attacks, Sybil, DOS, DDOS attacks can occur at L3	Apply encryption algorithm for all the connected devices during communication.	L3	Routing attacks, Sybil, DOS, DDOS attacks can occur at L3
L4	Traffic analysis, message modification, and falsification of the packet.	IDS can be implemented to detect this kind of attack so that it alerts the system when data comes from unknown sources.	L4	Traffic analysis, message modification, and falsification of the packet.
L5	The exploitation of Message integrity, non-repudiation, confidentiality.	S/MIME, SRTP can be used for security at the application level.	L5	The exploitation of Message integrity, non-repudiation, confidentiality.

Layer Wise Security Model

Layered Model

Security for IoT is crucial that can be applied at various levels of internet security protocols. By using the 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 acts as an 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, the 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. The 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. Table.1 describes the attacks on each layer and security guidelines are given.

Physical-Layer Security

The two major attacks performed in the physical layer are jamming and eavesdropping. Providing security at the 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 a 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 a proven security system for physical security [4]. The pilot contamination is one of the crucial security issues in the physical layer. 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 wants 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 variations 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].

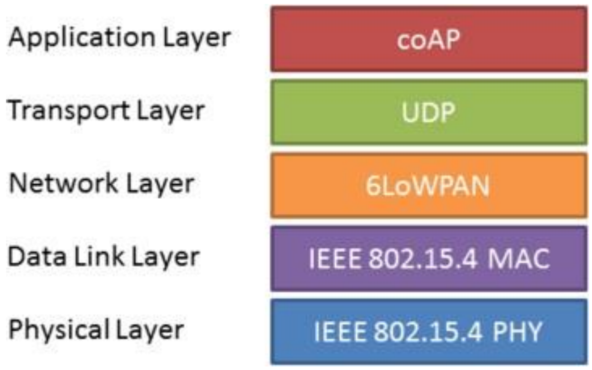

Figure 2. IoT Protocol Stack

Encryption

Network applications often secure their data with encryption due to the high risk of threats while transiting. But encryption is not a solution for all types of assaults in the 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 forms of encryption techniques, key distribution is always a critical issue. Keys that are required to encrypt and decrypt must be delivered to the sender and receiver in a secure path.

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. Since encryption is performed at L1, the message is exposed in all other layers of the sender and receiver. The message which is passed over intermediate hosts is also in clear because routing is performed only at higher layers. Since intermediate hosts cannot be trustworthy, this is suitable only with trustworthy hosts.

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 L5. With end-to-end encryption, messages sent through several hosts are protected. The data content of the message is still encrypted, as shown in Fig3. Therefore, even when the message passes through potentially insecure nodes on the intermediate path between the sender and receiver, the message is protected against disclosure while in transit.

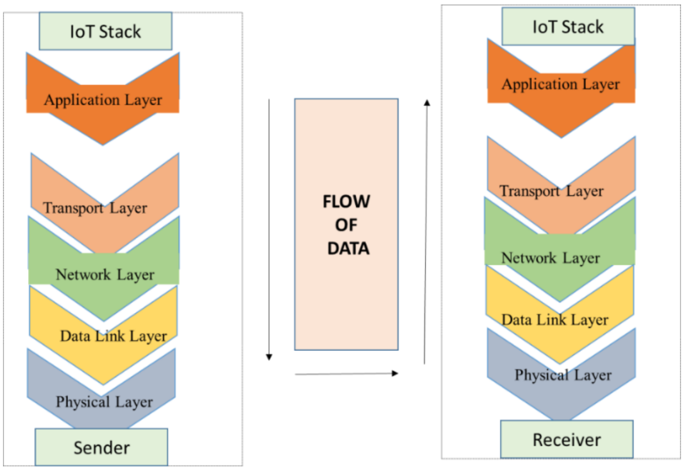

Figure 3. IoT Information Flow

Data Link Layer Security

The security for messages at L2 is more obscure than L1. The role of layer1 is to place the input frames on the medium and ensure the error-free delivery of packets. The security is crucial because it exposes all the MAC addresses of communication devices connected in the network. An example of an L2 threat is Hello flooding attack. Routing protocol retains the connections of the node only if Hello message packets arrive periodically from the concerned node. The attacker uses this packet and sends Hello packet repeatedly in order to flood the path. Several countermeasures are available against Hello flood attack. In the multipath data forwarding technique, the sensor node will maintain different keys. BS will have control over a 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 nodes are 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 a 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, the anti-reply technique must be applied using protocols such as CARP.

Network Layer Security

IoT nodes can exchange data securely using IPSec protocol suite in L3. IPSec is a part of ÌPV6 used for establishing secure communication between host – host or network – network or between gateway and host. IPsec is effectively used to prevent reply attacks. IPSec is further broken into multiple protocols such AH, IKE and ESP.

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.

IKE

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

Phase-1 (key selection)

In phase-1, it creates an encrypted channel between two devices by using an 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.

The major issue that can be occurred in the 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 needs to be implemented with the help IPSec protocols [9].

Transport Layer Security

In current IP infrastructure, the exchange of data can occur securely in the 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 a 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 the 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.

Application Layer Security

The application layer supports end – end encryption in the application level. This will simplify the needs for bottom layers and it reduced the computational overhead introduced for packet size and data processing since encrypted data can be easily implemented in the 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 at the application level. To overcome this issue, S/MIME (Secure Multipurpose Internet Mail Extension) and SRTP (Secure Real-time Transport Protocol) can help provide services such as confidentiality, integrity, authentication, and non-repudiation of the 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 the application level in IoT environment.

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 kinds of attacks can be prevented by using strong authorization and authentication mechanisms. 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 be guaranteed the trust level without the support of higher layers. So end- end security is guaranteed only if the security mechanism is implemented at L5/L3 in addition to PHY layer and MAC layer security.

When we consider communication layers such as a 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 into the number of pieces called fragmentation that leads to higher overhead and delayed transmission. Also, the energy consumption will be higher for the processing of a 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 security when combined, it leads to additional computational cost for setting up a 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.

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 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 are more harmful to the network environment. The several types of activities 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 [20]. In this paper, we have identified many DDoS attacks among which Reply attack is considered as the most important type which damages the network in its existence. The next important thing proposed in this paper is the analysis of different countermeasures on DDoS attack.

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 behaves as a reply jammer if the attack is not successful than the normal node will do its assigned operations.

- The noticeable characteristic of this assault is, it starts executing if another 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 the target node and it uses the channel for sending data.

- The node act as a jammer will find if the channel is available, if so it goes to the 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 decreases the throughput of the network.

Authentication

Authentication is done for each node in the network if the node shares the secret key during communication. To achieve this, each node in the participation performs challenge response system and the node will generate an answer for the random key every time if they want to participate in the network.

If a node S sends REQ to the destination node D, then the node will get REP from the node D in single hop. When the destination node D in multi hop, then node S request is broadcasted with RREQ to the destination node through many numbers of intermediate nodes in the communication. Finally, node D generates RREP and sends it to node S through intermediate nodes. This request – reply mechanism is based on the Bayesian theory of probability.

$$P(SD) = P(S/D) \;\&\&\; P(D) \;||\; P(D/S) \;\&\&\; P(S)$$

According to Bayesian theory the data is denoted by D and the hypothesis is denoted by H. P(H) refers to prior knowledge about the data in advance before it is to be considered. P(H/D) refers to the probability after considering the data.

$$P(H/D) = \frac{P(D/H) \;\&\&\; P(H)}{P(D)}$$

If a node Ni receives RREQ packet, then the density Di of multi hop will be resolved by computing the probability Pi and the node will forward it if the following Pi is obtained otherwise the node will reject the packet thus it prevents the many numbers of retransmissions.

$$Pi = \frac{P(D|Di) \;\&\&\; P(i)}{P(D|D1) \;\&\&\; P(D1) \;||\; P(D|D2) \;\&\&\; P(D2) \;||\; P(D|D3) \;||\ldots\ldots\ldots||\; P(D|Dn) \&\& P(Dn)}$$

Working function of Threshold based countermeasures

If a node Ni wants to send data to the destination node D in single hop or multi hop distance, first node D will authenticate the source node with challenge response system then the destination node B will check the average send of node Ni. This average send is the threshold value Th of source node which is fixed from the BS or CH side based on the data sending rate of node Ni. Figure 5 shows the working mechanism of the proposed countermeasure. The threshold value Th will be stored at each node in the communication and the destination node will check this Th before accepting the packet, if Th> avg.date rate of node Ni then it will reject the packet otherwise the packet it forwarded to Node Ni through intermediate nodes in the communication path.

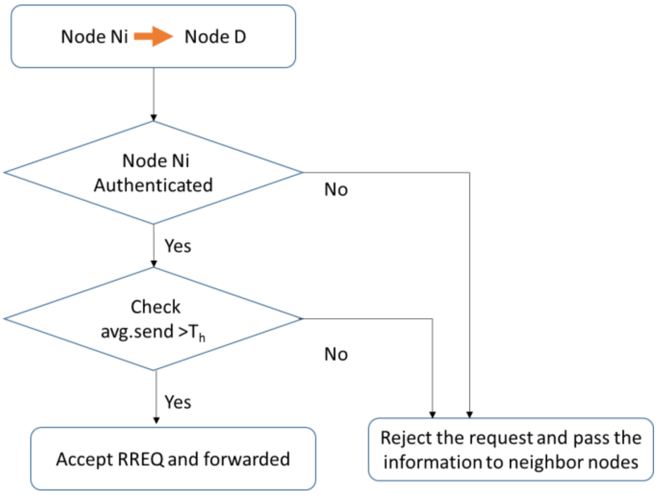
Node Ni
Node D
Node Ni Authenticated
No
Yes
Check avg.send >T_h
No
Yes
Accept RREQ and forwarded
Reject the request and pass the information to neighbor nodes

Figure 4. Flow of TBC

Relevant work Of Countermeasures for Blocking Attacks

The countermeasures for the blocking attacks are primarily categorized as Threat detection, Pre-active Mechanism, Reactive Mechanism, Mobile agent-based technique.

Detection Mechanism: As its name implies, the idea of this mechanism is to identify the blocking assaults during its execution. The strategies of this type of mechanism don't work with jamming itself; this technique can remarkably increase the security only if it is combined with other preventive measures by supplying valuable data.

Pre-active mechanism: The important part of pre-active countermeasures is to form the IoT resistance to DOS attacks rather than reacting after such occurrences [4]. Pre-active countermeasures are categorized in software: detection algorithms or encrypted transmission and sw/hw countermeasures.

Reply mechanism: The significant feature of reply countermeasures is the reactiveness nature when the time DOS is executed, IoT node sense the misbehavior. Reply countermeasures can be done with software or software and hardware collaboratively.

Mobile-agent based technique: The role of this type is that it uses MAs to improve the performance of IoT devices. Here Mobile Agent is nothing but an independent software product that has the capability to jump from one node to another and behave like proxy for the completion of an assigned task.

Proposed Countermeasure on Reply Blocking Attack

The work done here introduces the threshold based blocking countermeasure (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 a reply blocking attack. TBC saves the network by storing threshold values in each node in the environment. The algorithm can accomplish it by having the sending threshold which tells the maximum data that a node can transfer. The TBC algorithm is divided into two phases.

Phase -1

The first phase in TBC is deciding the sending threshold value for all the nodes. This value is fixed from the base station (BS) side. The Base Station will count how many times the data sent from each node and it is recorded in a separate table in the network. Each node in a network will send the data towards the BS after regular a time gap, this will happen based on the number of data a node obtained from a specific node per second regular situation; Base Station will decide the threshold value for each node. BS will maintain the average value for the number of time data arrived from each node as a sending threshold value.

Phase -2

In Phase-2, the algorithm will check upon sending threshold value. All the nodes in Phase-2 will keep three states ordinary state, suspicious state and attack state. In the ordinary state, the node don’t do anything i.e., the attacks will not be performed, In the suspicious state, the nodes might be turned harmful and in the third state the nodes are completely turned as attacking node and it starts destroying the environment. In beginning all nodes in the network will be in the ordinary state. They will transfer their data to Base Station in a single hop or in a multiple hop manner. The Base Station will change the node’s state to suspicious state if more data is arriving from one of the sources larger than the assigned threshold value. Route analysis is done by the algorithm for the node which is in the suspicious state; detecting the source of the suspicious source is quite simple with the help of single hop-route analysis if the origin is direct one-hop from Base Station. Perhaps if the analysis finds that it is multiple hop distance from Base Station during route analysis, the program can verify every node individually in the route for the number of packets sent per second. The node is said to be a blocking node when the number of generated packets by a node is larger than the average transmission and the algorithm will mark the node status as a blocking state. If the node is identified as a blocking node then the jammer node identified is removed from the route after the route is changed through the blocking node, this information is transferred to other nodes in the network so that all the neighbor nodes will come to know the presence of jammer node.

Simulation and Result Details

The different conditions for the simulation done are

- IoT environment with reply blocking attack
- IoT environment with reply blocking attack and TBC Algorithm

Table 2 shows the simulation parameters and the points given below are considered in the simulation:

- To measure the effectiveness of the attack and the effectiveness of its countermeasures, 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, 16, 25, and 30. In this work, we consider traffic interval 1 for fast traffic. To examine the impact of the attack and its countermeasures we have increased the malicious elements in the environment.

Table 2. Network simulation parameters

Parameters	**Value**
Area	100 X 100m
Network Interface type	IEEE802.15.4
Number of nodes	100
BS position	(50,250)
Initial energy(j)	0.5
Sensing range(m)	30
Packet size(bits)	1024
MAC	IEEE802.15.4
Threshold distance (m)	87
Energy receive	40nJ
Energy transmit	40nJ
Routing protocol	Energy aware
Traffic	CBR

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

Fig.5 and Fig.6 shows the average energy consumption and time delay by varying the number of malicious nodes in the environment. Fig.7 shows the average energy by varying the traffic interval. The results shows that the performance of the attack has been significantly reduced after applying the proposed TBC mechanism in the environment.

In the final part, the simulation is done with the inclusion of random mobility to each node in the environment. Here we consider random traffic interval within 1 to 10 in a random fashion.

The result gives that the TBC mechanism enhances energy utilization, time-delay, and throughput better under reply blocking the attack. TBC detects the blocking attack after examining the network and it decreases the impact of blocking the attack by isolating the blocking node from the environment.

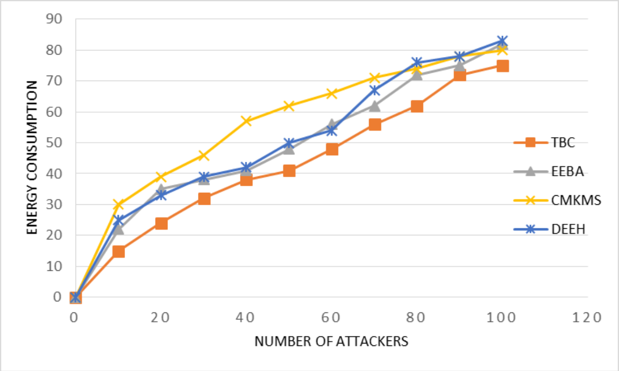

Figure 5. Avg. energy consumption by varying number of malicious nodes

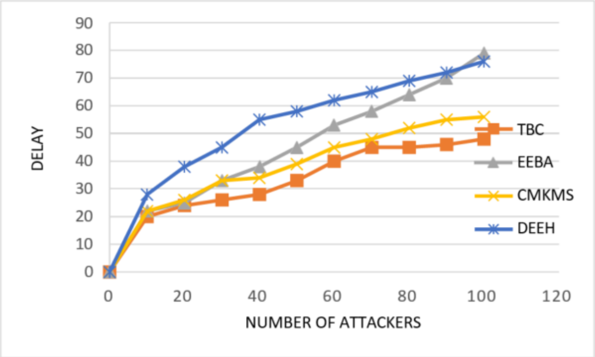

Figure 6. Avg. delay by varying number of malicious nodes

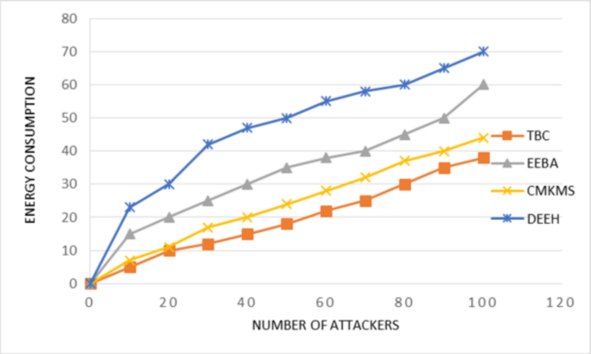

Figure 7. Avg. energy consumption by varying traffic interval

Conclusion

In this paper, the security requirements of IoT are explored by layer-wise security model. The data security and user privacy have been identified as 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 from 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 practical conditions where every node in the environment isn't transmitting at the same time yet nodes are transmitting at various time cases. The outcomes with various conditions demonstrate that TBC is a great choice for the reply blocking attack. The results from the simulated environment by considering mobility demonstrates TBC is adaptable when shifting the location of the 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.

References

[1] Hezam Akram Abdul-Ghani and Dimitri Konstantas, A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective , Journal of sensor and actuator networks., April 2019,8(2):38. https://doi.org/10.3390/jsan8020022

[2] Jithin R,Priya Chandran, Secure Dynamic Memory Management Architecture for Virtualization Technologies in IoT Devices, future internet, mdpi,Vol.10, Nov.2018, 119-225. https://doi.org/10.3390/fi10120119

[3] Simone Cirani, Gianluigi, Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview, algorithms, mdpi, April 2013,197-226. https://doi.org/10.3390/a6020197

[4] Dzevdan Kapetanovic, Gan Zheng, Fredrik Rusek, Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks, IEEE Communications Magazine, Volume: 53 Issue: 6, June 2015, 21- 27.
https://doi.org/10.1109/MCOM.2015.7120012

[5] M. Daniel, "Hidden Dangers of Internet of Things", Women in Security, pp. 69-75, 2017.
https://doi.org/10.1007/978-3-319-57795-1_7

[6] A. Al-Gburi, A. Al-Hasnawi and L. Lilien, "Differentiating Security from Privacy in Internet of Things: A Survey of Selected Threats and Controls", Computer and Network Security Essentials, pp. 153-172, 2017.
https://doi.org/10.1007/978-3-319-58424-9_9

[7] B. Payne and T. Abegaz, "Securing the Internet of Things: Best Practices for Deploying IoT Devices", Computer and Network Security Essentials, pp.493-506, 2017. https://doi.org/10.1007/978-3-319-58424-9_28

[8] Shruti Jaiswal and D. Gupta, "Security Requirements for Internet of Things (IoT)", Advances in Intelligent Systems and Computing, pp. 419-427, 2017.
https://doi.org/10.1007/978-981-10-2750-5_44

[9] M.Shainika, Mrs.C.Hema "Cluster Based Mobile Key Management Scheme to Improve Scalability and Mobility in Wireless Sensor Networks", National Conference on Research Advance in communication, computation, electrical science and structure, ISSN- 2348-8387, Nov 2015

[10] Maryam Sabet, Hamid RezaNaj "A decentralized energy efficient hierarchical cluster-based routing algorithm for wireless sensor networks", Volume 69, Issue 5, May 2015, pp. 790-799.
https://doi.org/10.1016/j.aeue.2015.01.002

[11] Pavithra G.S., Babu N.V, "Energy Efficient Hierarchical Clustering using HACOPSO in Wireless Sensor Networks", International Journal of Innovative Technology and Exploring Engineering, Vol-8 Issue-12, October, 2019.
https://doi.org/10.35940/ijitee.L2789.1081219

[12] Rafael F. Schaefer, Gayan Amarasuriya, H. Vincent Poor , Physical layer security in massive MIMO systems, Asilomar Conference on Signals, Systems, and Computers, April 2018. https://doi.org/10.1109/ACSSC.2017.8335124

[13] Dimitriya, Ziatka, Georgi, Vladimir ,Shifted 2-N-PSK Method for the Detection of Pilot Contamination Attacks, wireless personal communications, April 2019,1-26 .

[14] Muhammad Asim Khan, Mansoor Khan, A Review on Security attacks and solutionin Wireless Sensor Networks, American Journal of Computer Science and Information Technology, Vol.7 Feb 2019, 1-31 .

[15] Mac, F.; St, F.; Quisquater, J. ASIC Implementations of the Block Cipher SEA for Constrained Applications. Available online:
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.88.926

[16] Pecorella, T., Brilli, L., & Mucchi, L. . The role of physical layer security in IoT: A novel perspective. Information,January 2016 7(49), 1-17.
https://doi.org/10.3390/info7030049

[17] Feroz Khan, A.B. & Anandharaj, G. "A cognitive key management technique for energy efficiency and scalability in securing the sensor nodes in the IoT environment: CKMT", SN Appl. Sci. (2019) 1(12):1575.
https://doi.org/10.1007/s42452-019-1628-4

[18] Tariq Aziz Rao, Ehsan-ul-Haq, Security Challenges Facing IoT Layers and its Protective Measures, International Journal of Computer Applications (0975 - 8887) Volume 179 - No.27, March 2018.
https://doi.org/10.5120/ijca2018916607

[19] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, K. Wehrle, "Security challenges in the ip- based internet of things", Wireless Personal Communications, vol. 61, no. 3, pp. 527-542, 2011.
https://doi.org/10.1007/s11277-011-0385-5

[20] Mohsen Nia, A.; Jha, N.K. A Comprehensive Study of Security of Internet-of-Things. IEEE Trans. Emerg.Top. Comput. 2017, 5, 586-602.
https://doi.org/10.1109/TETC.2016.2606384

[21] Guzman, A. IoT Penetration Testing Cookbook; Packt Publishing: Birmingham, UK, 2017.

[22] UL LLC. List of IOT Security Top 20 Design Principles; White Paper; UL LLC: Northbrook, IL, USA, 2017.

[23] Emil Bjohnson, PILOT CONTAMINATION IN A NUTSHELL, www.ma-mimo.ellintech.se/, January 2017.

[24] Eastlake, D.E.; Jones, P.E. US Secure Hash Algorithm 1 (SHA1). Available online: http://www.ietf.org/rfc/rfc3174.txt

[25] Shital Patil, Sangita Chaudhari, DoS Attack Prevention Technique in Wireless Sensor Networks, ScienceDirect, 7th International Conference on Communication, Computing and Virtualization 2016. https://doi.org/10.1016/j.procs.2016.03.094

[26] Q. Zhou, J. Zhang, "Research prospect of Internet of Things geography", Proceedings of the 19th International Conference on Geoinformatics, pp. 1-5, 2011. https://doi.org/10.1109/GeoInformatics.2011.5981045

[27] M. Panda, "Security threats at each layer of wireless sensor networks", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, pp. 50-56, 2013.

[28] Puthal D., Ranjan R., Nepal S., Chen J. (2018) IoT and Big Data: An Architecture with Data Flow and Security Issues. In: Longo A. et al. (eds) Cloud Infrastructures, Services, and IoT Systems for Smart Cities. IISSC 2017, CN4IoT 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 189. https://doi.org/10.1007/978-3-319-67636-4_25

[29] Tommaso Pecorella, Luca Brilli , Lorenzo Mucchi, The Role of Physical Layer Security in IoT: A Novel Perspective, Information No.3, Vol.7, August2016, 7(3). https://doi.org/10.3390/info7030049

[30] Nick Ismail, The future of the 'Internet of Things' security issues, www.information-age.com, December 2017.

Publisher: Chinese Institute of Automation Engineers (CIAE)

ISSN: 2223-9766 (Online)