Received: July 23, 2020. Revised: October 4, 2020.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Securing an Internet of Things from Distributed Denial of Service and Mirai Botnet Attacks Using a Novel Hybrid Detection and Mitigation Mechanism

M. Ganesh Karthik[1]* **M. B. Mukesh Krishnan[2]**

[1]*Computer Science and Engineering, SRMIST, Chennai, India*
[2]*Information Technology, SRMIST, Chennai, India*
* Corresponding author's Email: ganeshkarthik16@gmail.com

Abstract: Internet of Things (IoT) has become more familiar in all applications and industrial fields such as medical, military, transportation, etc. It has some limitations because of the attack model in the transmission or communication channel. Moreover, one of the deadliest attacks is known as a Distributed Denial of Service Attack (DDoS). The Presence of DDoS in network layer cause huge damage in data transmission channel that ends in data loss or collapse. To address this issue the current research focused on an innovative detection and mitigation of Mirai and DDoS attack in IoT environment. Initially, number of IoT devices is arranged with the help of a novel Hybrid Strawberry and African Buffalo Optimization (HSBABO). Consequently, the types of DDoS attacks are launched in the developed IoT network. Moreover, the presence of strawberry and African Buffalo fitness is utilized to detect and specify the attack types. Subsequently a novel MCELIECE encryption with Cloud Shield scheme is developed to prevent the low and high rate DDoS attack in the Internet of Things. Finally, the proposed model attained 94% of attack detection accuracy, 3% of false negative rate and 5.5% of false positive rate.

Keywords: Denial of service attacks, Mirai botnet, Shield mechanism, Encryption mechanism.

1. Introduction

The IoTdevices are engaged with embedded sensors [1, 2] which are used to collect data or information [3]. In addition, the IoT has the capability to deliver multi solutions that radically enhance energy efficiency [4], health, security, education and other several aspects of daily routine. However, providing security in the transmission channel [5] is a critical task because of attack vulnerabilities [6]. In addition, IoT devices can easily affect by Mirai botnet and DDoS attacks [7], both attacks are harmful than any other attack [8]. Moreover, the presence of DDoS attacks in the network layer can affect the data link layer [9] also is has the capability to close all the web page which is in the current process [18]. Attackers who launch the bots to corrupt or damage the system are called Mirai botnet [10], it acts like a robot and takes control of the whole system [11]. The flow of distributed denial of service attack model is elaborated in Fig. 1.

Based on the modern advantages [12] some researchers have developed some innovative techniques [13] but, it has some limitation due to the lack of security. Thus, the efficient detection and mitigation strategy can enhance the performance of the IoT process also increase the huge demand towards IoT technology [14]. So the efficient hybrid optimization based attack detection and encryption with cloud shield scheme is proposed to end this security issues and to enhance the data transformation. Here the fitness model of hybrid optimization is utilized to detect the different types of DDoS attack. Also, the less efficient attack is prevented by encryption model and highly efficient attack is prevented by cloud shield process function. Thus, the main advantage of the proposed model in comparing with existing works are, the developed model attained high attack detection accuracy and mitigation of highly efficient attack like mirai botnet with high rate. The organization of the paper is as follows: Section 2 defines the recent works related to detection and

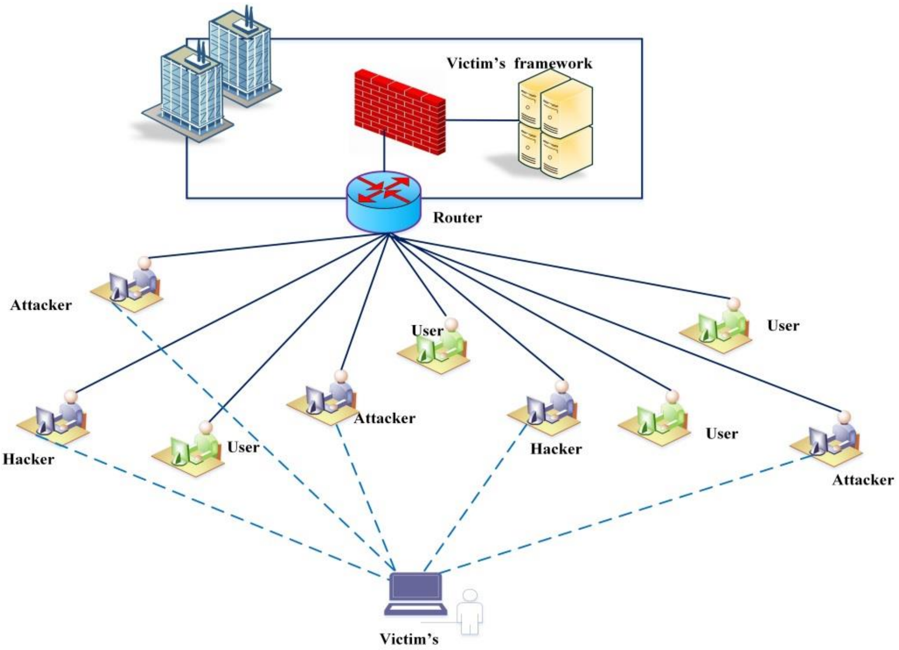


Figure. 1 DDoS attack flow model

mitigation of DDoS attacks; Section 3 explains the DDoS attack model in detail; Section 4 explains the proposed methodology, Section 5 demonstrates outcome and comparison of this research and Section 6 concludes the paper.

2. Related works

Some of the recent literatures related to secure the IoT device against DDoS attack are summarized below:

The investigation of all nodes during information transmission is one of the important things. So Hongsong Chen et al [15] proposed the detection and mitigation approach also Hilbert transforms as a trust mechanism to detect low rate DoS attacks.However, the trust mechanism Hilbert transform is complex to design in IoT environment.

Qiao Yan et al [16] created distributed way DoS mitigation framework model to protect the IoT transmission channel against unauthenticated users. This developed model proved efficient by securing the IoT device from malicious activities.But with the presence of mirai botnet attack it has achieved less accuracy of detection.

IoT gadgets are vulnerable to attacks because of their wireless infrastructure, thus providing security measures against harmful activities are the most important criteria. So, Da Yin et al [17] proposed an attack mitigation module with a switch port scheme. Thus, the presence of switch port in SDN is to monitor all nodes and predict attack nodes in network layer. Moreover, the developed scheme prevented data flooding and data loss problems.But it could not prevent the hacking attacks.

IoT devices are easy to use and applicable for all applications. However, protecting the data from malicious source became a serious threat. For this reason, YairMeidanet al [19] proposed an anomaly detection mechanism for IoT frame work to secure the IoT device against unauthenticated activities. Hence, the outcome of the proposed strategy proved the efficiency by detecting the harmful attack like Mirai, DDoS, etc.If the anomaly is act like trust node then it could not detect that attack.

Y. Yılmaz, and S. Uludag [20] proposed Mitigation via Detection Isolation and Localization (MIAMI-DIL) system frame work to detect the attack in IoT environment based on transmission time series. Moreover, the scalability of the developed model is estimated using proof concept. However, it doesn't have any prevention module to prevent the attack.

The key contribution of this research is summarized below:

- Initially design number of IoT device with the use of EDQP protocol, the purpose of EDQP protocol is to transfer the data.
- Launch the types of DDoS attacks in the developednetwork channel.
- Develop a attack detection model as hybrid Strawberry ABO optimization algorithm.
- Specify high and low rate attack.
- Consequently develop a novel MCELIECE Encryption mechanism with cloud scrubber

shield scheme to prevent thelow and high rate attack in the network channel.
- The effectiveness of the proposed model is compared with recent existing research works.

3. Distributed denial of service attacks and mirai botnet

In IoT vulnerabilities, one of the popular attacks is caused by the Distributed Denial of Service (DDoS). Mirai is proficient to launch different types of DDoS attacks, such as UDP flooding [2], SYN-flooding [2], query-flooding, ACK-flooding, GRE-flooding, pseudo-random label attacks, HTTP POST attacks, HTTP GET attacks, Network Type Protocol (NTP) attack, ICMP flood attack [2], slowloris attack and HTTP HEAD attacks. Thus, the specific types of DDoS attacks are defined below.

3.1 UDP flood attack

The User Datagram Protocol (UDP) flood attack is not a narrow forward attack. Moreover, this attack can send several UDP message bundles to a random layer. Furthermore, it tends to block the communication between the server and the user, thus the message sent by server does not reach authenticated clients. The process is defined in algorithm1.

Algorithm 1 UDP Flood Attack

```
$H$ is network size
$G$ is the IoT sensor nodes
int $D$
// UDP attack parameter
if ($D = NA$)
// here, N is the network location and $A$ is attack
then
$A$=$ACK$
$Target$=$UDP$
select the target node
$IP \rightarrow Spoofing$
else
Spoof the IP address of the target system
//performing attack by spoofing the Ip address
end if
```

3.2 Slowloris attack

These types of attacks can target the web server. It is explained by following steps,

- The multi connections should be opened by the attackers or hackers.
- The victim opens a thread for each and every incoming request; furthermore, it becomes more proficient that the connection takes more time, thus the server will timeout in this situation.
- To control the target from timing out the associations, the attacker sporadically sends limited appeal headers to keep the request lively, the process is defined in algorithm2.

Algorithm 2 Slowloris Attack

```
$H$ is network size
$G$ is the IoT sensor nodes
*int d**
*//slowloris attack parameter*
*check>> connection*
*if(U=y)*
*//$U$ is the affected server and $y$ is the partial connection*
*then*
*server→connection*
*packet=hack*
*else*
wait for connection
//performing attack by link failure
end if
```

3.3 NTP attack

NTP attack is an amplification attack. It reflects based on volumetric DDoS attack. Also, it affects the network layer or server link. Moreover, it can accept many requests at a time and causes traffic in network architecture. Further, the malicious user can be able to gain more information from small questions. The process is defined in algorithm3.

Algorithm 3 NTP Attack

```
$H$ is network size
$G$ is the IoT sensor nodes
int $t$
*//NTP attack parameter*
*t=Ct*
*// Ct is the system time. It captures the system time*
*if (X=port number)*
then *hack the port number*
else
*packet→back up*
//performing attack hacking the port number
end if
```

3.4 HTTP flood attack

HTTP flooding attack allows unwanted request to attack the application layer or web server. Also, it frequently utilized interconnected computers to take aid in their control. Moreover, this attack is hard to detect because it doesn’t rely on malware packets. In order to attack the application layer or web server it uses HTTP GET and POST request. The GET appeal is utilized to reclaim the static content like pictures. Typically, it induces low load on the web server for each request. POST request investigates present items in database and accepts all requests. Also, it typically imposes heavy load in server link.

Algorithm 4 HTTP flood attack

```
$H$ is network size
$G$ is the IoT sensor nodes
int $b, I$
// b is control system and I is server
Get request>>web server
//it tries to attack the web server
Post request>> Target server
if ($b \to I$)
then malicious server
//HTTP flood attack
else
Data traffic>>Target server
end if
```

3.5 Internet control message protocol (ICMP) flood attack

ICMP request needs several server sources for request and response also required bandwidth for incoming message and outgoing echo-reply. This attack overwhelms the particular device that has the capability to react quantity of requests and excess of correlation network devices through bogus traffic.

Algorithm 5 ICMP flood attack

```
$H$ is network size
$G$ is the IoT sensor nodes
int $E, I$
// E is error and I is server
send request>>host
//the host is un available
Post request>> traffic packets
if($E \to I$)
then
ICMP sends bulk of error queries to load the server
else
$E$-$Sp$
//Sp is the source Ip
$E$=discard packet
end if
```

3.6 SYN flood attack

SYN flood is the half-open attack and the category of DDoS attack. The attacker transfers number of repeated SYN packets frequently to each port on the targeted server with the usage of fake IP address. The attacker is capable to consume obtainable ports on a particular server machine when the SYN packets of the primary connection requests are sending continuously.

Algorithm 6 SYN Flood Attack

```
$H$ is network size
$G$ is the IoT sensor nodes
int $R$
// SYN attack parameter
if ($R$=$SR$)
// here, S is the server, it sends the request to the target node to make it as unresponsive
then F sends multiple ACK to another server
//F is the server
else
packet→Spoofing
//performing attack by spoofing the packet
end if
```

3.7 Mirai botnet attack

Mirai is the self-propagated botnet virus. It has efficiency to infect unsecured IoT devices and that are combined for DDoS attack which is against the particular victim. The poorly protected devices can easily be affected by the attackers. Also, the Mirai is divided into two main components, first one is a virus and another one is the Command control Center (CnC).

Algorithm 7 Mirai Botnet Attack

```
Start
int $n, S, D$ //P-plain text, S-source, D-destination
n= packets        // number of packets
$n \to S$
S>>D        // packets are transmitting source to destination
Initialize all the connected IoT systems
int bot ()
{
```

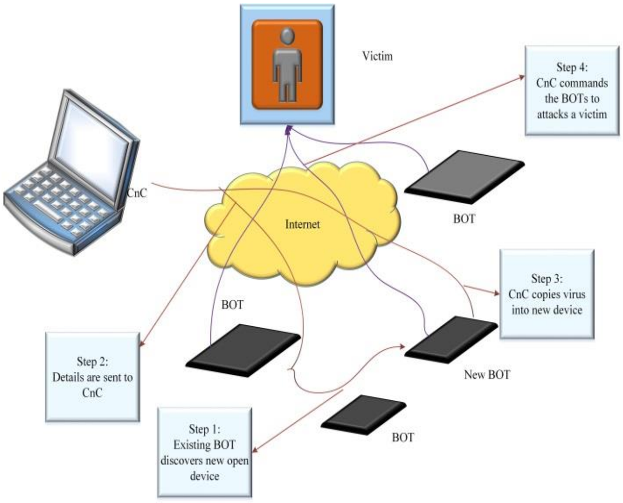

Victim
Step 4:
CnC commands the BOTs to attacks a victim
CnC
Internet
BOT
Step 3:
CnC copies virus into new device
BOT
New BOT
Step 2:
Details are sent to CnC
Step 1:
Existing BOT discovers new open device
BOT

Figure. 2 Mirai system

```
        $check \rightarrow S\text{-}D$
        $target \rightarrow D$
if ($i \leq j$)
//monitor all the connected devices
{
Control ($i \leq j$) //control all the devices by bot
$hack >> info$
$bits \geq M$          //assumption
$Check\ data\ statistics \rightarrow corrupt\ whole\ system$
}
then
return True
enter the bot into channel of IoT device
}
else
return False
end if
```

The scanning progression should be run endlessly on every bot using telnet protocol in Fig. 2.

3.8 Low and high rate attacks

The attack which is able to predict in router border also is able to prevent by conventional algorithms is termed as low rate attack. The high rate attacks also called as economic dos attacks which are not controlled by conventional algorithms because of its effectiveness. These types of attack are prevented by processing the shielding strategy.

4. Proposed methodology

The aim of this research is to secure the IoT device from DDoS and Mirai botnet attack. Initially develop an IoT device using EDQP protocol by Network simulator. Design an Innovative detection algorithm as Hybrid Strawberry African Buffalo Optimizer (HSABO) to detect the DDoS and Mirai botnet attack. Subsequently, the encryption mechanism McEliece encryption with EDoS-Shield architecture is utilized to prevent high rate DDoS and Mirai botnet attacks. Thus, the high crowed and the malicious program is turned to EDoS-Shield architecture which presents in encryption mechanism.

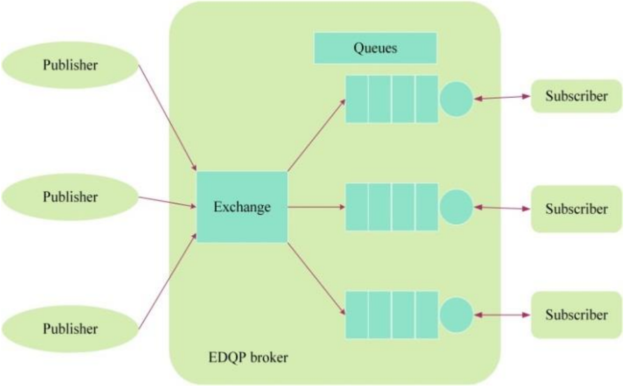


Figure. 3 Enhanced data queuing protocol (EDQP)

Nomenclature	
$K_{run} >> K_{root}$	Attack node
$R_{locat(i)}$	Source and destination
$d(r)$	Distance of node
r, r_1, r_u	Number of IoT nodes
T	Entire nodes in IoT
T^n	n number of nodes
P	Columns
$X_1 and\ x_2$	Learning parameters
$r_{pmax.n}$	Best individual nodes
$R_{gmax.n}$	Node fitness
W_n	Attack node
$\mathrm{m_n}$	Good node
$‘k$	Detection of attack node
H	Encryption code
B	Errors
Z	Contrary element
(H^*,b)	Public key
Z,H,Y	Private key
C*a	Matrix generator
n= 1,2,….N	IoT environment
R	SYN attack parameter
S	Server
D	Destination
H	Network size
X	Port number
Ct	System time

4.1 Enhanced data queuing protocol (EDQP)

The EDQP protocol approach is mainly utilized for server messaging on the board of IoT gadgets. It is capable of moveable and multichannel surroundings that offered for assigned errands and construction of servers in Fig. 3.

Received: July 23, 2020. Revised: October 4, 2020.

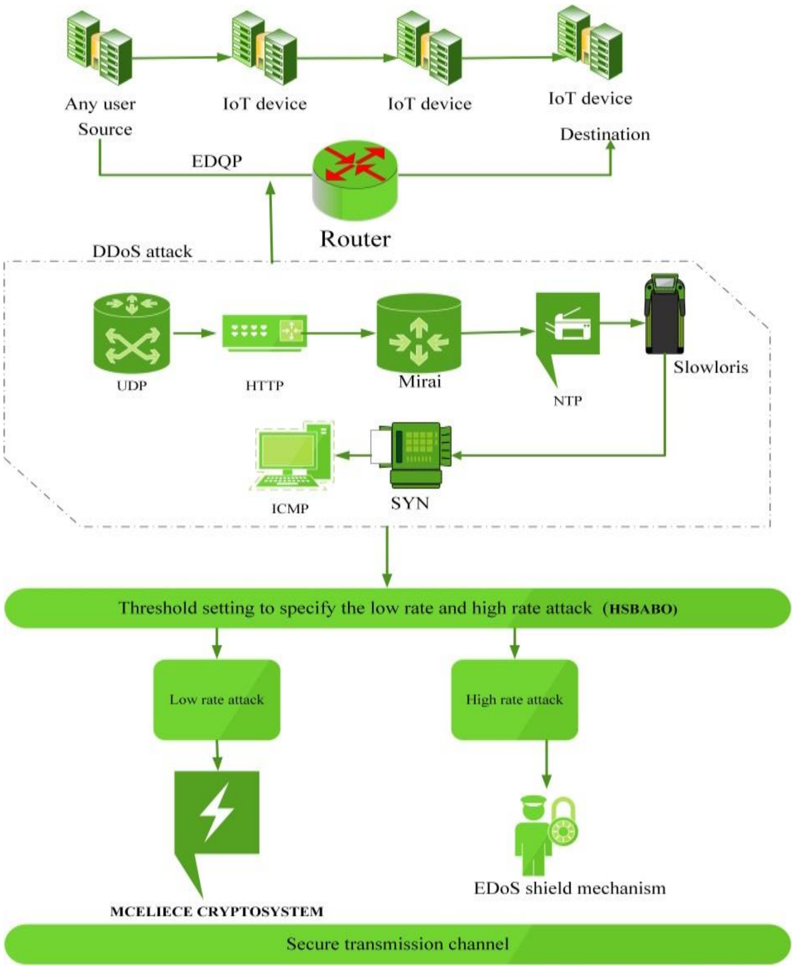


Figure. 4 Proposed flow model

4.2 Hybrid strawberry and african buffalo optimization (HSBABO)

The fineness function of ABO is worked along with Strawberry algorithm; thus, the attack is initialized by strawberry initialization process. Then the different types of attacks are detected using the parameters of ABO algorithm and the efficiency and expired level of attack are evaluated as the best solution in Fig. 4.

Step: 1 To predict the attack node, the distance location of entire node is evaluated using Eq. (1).

$$min\ d(r),\ r_1 \leq r \leq r_u,\ d{:}T^n \rightarrow T \quad (1)$$

Step: 2 Where, $r,\ r_1,\ r_u$ is represent number of presented nodes in IoT environment. In i^{th} iteration the p_{th} source node can be represented as$R_{p(i)} \in T^n$, and$R_{locat(i)}$ denote the matrix value of destination nodes that is calculated by Eq. (2),

$$R_{locat(i)} = [\,R_{root(i)} R_{run(i)}] = [\,R_{(i)}\ R_{(i)}] + [\,K_{(root)} S_1\ K_{(run)} S_2] \quad (2)$$

The investigation of nodes location is processed using Eq. (2).

Step:3 Where, $R(i)=[r_{1(i)} r_{2(i)} \ldots\ldots r_{p(i)}]$, $R_{local(i)}=[r_{1,local(i)} r_{2,local(i)} \ldots\ldots. r_{p,local(i)}]$ and $R_{root(i)}$, $R_{run(i)} \epsilon S^{n.N}$ represents the location of attacked nodes which is solved using Eqs. (3) and (4).

$$R_{root(i)} = [r_{1,\ root(i)} r_{2,\ root(i)} \ldots\ldots. r_{N,root(i)}] \quad (3)$$

$$R_{run(i)} = [r_{1,\ run(i)} r_{2,\ run(i)} \ldots\ldots. r_{N,run(i)}] \quad (4)$$

Step: 4 The distance identification of attacked node can be represented as scalars like $K_{run} >> K_{root}$. For the transmission the network channel requires two nodes that are source and destination which are represented as $R_{local(i)}$ with $2P$ columns and $R_{(i)}$ with $p$columns. They also set the energy value of nodes.

Received: July 23, 2020. Revised: October 4, 2020.

$$fit\left(r_{p,locat}(i)\right) = \begin{cases} \frac{1}{m+d\left(r_{p,locat}(i)\right)} & d\left(r_{p,locat}(i)\right) > 0, p = 1,2 \ldots N \\ m + d\left(r_{p,locat}(i)\right) & d\left(r_{p,locat}(i)\right) \geq 0 \end{cases} \tag{5}$$

Where, the node *d(x)*can be reduced and the value of parameter $m \geq 0$. The value of fitness can be calculated to the option of randomly selected the K^{th} (detection of attacked node).

$$V_p = fracfit\left(r_{p,locat}(i)\right)\sum_{k-1}^{N} fit\left(r_{p,locat}(i)\right) \tag{6}$$

The selected values through the process will be measured as parent plants for next iteration.

The node energy value and attacked node position is trained to the ABO function, the efficiency of the attack is calculated as expired time of an attack, which is elaborated in Eq. (7).

```
1  Objective function (IoT nodes)
                $U^*=(u_1,u_2,....u_n)T$
2  Initiate the attack parameter
//spoofing IP, hacking port number, link failure, discarded packet, spoofing packet, targeting server
3  Minimum life time of node is evaluated using Eq. (7)

   $m_{n+1}=m_n+l_1x_1(r_{gmax.n}-w_n)+l_2x_2(r_{pmax.n}-w_n)$   (7)

Where $m_n$ and $w_n$ represent good nodes and attack nodes within the entire IoT environment $(n=1, 2,...N)$; $l_1$ and $l_2$are the learning factors; $x_1$ and $x_2$ are random numbers between [0, 1];$r_{gmax.n}$is expired time of the attack and $r_{pmax.n}$ denotes the best individual nodes.
4  Update attack parameters from step 2μ about ($r_{gmax.n}$ and $r_{pmax.n}$) using Eq. (8)

                $M_{n+1}=(w_n+m_n)/+0.5$   (8)

//identify low rate or high rate attack using Eq. (8)
// the attack which destroys the link or server is termed as high rate attack
5  Is $r_{gmax.n}$ updating. Yes, go to step 6. No, go to step 2
6  If the stopping criteria aren't met, return to algorithmic rule step 3, else visit step 7
7  Output the best solution. (Attack detection)
```

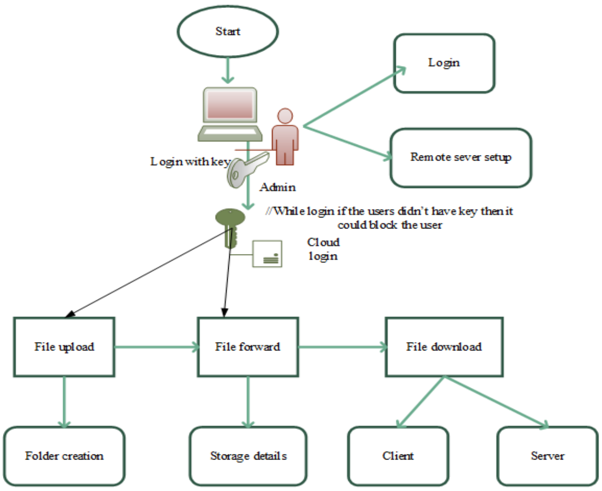


Figure. 5 Mitigation model

4.3 MCELIECE cryptosystem and cloud scrubber shield

The working of this crypto model is initially the server chooses the private code which is randomly generated. Then, the server wants to check all the IoT nodes which are in good manner or not.

4.3.1 Key generation

A binary (a, c) linear code *K* is capable of correcting *b* errors. This code can have a coherent decoding algorithm and develops a $c \times a$ generator matrix *H* for the code *K*. The unarranged $c \times c$ binary dual non-singular matrix *Z*, a random $a \times a$ transformation matrix *Y*. Computes the $b \times a$ matrix $H^*=ZHY$, public key is (H^*, b); private key is (Z, H, Y).

4.3.2 Message encryption

To encrypt a plain text *n*, choose a vector *x* of weight *b* randomly and computes the cipher text *k* as$k=k'+x$, where, $k'=nH^*$.

4.3.3 Message decryption

To decrypt a cipher text *k* calculates $k^*=ky^{-1}$ and $n=n^*Z^{-1}$, note that $k^*=kY^{-1}=nH^*Y^{-1}+xY^{-1}=nZH+xY^{-1}$, and that *Y* is a transformation matrix, thus xY^{-1} has weight *b*. The encryption code *H* can accurate up to *b* errors, and *nZH* is at expanse at most *b* from kY^{-1}. Therefore, the correct code word $n^*=nZ$ is obtained. Then, multiply it with the contrary of *Z* gives $n=n^*Z^{-1}=nZZ^{-1}$ that is the normal text message.

5. Result and discussion

The proposed model is implemented using Network simulator NS2 running on windows 10

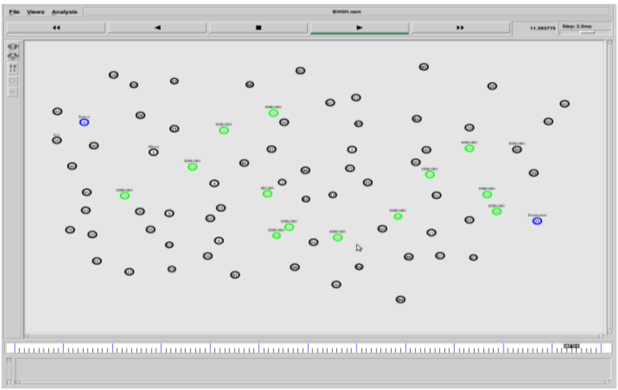
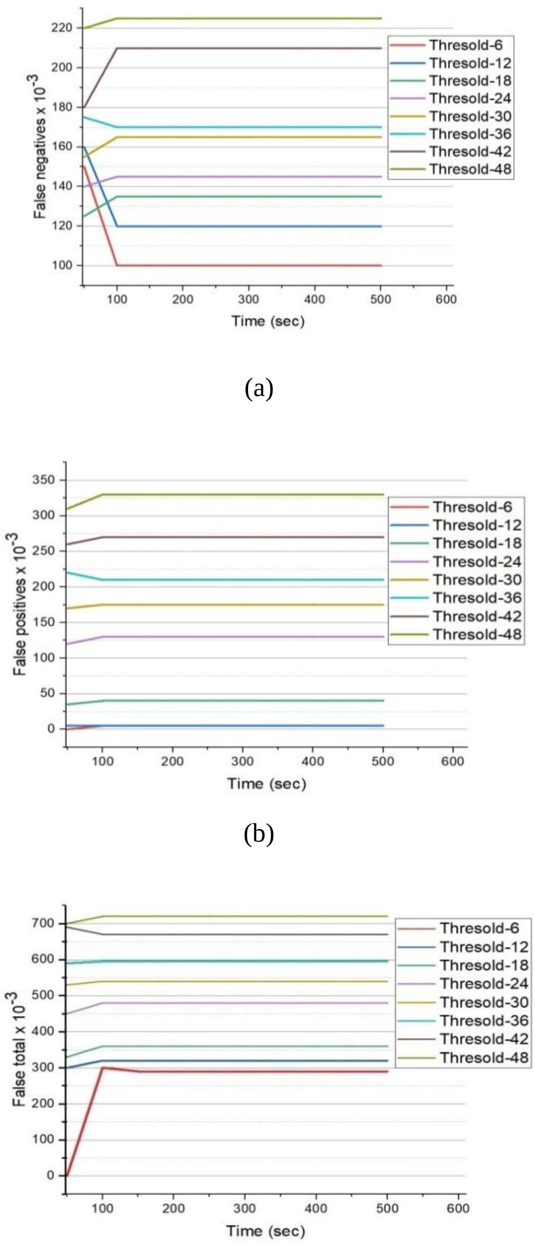


Figure. 6 Node creation in-network, attack node formation and detection of attack



(a)

(b)

(c)

Figure. 7 False total measure: (a) false negatives (b) false positives, and (c) false total

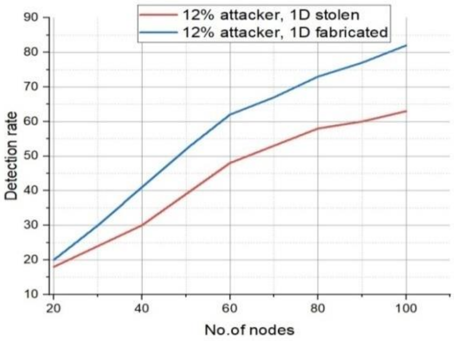


Figure. 8 Detection rate

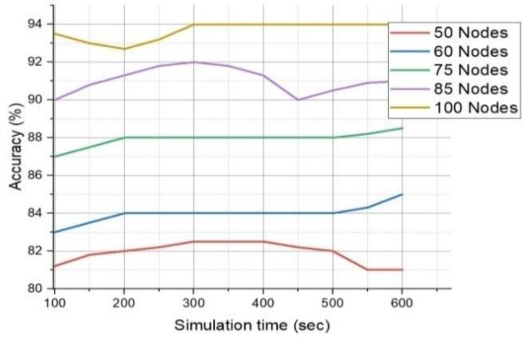


Figure. 9 Accuracy of detection

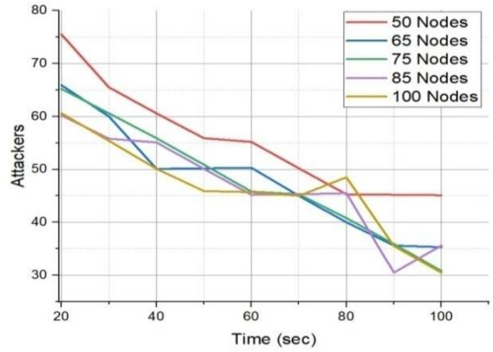


Figure. 10 Number of attackers present in transmission channel: ID stolen attackers

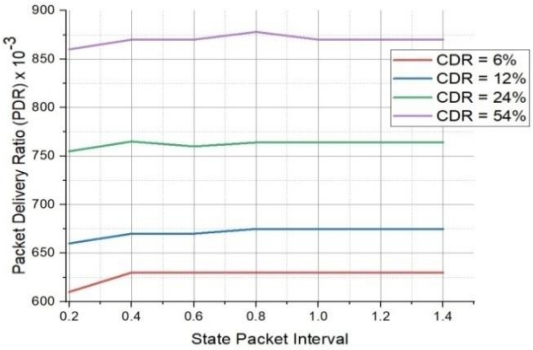


Figure. 11 Packet delivery ratio

Received: July 23, 2020. Revised: October 4, 2020.

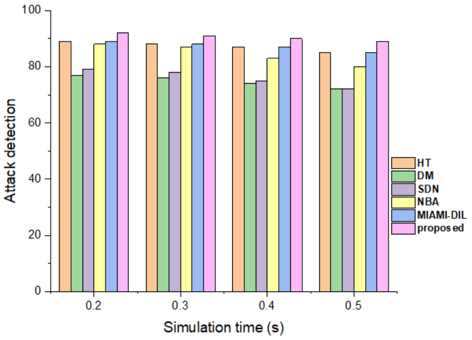


Figure. 12 Detection rate

platform. This research target is to detect and prevent DDoS, Mirai botnet and other harmful and other unknown attacks in IoT device. Thus, for the detection HSBABO optimization mechanism is utilized within the parameters of ABO and SB, the attack is detected. Moreover, the efficiency of attack is calculated using fitness function of the ABO. The node creation in-network is generated based on protocols that are in the current process, thus, the current research focuses on Enhanced Data Queuing Protocol (EDQP) for node creation. Furthermore, the node which is created in the network layer is connected in Fig. 6.

In addition, the false total measure is evaluated under both false positive and negative rate in Fig. 7.

The overall attack detection rate of both ID fabricated and ID stolen is elaborated in Fig. 8.

Detection accuracy of ID stolen and ID fabricated is defined using Fig. 9.

Number of attackers present in transmission channel as ID stolen attackers and ID fabricated attackers. Some attackers are present in network transmission channels to create duplicate key. This kind of attacker is termed as ID fabricated attackers. The attacker who steals the security password is termed as ID stolen attacker in Fig. 10.

The ratio of packet transmission and packet drop rate between different state packet intervals is in fig.11.The efficiency of the proposed model is evaluated using some recent existing work such as Hilbert transform (HT) [15], Distributed Mitigation (DM) [16], Switch SDN [17], Network based false or anomaly detection (NBA) [19] and Mitigation through Detection Isolation and Localization (MIAMI-DIL) [20].

The attack detection ratio is calculated as attack detection rate which is evaluated based on simulation time, also the efficiency of the proposed strategy is validated with the different existing approaches is defined in Fig. 12.

Table 1. Performance Evaluation Table

Methodologies	FPR	FN R	DR	AoD	PDR
NBAD [19]	23	15	77	90	85
HT [15]	22	26	89	89	90
DM [16]	20	23	78	76	83
Switch SDN [17]	17	19	79	78	80
MIAMI-DIL [20]	15	11	89	89	90
HSBABO	5.5	3	92	94	98.6

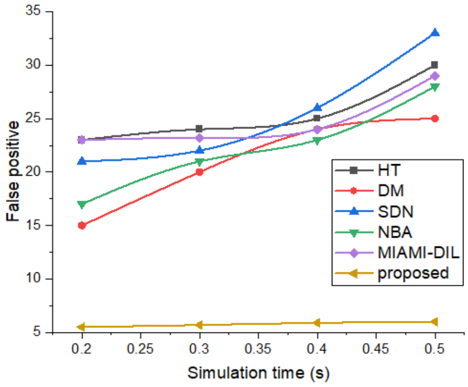


Figure. 13 False positive rate

The developed mechanism can attain a false positive rate as 5.5% with a different interval of simulation time, which is validated with recent approaches shown in Fig. 13. The proposed approach reduces the false negative rate as 3% with the different simulation time that is compared with different techniques and gains the better proficient

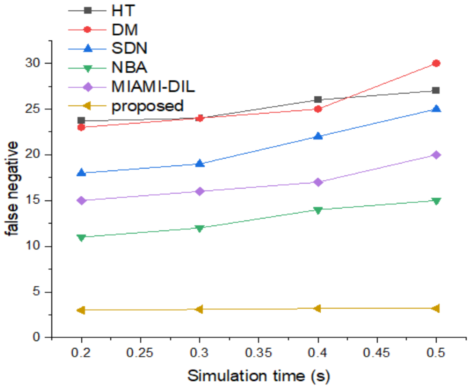


Figure. 14 False negative rate

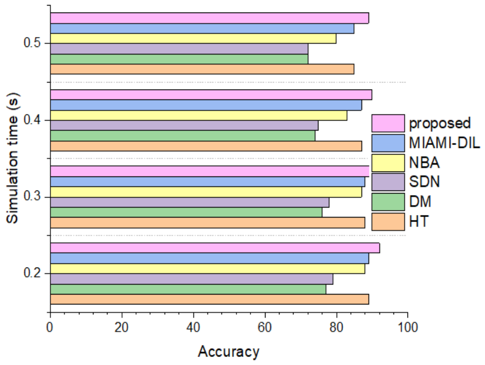


Figure. 15 Accuracy comparison

result is shown in Fig. 14. The success of the detection algorithm is based upon the process functioning rate. Considering this the function of the detection mechanism is proved by the accuracy of detection. Moreover, the comparison result verified the effectiveness of the proposed work in Fig. 15.

6. Conclusion

The Mirai botnet and DDoS attacks in IoT devices are more powerful than any other software because it acts like a robot and it controls the IoT devices. Thus, the hybrid optimization mechanism with the Encryption mechanism and EDoS shield approach is used to detect and prevent such attacks in the Internet of Things. The proposed strategy attains 94% accuracy of detection and also reduced false negative rate as 3% and false positive measure 5.5%. In future, the hybrid machine learning model with hybrid optimization model will enhance the accuracy of attack detection and prevents high economic denial of service attack to obtain high confidential rate.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, methodology, software, validation, writing, original draft preparation, Mr. M. Ganesh Karthik; review and editing, supervision, project administration, Dr. M. B. Mukesh Krishnan.

References

[1] R. Radhika and K. Kulothungan, “Mitigation of Distributed Denial of Service Attacks on the Internet of Things”, *Applied Mathematics*, Vol. 13, No. 5, pp. 831-837, 2019.

[2] H. F. El-Sofany, “A New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks”, *International Journal of Intelligent Engineering and Systems*, Vol. 13, No. 2, pp. 205-215, 2020.

[3] J. Habibi, D. Midi, A. Mudgerikar, and E. Bertino, “Heimdall: Mitigating the internet of insecure things”, *IEEE Internet of Things Journal*, Vol. 4, No. 4, pp. 968-978, 2017.

[4] K. Kaur, S. Kumar, and A. Baliyan, “5G: a new era of wireless communication”, *International Journal of Information Technology*, Vol. 12, No. 2, pp.619-624, 2020.

[5] K. F. Xylogiannopoulos, P. Karampelas, and R. Alhajj, “Detecting DDoS Attacks on Multiple Network Hosts: Advanced Pattern Detection Method for the Identification of Intelligent Botnet Attacks”, *Developments in Information Security and Cybernetic Wars*, IGI Global, pp. 121-139, 2019.

[6] P. Kaur, M. Kumar, and A, Bhandari, “A review of detection approaches for distributed denial of service attacks”, *Systems Science & Control Engineering*, Vol. 5, No. 1, pp. 301-320, 2017.

[7] A. Arıs, S. F. Oktug, and T. Voigt, “Security of internet of things for a reliable internet of services”, *Autonomous Control for a Reliable Internet of Services*, Springer, pp. 337-370, 2018.

[8] M. Schwarz, S. Weiser, D. Gruss, C. Maurice, and S. Mangard, “Malware Guard Extension: abusing Intel SGX to conceal cache attacks”, *Cybersecurity*, Vol. 3, No. 1, p. 2, 2020.

[9] R. Vishwakarma and A. K. Jain, “A survey of DDoS attacking techniques and defence mechanisms in the IoT network”, *Telecommunication Systems*, Vol. 73, No. 1, pp. 3-25, 2020.

[10] D. Acarali and M. Rajarajan, “Botnet-Based Attacks and Defence Mechanisms”, *Versatile Cybersecurity*, Springer, Cham, Vol. 72, pp. 169-199, 2018.

[11] J. C. Mateus, D. Claeys, V. Limère, and J. Cottyn, “A structured methodology for the design of a human-robot collaborative assembly workplace”, *The International Journal of Advanced Manufacturing Technology*, Vol. 102, No. 5-8, pp. 2663-2681, 2019.

[12] K. Sha, T. A. Yang, W. Wei, and S. Davari, “A survey of edge computing-based designs for iot security”, *Digital Communications and Networks*, Vol. 6, No. 2, pp. 195-202, 2020.

[13] R. Gorwa and D. Guilbeault, “Unpacking the social media bot: A typology to guide research and policy”, *Policy & Internet*, Vol. 12, No. 2, pp. 225-248, 2020.

[14] A. Sajid, H. Abbas, and K. Saleem, “Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges”, *IEEE Access*, Vol. 4, pp. 1375-1384, 2016.

[15] H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, “A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation”, *IEEE Access*, Vol. 7, pp. 32853-32866, 2019.

[16] Q. Yan, W. Huang, X. Luo, and Q. Gong, “A multi-level DDoS mitigation framework for the industrial internet of things”, *IEEE*

Communications Magazine, Vol. 56, No. 2, pp. 30-36, 2018.

[17] D. Yin, L. Zhang, and K. Yang, “A DDoS attack detection and mitigation with software-defined Internet of Things framework”, *IEEE Access*, Vol. 6, pp. 24694-24705, 2018.

[18] S. Sicari, A. Rizzardi, D. Miorandi, and A. Coen-Porisini, “REATO: REActing TO Denial of Service attacks in the Internet of Things”, *Computer Networks*, Vol. 137, pp. 37-48, 2018.

[19] Y. Meidan, M. Bohadana, and Y. Mathov, “N-BaIoT—Network-based detection of IoT botnet attacks using deep auto encoders”, *IEEE Pervasive Computing*, Vol. 17, No.3, pp. 12-22, 2018.

[20] Y. Yılmaz and S. Uludag, “Timely detection and mitigation of IoT-based cyberattacks in the smart grid”, *Journal of the Franklin Institute*, https://doi.org/10.1016/j.jfranklin.2019.02.011, ISSN: 0016-0032, 2019.