International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

A New Framework and Defensive Techniques for DDOS Attack on IoT

Feroz Khan A.B, G.Anandharaj

Abstract : The Internet of Things (IoT) comprised of interrelated things such as computing gadgets, wearable devices, handheld devices, digital machines, mechanical devices, people, objects, 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, 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. 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.The real work of this paper is that the conduct of various types of DDOS assaults found in IoT is demonstrated utilizing activity modeling and discovered counteragent against it. DDOS assault is one of the catastrophic assault which hinders the channel by sending a large amount of undesirable data constantly so as to flood a system. The action demonstrating of DDOS assault indicates all around obviously about how it executes on IoT environment and it is additionally helpful in building up the counteragent for security assault.This paper further presents the survey of IoT attacks and the counteragents against those attacks, also the paper introduces the new counteragent for DDOS attack. The new Threshold based Blocking Counteragent (TBC) is proposed in our work for the reply blocking attack. TBC detects the blocking in the network and prevents it from reply blocking attack. The proposed implementation in different realistic conditions perfectly shows that TBC helps IoT against reply blocking attack by varying the network traffic and adding the malicious nodes in a network. The proposed work clearly shows the good performance of the algorithm in various conditions such as mobility among secured nodes and malicious nodes, change of traffic interval.

Index terms: Activity modelling, DDOS attacks, Security assaults Threshold based Blocking Counteragent (TBC).

I. INTRODUCTION

The research in IoT recently introduces the wide range of application domains. The IoT network comprises of the number of interconnected nodes which sense the input and transforms the sensor information to the central base station (BS) [1]. The IoT node depends on larger energy resources so battery power should not be limited. 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 [2, 3], 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 all of these security assaults are modelled using UML for understanding its different behavior when they are executed in the environment. The UML [5] based activity modelling methods is used in modelling the behavior of different DDOS attacks. In UML activity modelling, the behavior of various attacks is modeled by using variable states and the different conditions, exchanging of information between the states. This is considered as the important approach to discover the intelligent behavior of DDOS attack. The UML activity modelling also presents the required solution for minimizing the consequence of attack on IoT. The second important thing proposed in this paper is the analysis of different counteragents on DDOS attack. In this paper, the literature survey clearly indicates that the most of the security solutions on DDOS attack are hardware based and are very expensive to put into effect and modify. The survey suggests that the solution can be software based algorithm and it is more efficient and inexpensive to stop the occurrence of DDOS attack. The security solution for blocking attack developed by the researcher contributed an efficient job for identifying the blocking attack and minimize its effect to improve the performance of IoT by using some defensive techniques [6]. The defensive techniques can be useful to develop the efficient model for securing the Internet of Things (IoT) [7]. The effort for developing defensive techniques will be easier and efficient once we understand the behavior of the attacks completely.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Feroz khan A.B, PG and Research Department of computer science, Adhiparasakthi College of Arts and Science, Vellore, India.
Anandharaj G, PG and Research Department of computer science, Adhiparasakthi College of Arts and Science, Vellore, India.

The final scope of the paper is to obtain the effective defense mechanism for DDOS attack after understanding the activities of different security assaults and various counteragents. The work proposed a new counteragent for reply blocking attack called TBC. The idea of TBC algorithm is that it permit the attack inside the network, then it starts its preventive mechanism after detecting the attacks on IoT. To detect and prevent the attacks, the algorithm uses threshold based security mechanism. Every node in the network consist of some threshold value then the current transmission is periodically compared with the maintained threshold value. If the value cross the maintained threshold, it means that an attack has occurred and after finding this, it implement defensive mechanism. The malicious node which performs blocking is detected first, then this information is passed to all neighboring node the paths arrived from malicious node will be changed. This work also simulates the behavior TBC using Network Simulator-2 environment by considering practical situations. The output of simulation show that TBC performs better in the presence of reply blocking attack. It further proves that the TBC is performed well during the occurrence of reply blocking attack with varied traffic interval and varied malicious nodes in the network. The primary benefit of TBC is that it performed well during attacks with increasing number of malicious nodes in the environment.

II. PROPOSED ACTIVITY MODELLING OF DDOS ATTACK

This part describes the functionality point of a system by representing logical operations. Each logical operation is viewed as a sequence of activities for when and how they are performed. The UML Activity modelling is done for providing functional part of any processes [5, 8]. The activity diagram represent a flow after the completion of an action. This UML model using activity modeling is helpful in understanding the fundamental flow of security attacks. In the next part of this section we describes the activity modelling diagram for 4 kind of DDOS attacks,

- Constant Blocking
- Illusive Blocking
- Random Blocking
- Reply Blocking

A. Constant Blocking Attack

Fig.1 of this paper demonstrates the flow of constant blocking attack using UML activity model. Figure 1 shows the various activities that are performed during the occurrence of attack on IoT. The sequences of behavior are given below:

- The attacker will start the constant blocking attack. The node in the environment acts like a jammer node after the attack is successful, then it start flooding the network by sending malicious packets, if attack not successful then the node do its regular activity.
- The non-malicious node sense the channel and identified some event then it attempt to send the data to destination node. The misbehavior node will check if the channel is idle or not, when it is available then it transform the data over the channel and relay it to the target. If the channel is not accessible then it will check continuously after some particular time gap for the availability of channel.
- The jammer node creates or generates random data for every time gap and it tries to send the data by violating MAC policies i.e.it won't check channel's availability.
- The random data which is sent by the jammer node may crash with the data that are arrived from non-malicious node and it block the entire traffic in the environment by enlarging the collision on it. The effect of this attack can be even more if time-gap between the generations of random data is too less.

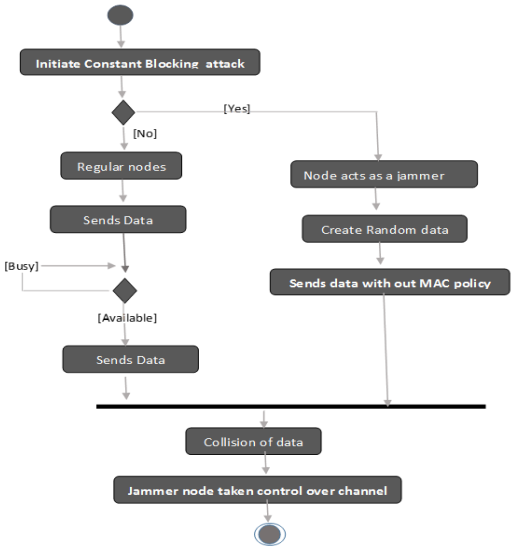

Figure 1: Constant Blocking Attack.

B. Illusive Blocking Attack

Figure 2 demonstrate the series of behaviors in illusive blocking attack. In illusive blocking, the attacker will completely down the channel by making the channel busy. The various activities during the implementation of attack are as follows:

- The attacker outside the network will first perform the illusive blocking attack in a network on any node. If the attack is successfully executed then the non-malicious node will act like a jammer, if the attack is unsuccessful then it act as a normal node.
- The non-malicious node creates the data and send it towards the target after ensuring the channel's availability.
- The node which turned as a jammer repeatedly generates the data packets not following any time gap between two packets. It will make the channel busy for long time.
- The busy state makes other normal node in a network to receiving state. This behavior will increases the consumption of larger energy, delay and total throughput of the network gets decreased.

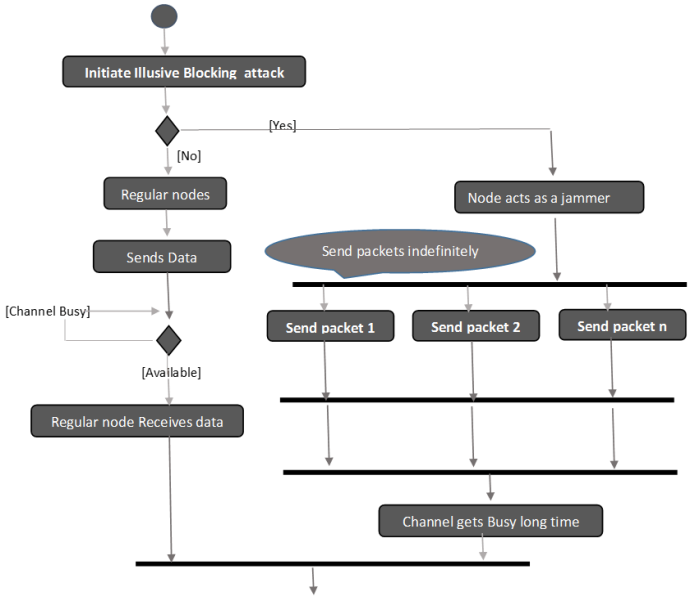

Figure 2: Illusive Blocking Attack.

C. Random Blocking Attack

Fig.3 explains the sequence of behaviors that can be occurred in the occurrence of random blocking attack. This attack is a brainy attack in which the blocking node will try to save its energy. This node run in 2 modes such as blocking mode and sleep mode. The different activities involved in this attack are as given below:

- If the attack happens to be successful, then the attacker outside the network will first start the attack by changing the normal node in the network to blocking node.
- If the channel is free, the non-malicious node finds something to send and it will try to transfer the packet to another node or target. The sender node will always looks for the availability of channel every time when it has something to send.
- The node act like a jammer in a network run in 2 modes for energy saving and keeps its impact for long time. In blocking mode the node will make the channel unavailable either by creating the data continuously like illusive blocking or by generating random data after every time interval by violating MAC policies like constant blocking.
- The jammer node which makes the channel unavailable keeps the non-malicious node in a receiving state for long time.
- The node considered as normal node can change its state to receive state and every time when the jammer node is in sleep state, the channel is available for the normal node. It leads long delay in transferring the data from that node.

D. Reply Blocking 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.

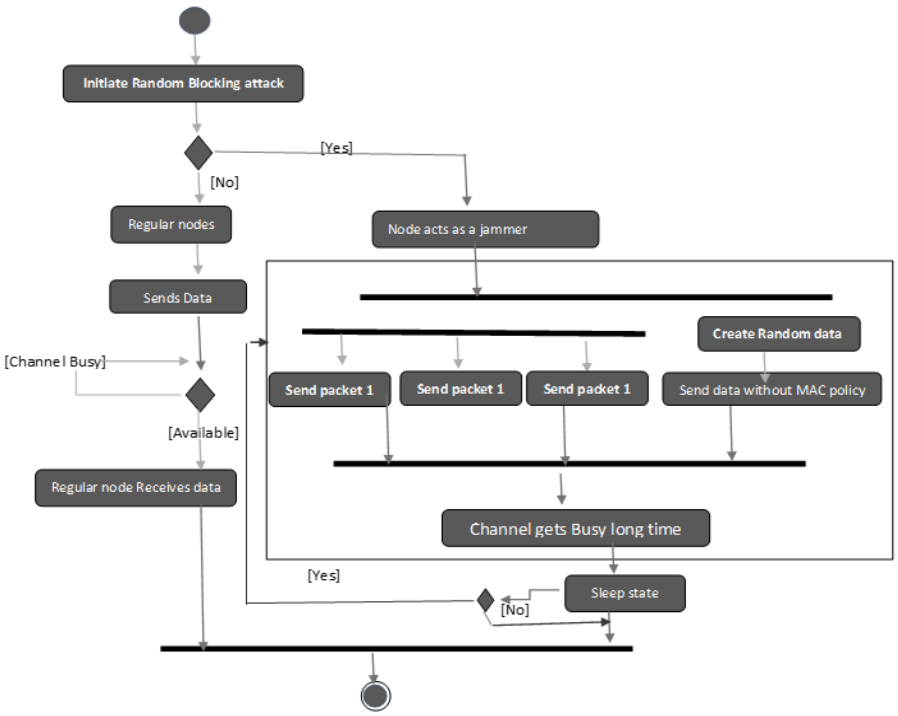

Figure 3: Random Blocking Attack.

III. RELEVANT WORK ON COUNTERAGENTS OF BLOCKING ASSAULTS

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

Reply mechanism: The significant feature of reply counteragents is the reactiveness nature when the time DOS is executed, IoT node sense the misbehavior. Reply counteragents 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.

IV. PROPOSED COUNTERAGENT ON REPLY BLOCKING ATTACK

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 TBC algorithm is divided in two phases.

A. Phase -1

The first phase in TBC is deciding the sending threshold value for all the node. This value is fixed from 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 network will send the data towards the BS after regular time gap, this will happen based on the number of data a node obtained from specific node per second regular situation; Base Station will decide the threshold value for each node. BS will maintain the average value for number of time data arrived from each node as a sending threshold value.

B. Phase -2

In Phase-2, 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 ordinary state, the node don't do anything i.e., attack will not be performed, In suspicious state the nodes might turned harmful and in the third state the nodes are completely turned as attacking node and it starts destroying the environment. In the beginning all nodes in the network will be in 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 arrived from one of the source larger than the assigned threshold value.

Route analysis is done by the algorithm for the node which is in suspicious state; detecting the source of 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 find that it is multiple hop distance from Base Station during route analysis, the program can verify every node individually in the route for number of packet 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 blocking state. If the node is identified as blocking node then the jammer node identified is removed from the route after the route is changed through 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.

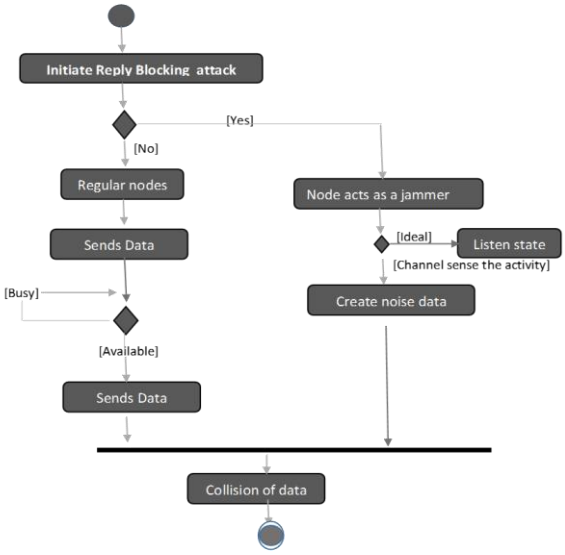

Figure 4: Reply Blocking Attack.

V.SIMULATION OF TBC AND RESULT DETAILS

A. Execution work

In this effort, all the attacks explained above are done with the help of Network simulator tool NS-2. Table-1 shows the arguments used for this execution. All powers required for communication, awake and sleep etc., are assessed based on IEEE 802.15.4 standard.

//ALGORITHM: FLOW OF TBC ALGORITHM

// Input: Fix variables for data sending and threshold value

// Output: changing and informing the route of node to CLH or BS

1. Start
2. Fix the data sending threshold value ;

Level1: CLH Level2:BS

// CLH: Cluster Head BS: Base station

// CLH and BS will check for data to be sent and Threshold value for each node after regular time gap

3. If DS > TH

Inspect the data sending from each node on the route

// check individual node of their send data

If DS > TH

Declare node as blocking node inside and outside the clusters

4. Change the route of CLH or BS and information
5. Stop

The different conditions for the simulation done are

- IoT environment with reply blocking attack
- IoT environment with reply blocking attack with TBC counteragent. 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.

B. Internal Process of TBC

i. Examination by changing traffic interval

Fig.5 and Fig.6 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. Variables used in simulation is given in table1.

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.

TBC mechanism decrease the power utilization after it is executed in the environment than in the implementation of reply blocking attack. The main cause for the reduction of energy level is identification of reply attack in IoT and keeping it away from the environment. The energy consumption taken by the reply blocking attack is reduced and hence save the energy consumption.

Variable Name	Setting Used
NIC	PHY:802.15.4
Antenna	Omni-directional
Link Propagation	Two-ray ground
Type of Channel	Wireless
Type of queue in interface	Priority queue
Queue size	50
MAC	MAC:802.15.4
Routing Algorithm	AODV
Initial Energy	100 J
Idle energy	30 mW
Transmission energy	34 mW
Receiving energy	30 mW
Sleep energy	15 µW
Avg number of nodes	50
Node position	Random

Table 1: simulation variables

ii. Examination by Varying Number of Malicious-nodes

The malicious-nodes involved in blocking the route of the environment increases from 1 to 16. The outcome of this examination clearly says that the performance of TBC is improved against reply blocking while the number of malicious node in the environment is increased. If the blocking situation is increased in the network then the analysis gives more realistic effect of TBC.

The energy utilization in average with the variation of misbehavior nodes in the environment is reduced it means that TBC performs better when the increment of malicious node is done in the network. The main reason for the reduction of energy consumption here is because of the detection mechanism in TBC, it combat the energy that happens due to blocking nodes and nodes' active state without sending anything to the target. TBC's detecting technique actually decrease the time- delay and improve throughput. TBC is used in reducing the delay by reducing the waiting time of the channel and enhance throughput by showing immediate channel availability to nodes during the presence of reply blocking.

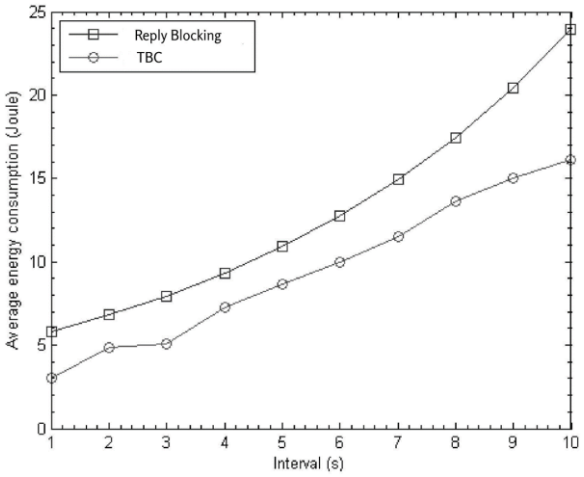

Fig. 5: Average energy consumption with time interval

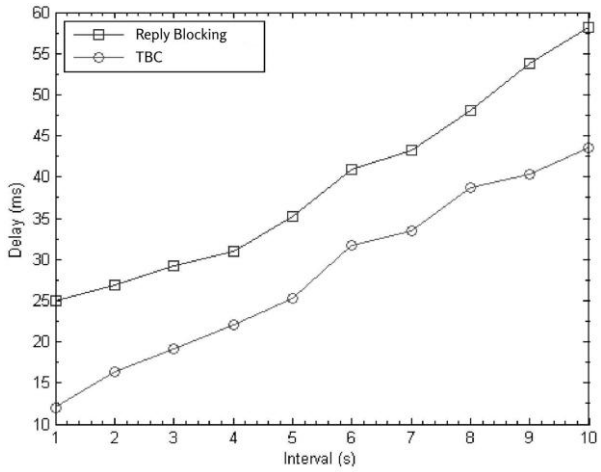

Fig. 6 Average energy consumption with time delay

iii. Evaluation of TBC in Realistic Conditions

The efficiency of proposed TBC mechanism is evaluated in more practical conditions like maintaining time-gap randomly between the data packets and the data to be sent from each node is relayed not at same time but at different time. The realistic condition tells that the performance of TBC behaved well in presence of reply blocking attack. The average level energy consumption of reply blocking using TBC and without using TBC are evaluated by changing number of malicious nodes in the network. It shows that technique used by TBC is used to minimize the delay and enhances the throughput and the energy efficiency is also improved. The performance improvement of TBC is achieved because of efficient availability of channel compared to reply blocking.

iv. Evaluation of TBC in Mobility

The work done here is the performance measurement of average energy consumption, through-put and response time respectively with the variation of the number of misbehavior nodes time to time. The outcome produce a candid support to the proposed work for reason that the measurement we consider here is the mobility in random fashion among the malicious nodes between the tradeoff.

The random waypoint mobility model is considered as a mobility model in this environment. This consideration is used to investigate the versatility of the corresponding counteragent in the existence of mobility among malicious and non-malicious nodes.

VI. CONCLUSIONS AND FUTURE WORK

The various DDOS attacks modeled in the work gives the practical perspective of tasks that is implemented on the occurrence of the blocking assault. This learning is helpful for developing effective security techniques for DDOS attacks. The work also shows the survey of counteragents which are exist and proposes the new counteragent for reply blocking assault. We also propose TBC counteragent which indicates great resistance to reply blocking attacks with fluctuating traffic interim and adding misbehavior nodes in IoT. 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 that the TBC is adaptable when shifting the location of node in the network.

The research will focus on discovering counteragents against remaining types of DDOS attacks with the consideration of the mobility. The TBC algorithm proposed here can likewise be stretched out for cluster-based system by delivering the tasks of threshold measurement among the Cluster Head (CH) nodes to safeguard the network from regular reply blocking and intelligence Cluster head reply blocking attacks.

REFERENCES

1. Mahmoud Ammar , Wilfried Daniels , Bruno Crispo , Danny Hughes, SPEED: Secure Provable Erasure for Class-1 IoT Devices, Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, March 19-21, 2018, Tempe, AZ, USA.
2. Ashraf Al Sharah , Taiwo Oyedare , Sachin Shetty, Detecting and Mitigating Smart Insider Jamming Attacks in MANETs Using Reputation-Based Coalition Game, Journal of Computer Networks and Communications, 2016, April 2016.
3. Khaja Ziauddin, Majoju Sridhar KumarA Prevention of Selective Jamming Attacks by using Packet – Hiding Methods, International Journal of Advanced Research in Computer Science and Software Engineering, September 2014.
4. Shital Patil, Sangita Chaudhari, DoS Attack Prevention Technique in Wireless Sensor Networks, ScienceDirect, 7th International Conference on Communication, Computing and Virtualization 2016.
5. T. Peder, UML Bible. John Wiley & Sons, 2003.
6. Opeyemi Osanaiye, Attahiru S. Alfa, Gerhard P. Hancke, A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks, May 2018.
7. Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad. Proposed security model and threat taxonomy for the Internet of Things (IoT). In Springer CNSA, Chennai, India, 23–25 July, pp. 420–429, 2010.
8. K. Ganesh Reddy, P. Santhi Thilagam, MAC layer security issues in wireless mesh networks, AIP Conference Proceedings 1715, 020028 (2016).
9. Tommy Sparber , Carlo Alberto Boano , Salil S. Kanhere , Kay Romer, Mitigating Radio Interference in Large IoT Networks through Dynamic CCA Adjustment, 2017.
10. Rita Castro, Antonio Gutierrez , José Barbosa, A First Set of Techniques to Detect Radio Frequency Interferences and Mitigate Their Impact on SMOS Data, IEEE Transactions on Geoscience and Remote Sensing, May 2012.
11. Y. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer blocking attacks against wireless sensor network MAC protocols. ACM Transaction on Sensor Network, 5(1):6.1–6.38, 2009.
12. Ahmed R. Mahmood , Hussein H. Aly , Mohamed N. El-Derini, Defending against energy efficient link layer jamming denial of service attack in wireless sensor networks, 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA) , December 2011.
13. Manjunath C R , Sindhu Anand , Jeevan Yadav N S, Secure Transmission in MANET and Wireless Sensor Network, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, May 2014.
14. Dave Evans, The Internet of Things How the Next Evolution of the Internet Is Changing Everything, Cisco Internet Business Solutions Group (IBSG), April 2011.

AUTHORS PROFILE

Mr. A.B. Feroz khan is currently working as Assistant Professor in the Department of MCA, C.Abdul Hakeem College of Engineering and Technology, Vellore, India. He completed MCA in JMC, Tiruchirapalli and M.E.,Computer Science and Engineering in CAHCET, Vellore .He is having 13+ years of teaching experience in computer science & Engineering field. He is currently a Research scholar in Thiruvalluvar University, Vellore, India. He has published many papers in international journals. He also presented papers in many national and international level conferences. His some of the research topics are wireless sensor networks, information security, and Internet of Things.

Dr. G. ANANDHARAJ is currently working as Associate Professor and Head in the Department of PG and Research Department of Computer Science,Adhiparasakthi College of Arts and Scince, Kalavai 632506. He has obtained his MCA Degree from Bharathiar University, M.Phil (Computer Science) in Bharathidasan University and Ph.D from Anna University. He has vast experience in teaching as well as research. He has presented papers at several International and National Conferences and has published research articles in leading Journals. He is an active researcher and is usually associated with reputed Academic Forums and Associations of research interest. gineering College, Tiruchengode, Tamilnadu, India. His research interests include mobile computing and wireless network technology. He is life member of the ISTE. He has guided Ten M.Phil students and currently guiding four Ph.D (Research) scholars in Thiruvalluvar University.