Isolation of Distributed Denial of Service Attack using Threshold Based Technique in Internet of Things

Naveen Kumar, Nitin Mittal,Yogendra Naryan

ABSTRACT--- The internet of things (IoT) is the network which is venerable to security attack. The security attacks affect the network performance in terms of various parameters. The DDOS attack is the active type of attack which reduces network performance. Generally, the cosine similarity technique is used for the isolation of malicious nodes that requires extra hardware for the isolation of malicious nodes. In this research work, the novel technique is proposed for the isolation of malicious nodes. The threshold based technique is proposed in this research work for the detection of malicious nodes from the network. . This technique uses the two parameters for the malicious node detection which are data rate and delay. In threshold based technique, the sensor nodes which increased delay above threshold value will be marked as malicious nodes.

Keywords– Cosine similarity, DDOS, Threshold based technique, IoT.

INTRODUCTION

The network in which several objects are interconnected with each other to interact and communicate in real-time is called Internet of Things (IoT) [1]. Mainly the monitoring and sensory devices that aim to monitor the physical surroundings are placed as devices in these networks. There are uniquely addressable data communicating and collecting devices [2], data transmission network, computing platform and customized user applications are the important components included within the IoT network. It is possible to include almost all the electronic devices in IoT since it is inexpensive and is gaining huge popularity with time [3]. Within several fields like military, government, logistics and medical systems, IoT is applied for supporting the global services and goods supply chain networks since it provides a smart architecture for information exchange [4]. After the Internet and mobile communication network, IoT is known to be the third wave of information technology. However, challenges related to IoT technology have also been faced with the increase in growth of IoT application in different regions [5]. Several heterogeneous devices have been included in IoT network as compared to internet that mainly connects only the personal computers and mobile communication device at most [6]. With the increase in population, the number of IoT sensory devices is also increasing. Different kinds of challenges are being faced during the information modeling and reasoning of data since such huge amount of data is generated and collected in this network [7]. It is importance to perform communication among the distributed heterogeneous devices in real time such that the physical world and digital world can interact [8]. So, to ensure highly efficient and reliable end-to-end communication across IoT networks, a solution needs to be derived. The data collected is very sensitive in certain applications which also highlights the concern of maintaining authentication, access control as well as client privacy [9].

A type of network attack that disrupts the legitimate requests is called Distributed Denial of Service (DDoS) [10]. The targeted host server is flood with bad requests such that the bandwidth of legitimate users can be reduced temporarily through DDoS attack [11]. For causing serious threats the DDoS attack engages more computers and internet connections to an attacking behavior where the accesses of users to host server are blocked or suspended [12]. The client inconvenience and loss of private information is faced in such cases. The carefully designed packets within the host server are disrupted by the attack that is crashed on the targeted service [13]. This results in freezing or rebooting of the operating system. Other than that, all the resources on the host server are occupied by the malicious packets with bad requests.

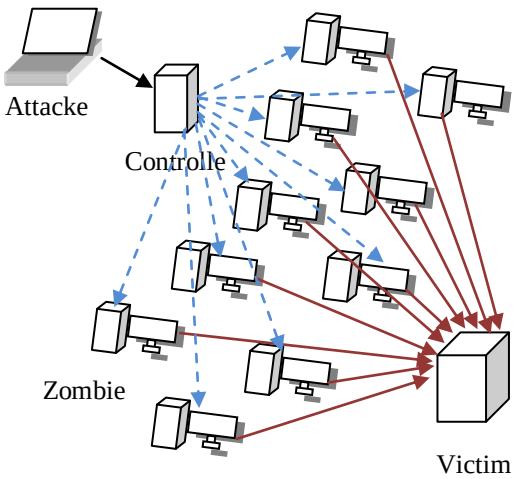

Figure 1: DDoS Attack in IoT

Revised Manuscript Received on May15, 2019.

Naveen Kumar Research Scholar, Chandigarh University Gharuan, Mohali, India. (E-mail: navthakur91@gmail.com)

Dr.Nitin Mittal Associate Professor, Chandigarh University Gharuan, Mohali. (E-mail :Mittal.nitin84@gmail.com)

YogendraNaryanAssistant Professor, Chandigarh University Gharuan, Mohali, India. (E-mail: narayan.yogendra1986@gmail.com)

Vulnerability within one computer system is exploited initially by the hacker in a typical DDoS attack [14]. This vulnerable device is chosen to be the DDoS master and the remaining malicious activities are performed from this device. The remaining systems which can be compromised are connected through this master system. On around thousands of compromised systems, the cracking tools available on Internet are loaded by the intruder [15]. For launching one of the many flood attacks against a particular target, the controller machines as instructed by the intruder using one single command. A denial of service is caused by the inundation of packets to the target.

The internet of things is the decentralized network due to which makes entry of attacker nodes possible within the network which affects performance of the things. In the previous approaches, no counter technique is proposed which can authenticate sensor devices The techniques which can which proposed so far for the detection of malicious nodes required extra hardware for the detection of malicious nodes. The techniques needs to be proposed which donot require extra hardware for the detection of malicious nodes The techniques which are proposed in the previous years have the much complexity which take extra time for the detection of malicious nodes. In this research work, the novel approach needs to be proposed which detect malicious node accurately in the least amount of time. The novel approach is proposed in this research work, for the detection of malicious nodes. The proposed technique will detection malicious and does not use any extra hardware and software for the detection which is the main contribution.

In the section 1, the introduction is given related to internet of things and also various issues related to IoT. The DDOS attack affects network performance and various techniques have been designed so far for the detection of malicious nodes which are presented in section 2. The technique which is designed in this research work is highlighted in section 3. In the last section results of the proposed technique is presented and compared with existing technique.

LITERATURE REVIEW

The various techniques has been proposed by the authors for the detection of malicious nodes from the techniques. The previous proposed techniques are based on certain concepts which are presented in this section

Yin, et.al (2018) proposed an approach which was based on SDx paradigm for the SD-IoT (Software-defined IoT) networks [16]. A controller pool that includes SD-IoT controllers, IoT devices and SD-IoT switches linked with an IoT gateway were included within this proposed mechanism. For determining if the DDoS attacks occur in IOT or not, the cosine similarity of vectors of packet-in message rate was used at the boundary SD-IoT switch ports. The simulation outcomes showed that the presented approach performed better by means of power utilization and packetloss. With the help of heterogeneous and vulnerable devices the security of IoT was improved.

Gurulakshmi, et.al (2018) proposed a study in which the network traffic was classified with certain predefined parameters to prevent DDoS attack [17]. For the classification of packets with good accuracy, both SVM and k-NN classifiers were applied. The results achieved showed that the proposed approach outperformed existing techniques in terms of throughput and routing overhead. In future, machine learning concepts could be applied to prevent the attack and entrance of suspicious traffic from the port to the network.

Zheng, et.al (2018) proposed a MDP-based optimal mechanism through which the DDoS attacks were detected and mitigated from SDN based IoT networks [18]. To keep the flow optimized traffic and alerting the system administrators regarding the scenarios was the main objectives of this approach. Thus, the DDoS attacks could be detected at an early stage and enough time for mitigating the attacks could be provided to the administrators. Simulation results that the manner in which system could transit from one state to another could be controlled by the administrator by adjusting the reward weight and discount factor when applying the proposed technique.

Huraj, et.al (2018) proposed a novel approach to handle the Distributed Reflective DoS Attack (DRDoS) a sort of DDoS intrusion [19]. The attacker flooded the packets to the IoT device that acted as a reflector with the source IP address to the victim's IP address which received the reflected replies and could be overloaded as well. The IoT devices can be integrated into DRDoS intrusion as per these outcomes of this proposed technique. Also, the possibility of a device to act as a target victim by flooding the network was also be eliminated.

Adat, et.al (2017) presented the study of risk transfer mechanism when applied in IOT-based smart home scenarios [20]. The DDoS mitigation algorithm and safety of previous approaches were simplified in this research through improvements. Also, for improving the response time, the blacklist and graylist were removed. For providing additional security as per the need a protected correlation with the client's IoT scenario was provided by the developed EDoS server. The end level clients who create their individual networks by utilizing IoT technologies from several suppliers mainly used this model. Extra security was provided through proposed approach in IoT scenario.

Kawamura, et.al (2017) proposed a novel event detection module through which DDoS attacks were detected [21]. This module was based on the system behavior in the presence of DDoS attacks and the information achieved from network time protocol(NTP). This phenomenon was used to perform synchronization for detecting these attacks. The pseudo DDoS attacks were generated to evaluate the performance of designed module. High recall and precision values were achieved as per the outcomes achieved after implementing proposed technique.

The techniques whichare proposed so far are based on the malicious nodes are based on software defined techniques. The software defined techniques require extra hardware and software for the detection of malicious nodes. The second type of techniques for the malicious node detection are based on the classification techniques. The classification techniques increase complexity of the model and software defined techniques increase cost of the model.

Table 1: Literature Review Analysis

Author	Technique	Outcome
Yin, et.al	A controller pool that includes SD-IoT controllers, IoT devices and SD-IoT switches linked with an IoT gateway were included within this proposed mechanism. For determining if the DDoS attacks occur in IOT or not, the cosine similarity of vectors of packet-in message rate was used at the boundary SD-IoT switch ports.	The simulation results show that the proposed approach performed better in terms of energy consumption and packetloss
Gurulakshmi, et.al	A study in which the network traffic was classified with certain predefined parameters to prevent DDoS attack	The results achieved showed that the proposed approach outperformed existing techniques in terms of throughput and routing overhead.
Zheng, et.al	The DDoS attacks could be detected at an early stage and enough time for mitigating the attacks could be provided to the administrators	Simulation results that the manner in which system could transit from one state to another could be controlled by the administrator by adjusting the reward weight and discount factor when applying the proposed technique.
Huraj, et.al	The attacker flooded the packets to the IoT device that acted as a reflector with the source IP address to the victim's IP address which received the reflected replies and could be overloaded as well.	Also, the possibility of a device to act as a target victim by flooding the network was also be eliminated.
Adat, et.al	The DDoS mitigation algorithm and safety of previous approaches were simplified in this research through improvements. Also, for improving the response time, the blacklist and graylist were removed.	Highly required market of extra security was provided through this proposed approach.
Kawamura, et.al	A novel event detection module through which DDoS attacks were detected [21]. This module was based on the system behavior in the presence of DDoS attacks and the information achieved from network time protocol(NTP)which was used in synchronization service was used to detect these attacks.	High recall and precision values were achieved as per the outcomes achieved after implementing proposed technique.

THRESHOLD BASED TECHNIQUE

The complete SD-IoT framework is categorized into three layers which are application layer, control layer and infrastructure layer. IoT server is included in the cloud computing center within the application layer. The controllers present in the SD-IoT controller pool are connected to this IoT server. APIs are used by IoT server to provide several applications and services. A controller pool that includes several SD-IoT controllers is provided in the control layer through which a distributed operating system is run. Thus, for forwarding data in a distributed physical network scenario, a logical centralized control and a topology view is provided by these SD-IoT controllers. A mass of SD-IoT switches is included in the infrastructure layer. Te function of an IoT gateway and an SDN switch are integrated in each SD-IoT switch. Also, by controlling the data plane interface, various IoT actuating devices and sensing devices can be accessed by each SD-IoT switch.

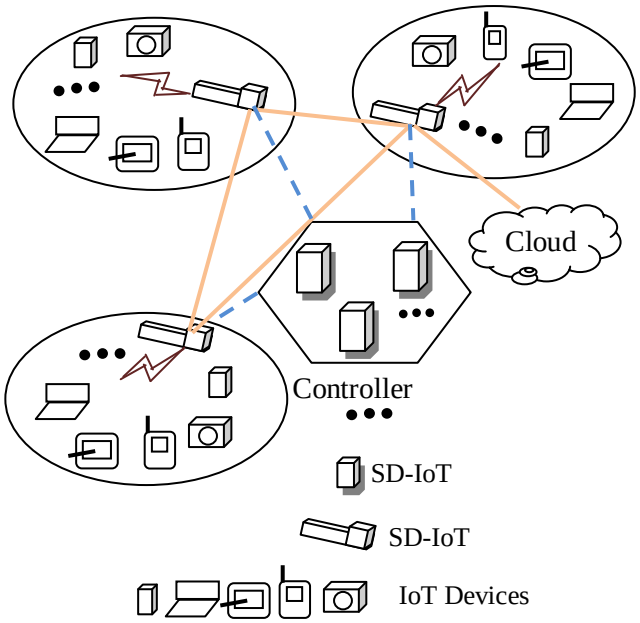

Figure 2: SD-IoT framework

IOT is the decentralized type of network which makes entry of malevolent nodes possible within the network which affect performance of the things. In the previous approaches, no counter technique is proposed which can authenticate sensor devices. The techniques which proposed so far to detect attacker nodes required extra hardware for the detection of malicious nodes. The techniques need to be proposed which does not require extra hardware for detecting attacker nodes. In this research work, the novel approach should be proposed for the accurate detection of attacker nodes in the least amount of time.

The proposed trust based mechanism for the discovery of malevolent nodes on the basis of data rate of the sensor nodes. The data rate of the sensor nodes is the base ofproposed trust based mechanism.

Different phases of the proposed flowchart are described below:-

1. Network Deployment and pre-processing:- The wireless sensor network is organized with fixed amount of sensor nodes. The DDOS attack is trigger by the malicious node. The researchers have proposed several approaches for detecting attacker nodes. Such techniques detect the malicious nodes by using extra hardware and software[].The technique of intrusion detection increases complexity of the system. The threshold based technique calculate threshold value of data rate. The formula which define threshold data rate for the detection of malicious node is given below

P = Pb *max_p;

The average data rate used in simulation is described by a variable called “Pb”. The standard data rate used in simulation is 1 packet per 0.05 second. The lower bound value of the delay is defined by the “max_p”. The upper bound value is denoted by “max”. The average data rate is represented by “Pb”. when this variable is multiplied by the upper bound value then the threshold data rate is obtained.

2. Detection of Malicious nodes: - The sensor nodes are deployed arbitrarily in a restricted area. The proposed approach is based on the per hop delay for detecting attacker nodes.Per hop delay is calculated on the basis of rounds trip time. The rounds trip time is calculated on the basis of time when the source send the route request packets and when the source receives reply message. The source node chooses optimal route on the basis of hop count and series number. The source starts sending the data on the selected path. The source analyzes the network parameters for the detection of malicious node. The source check delay in the network, when the delay is increased in the network then it calculates per hop delay. The per hop delay is calculated with the equation 1

$$\text{Threshold delay} = \frac{Round\ \ trip\ \ time}{2hi} = \frac{ti - ts}{2hi} \text{---} \quad (1)$$

The round trip time is calculated with the ti and ts which is represented as the time used for the delivery of route request packets and time consumed in the delivery of route reply packets

The delay at each hop is calculated with the equation number 2

$$\text{Delay} = \sum_{i=0}^{i=n} Packet\ arrive\ time - Packet\ send\ time \ / \sum_{i=o}^{i=n} number\ of\ connection \text{ ---} \quad (2)$$

When the delay is higher than the threshold delay, then sensor node is considered as the malicious node.

3. Isolation of Malicious nodes:-The malicious node detect process use the threshold delay and maximum data rate. When source node transmits information towards destination as per the defined data rate and any node which is increasing delay than the threshold delay will be identified as attacker node. The alert message will be generated in the network, which informs all nodes about malicious nodes in the network.

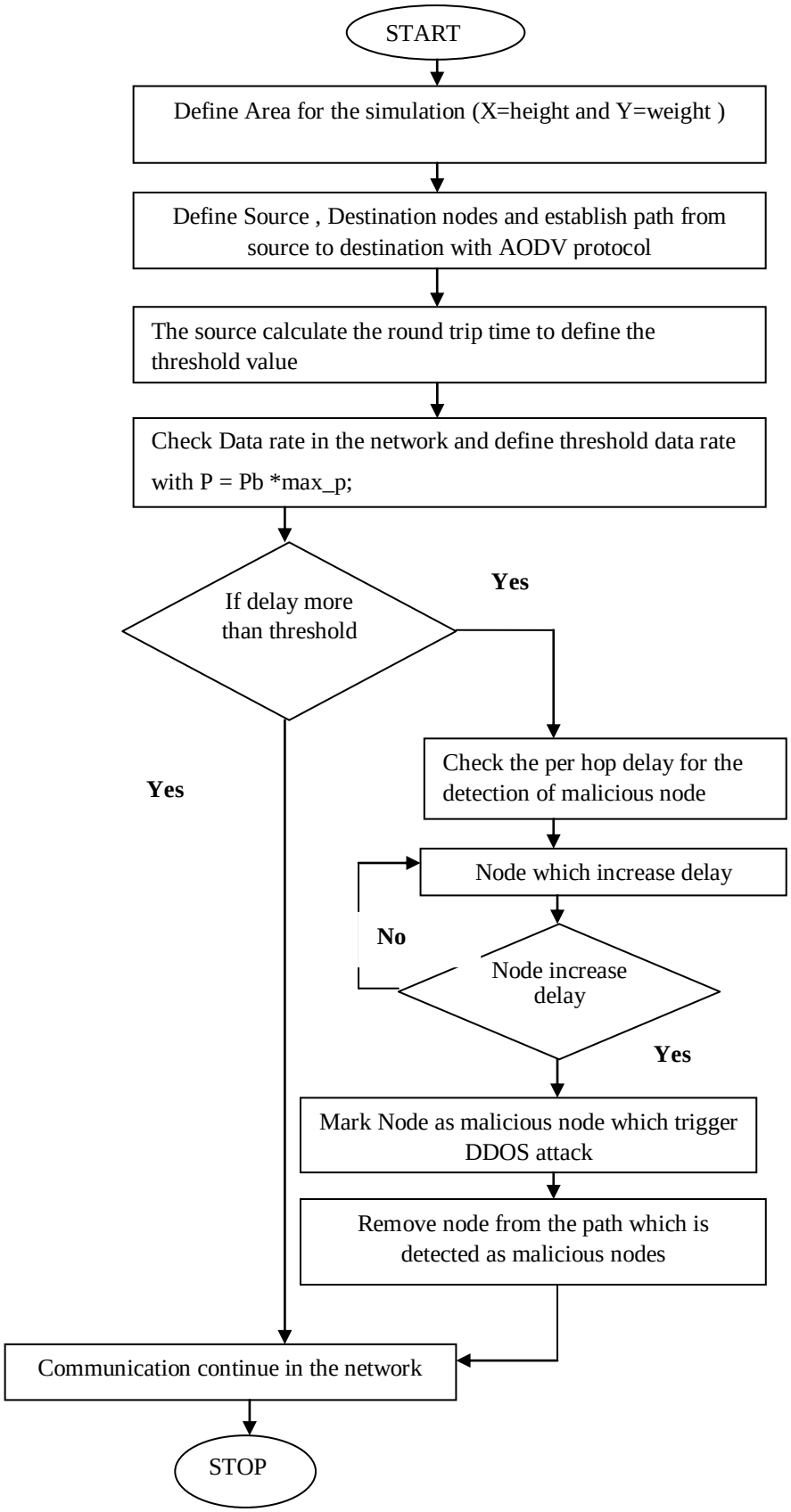

Fig 3: Proposed Flowchart

RESULT AND ANALYSIS

A tool named MATLAB is used for the implementation of proposed approach. The outcomes are analyzed on the basis of certain parameters like throughput and packetloss.

1. Throughput : The throughput is the parameter which analyze that how many packets are successfully delivered on the destination

Throughput =(No of packets Received)/(Total number of packet send) * time

2. Packetloss : The packet loss is the number of packets which are lost during data transmission in the network

Packetloss= No of packets send - No of packets received

Table 2: Simulation Parameter

Simulation parameters	Values
Channel – Type	Wireless channel
Propagation model	Two ray ground propagation
Mobility Model	Random way point
Antenna Type	Omi-directional
Number of nodes	100
Speed (s)	150 m/second
Traffic Type	CBR
Mac Type	IEEE 802.11 (b/g)
Routing Protocol	AODV
Area ofsimulation	800* 800
Time of simulation	100 seconds

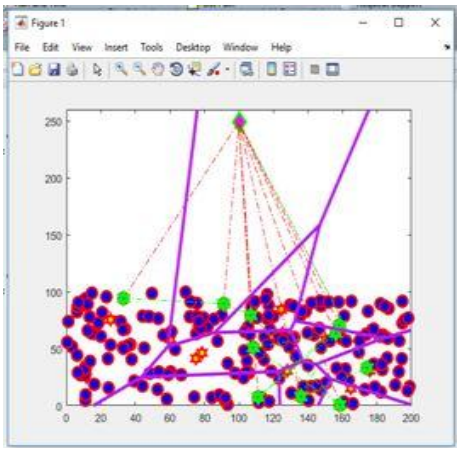

Fig 4: Network Deployment

The figure 4 shows that the IoT network is organized with fixed amount of sensor nodes. The division of entire network is performed with fixed size clusters for the delivery of information towards the base station.

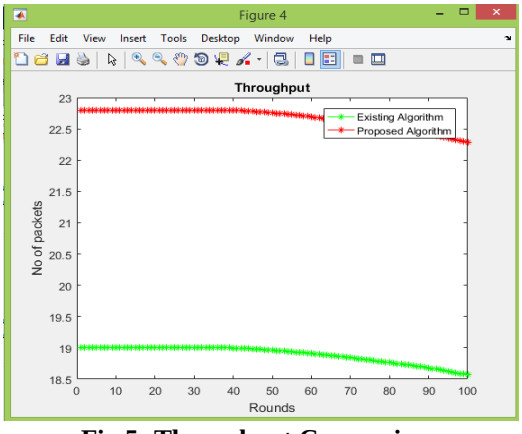

Fig 5: Throughput Comparison

The figure 5 shows that the throughput of the projected technique is compared with the attack scenario. In the attack scenario, the DDOS attack is triggered inside the network. The proposed approach is applied for the isolation of malicious nodes.

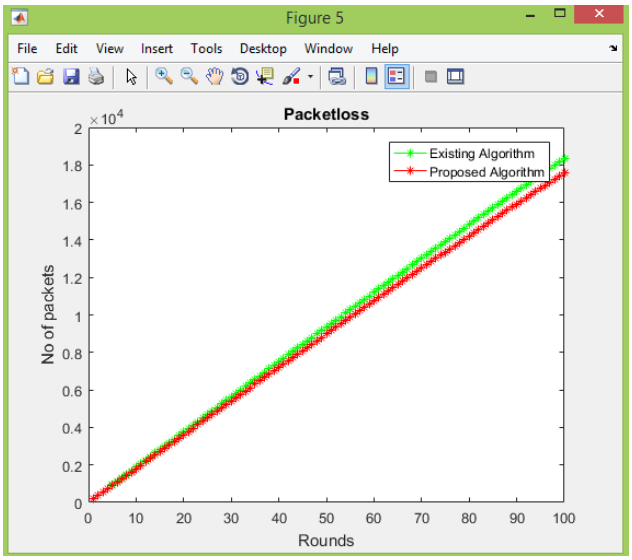

Fig 6: Packet loss Comparison

The figure 6 shows that the packet loss of the threshold technique is compared with the attack scenario In the proposed technique novel technique is proposed for the isolation of malicious nodes. It is analyzed that proposed technique has less packet loss in comparison with attack scenario

CONCLUSION

In this work, it is concluded that internet of things is the network which is a self arranging type of network. Because of self configuring nature, the malicious nodes enter the network and triggers different kinds of active and passive intrusions. The DDOS intrusion is an active kind of intrusion which reduces network performance. The cosine similarity based technique requires additional hardware to discover attacker nodes. In this research work a novel approach is proposed to detect the attacker nodes. The threshold technique does not require any hardware and software for the detection of malicious node. The threshold technique increase network throughput and reduce packet loss. In future, the secure encryption technique will be proposed to increase security of the network.

REFERENCES

1. S. Srivastava, and N. Pal, “Smart Cities: The Support for Internet of Things (IoT).” Int. J. Comput. Appl. Eng. Sci., 6(1), 5. 2016, pp. 5-7.
2. Suo, Hui, Jiafu Wan, CaifengZou, and Jianqi Liu. “Security in the internet of things: a review.” Proc. of IEEE Int. Conf. on Comp. Sci. and Electr. Eng. (ICCSEE), vol. 3, IEEE, 2012, pp. 648-651.

3. I. DirgovaLuptakova, and J. Pospichal, "Community Cut-off Attack on Malicious Networks", Proc. of Conf. on Creativity in Intelligent Technologies and Data Science. Springer, Cham, 2017, pp. 697-708.
4. D. Pishva, "IoT: Their Conveniences, Security Challenges and Possible Solutions", Adv. Sci. Technol. Eng. Syst. J., 2.3, (2017), pp. 1211-1217.
5. L. Berti-Equille, and Y. Zhauniarovich, "Profiling DRDoS Attacks with Data Analytics Pipeline", Proc. of ACM Conf. on Information and Knowledge Management, November 6–10, 2017, Singapore, pp. 1983- 1986.
6. R. van Rijswijk-Deij, A. Sperotto, and A. Pras, "DNSSEC and its potential for DDoS attacks: a comprehensive measurement study", Proc. of the 2014 Internet Measurement Conference. ACM. 2014, pp. 449– 460.
7. S. Kumar, "Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet," Proc. of the 2 nd Int. Conf. on Internet Monitoring and Protection. IEEE, 2007.
8. R. Shankesi, M. AlTurki, R. Sasse, C. A. Gunter, and J. Meseguer, "Model-checking DoS Amplification for VoIP Session Initiation", Computer Security–ESORICS. Lect Notes ComputSc, vol 5789. Springer, Berlin, Heidelberg, 2009, pp. 390–405
9. AbdulazizAborujilah and ShahrulnizaMusa,"Cloud Based DDoS HTTP Attack Detection Using Covariance Matrix Approach", Journal of Computer Networks and Communications Volume 2017
10. David Beckett, SakirSezer, John McCanny, "New Sensing Technique for Detecting Application Layer DDoS Attacks Targeting Backend Database Resources", IEEE ICC 2017 Communication and Information Systems Security Symposium.
11. L. Arockiam, B. Vani, "Security algorithms to prevent Denial of Service (DoS) attacks in WLAN", International Journal of Wireless Communications and Networking Technologies, 2013
12. Y. Bekeneva, N. Shipilov, A. Shorov, "Investigation of Protection Mechanisms Against DRDoS Attacks Using a Simulation Approach", Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Lect Notes ComputSc, vol 9870. Springer, 2016.
13. Kolias, Constantinos, et al.: "DDoS in the IoT: Mirai and other botnets", Computer 50.7 (2017): 80-84.
14. I. van der Elzen, and J. van Heugten, "Techniques for detecting compromised IoT devices", Project Report. University of Amsterdam, 2017.
15. J. D. T. Gonzalez, and W. Kinsner, "Zero-crossing analysis of Lévy walks for real-time feature extraction: Composite signal analysis for strengthening the IoT against DDoS attacks", Proc. of IEEE 15th Int. Conf. on Cognitive Informatics & Cognitive Computing (ICCI* CC), IEEE, 2016.
16. Da Yin, Lianming Zhang, Kun Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework", 2018, IEEE Access, Volume: 6, pp- 24694 – 24705
17. K. Gurulakshmi, A. Nesarani, "Analysis of IoT Bots Against DDOS Attack Using Machine Learning Algorithm", 2018, 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Pages: 1052 – 1057
18. JianjunZheng, Akbar SiamiNamin, "Defending SDN-based IoT Networks Against DDoS Attacks Using Markov Decision Process", 2018 IEEE International Conference on Big Data (Big Data), Pages: 4589 – 4592
19. LadislavHuraj, Marek Simon, TiborHorák, "IoT Measuring of UDP-Based Distributed Reflective DoS Attack", 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Pages: 209 – 214
20. VipindevAdat, B. B. Gupta, Shingo Yamaguchi, "Risk transfer mechanism to defend DDoS attacks in IoT scenario", 2017, IEEE International Symposium on Consumer Electronics (ISCE), Pages: 37 – 40
21. Tamotsu Kawamura, Masaru Fukushi, Yasushi Hirano, Yusuke Fujita, Yoshihiko Hamamoto, "An NTP-based detection module for DDoS attacks on IoT", 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2017, Pages: 15 – 16