INTRUSION DETECTION SYSTEM FOR HYBRID DOS ATTACKS USING ENERGY TRUST IN WIRELESS SENSOR NETWORKS

[1] Er. Sandeep Kaur
Research Scholar,
Department of Computer Science,
BGIET, Sangrur, Punjab, India.

[2] Er. Renu Nagpal,
Assistant Professor,
Department of Computer Science,
BGIET, Sangrur, Punjab, India.

***Abstract*:** The research content of this article is to design an intrusion detection scheme based on Traffic Prediction for the large-scale tiled WSN (Traffic Prediction Intrusion Detection Scheme, or TPIDS), detecting attacks which have considerable influence on the flow, such as the selective forwarding attacks and DOS attacks. As far as we know, this is first intrusion detection scheme for WSN at home and abroad using the traffic prediction model. An important such perspective in terms of detecting DoS attacks is to view the problem as that of a classification problem on network state (and not on individual packets or other units) by modeling normal and attack traffic and classifying the current state of the network as good or bad, thereby detecting attacks when they happen. ACO is used to control the energy and Bayesian network is used to control the transmission route between nodes, CH and base stations of different tires. The result being obtained with different parameters like Network lifetime, Network throughput and Detection ratios. In this research work network life time is 98, throughput is 16.5 and detection ratio is 1.0 that is calculated in this work. It is due to DAG and ACO, because if shortest path is found then energy is saved. If energy is saved the network life time is high and throughput is also varied. In the future work other different types of network attacks are prevented with the help of different protocols and different techniques.

***Index Terms*: DDOS, Attack, ACO, WSN, sensor network etc.**

I. INTRODUCTION

An intrusion detection scheme based on node energy prediction. It analyzes the energy consumption difference of different DoS attack comprehensively, predicts the energy consumption of nodes by Markov chain model, and judges the security state of nodes. A detection model of Sybil attack through the node energy trust mechanism, and the Sybil attack was identified by multilevel detection. A wireless sensor network energy saving intrusion detection scheme based on Bayesian energy prediction, which detected the malicious nodes with energy consumption by comparing the actual energy and the predicted energy. The node of the energy anomaly is detected as a malicious node.

Cluster head nodes detect malicious attacks by monitoring the energy of the nodes. The monitoring node uses the hidden Markov model (HMM) to predict the energy and compares it with the actual energy detected by the energy query technology. The detected attacks are classified according to the energy threshold. The above intrusion detection mechanism based on energy consumption all have a good detection effect for a single DoS attacks, but they do not consider the actual situation of the node being attacked by hybrid attacks. Aiming at the hybrid DoS attack in wireless sensor network, a new intrusion detection method based on energy trust (IDSET) is proposed on the existing detection mechanism, which improves the detection rate of hybrid DoS attacks. WSN, which is the abbreviation for wireless sensor network, can implement complex and large-scale environmental monitoring and tracking tasks in a wide range of application areas, so it has highly application[1,2]in the national defense and military, environmental monitoring, traffic management, disaster rescue and many other fields. Wireless transmission of WSN, characteristics which are no one care and other natural make it vulnerable to all kinds of attacks. One of the most damaging attacks is deceptive and denial of service (or DoS) attacks.

Under the premise of the covering as much as possible, the former seeks to produce the monitoring results of a false so that the results cannot be trusted to monitor. The latter seeks to damage local network or even the overall function of the network so that facilities are not available. So when WSN has been used in the scene with important mission, such as the residential wireless protection network of the commercial, battlefield surveillance of the military and so on, how to ensure that information can quickly and accurately transmit plays a key role in the success or failure of the whole mission. A sensor node is a tiny and simple device with limited computational capability and broadcast power. Wireless sensor networks are generally provisioned to consist of a large number of inexpensive nodes reporting their data to a central, more capable sink node using multihop transmission.

II. NETWORK SECURITY

As a society we are becoming increasingly dependent on the rapid access to and faster processing of information. As this demand has exponentially increased in recent times, more information is being stored and processed by computers. The increased use of computers has made rapid tabulation of data from different sources possible. Correlation of information from different sources has allowed additional information to be inferred that may be difficult to obtain otherwise. The proliferation of inexpensive computers and of computer networks has exacerbated the problem of unauthorized access and tampering with data. Increased connectivity not only provides access to larger and varied resources of data more quickly than ever before, but also provides an access path to the data from virtually anywhere on the network. Network hackers such as Internet worm attacks have easily overcome the password authentication mechanisms designed to protect systems. With an increased understanding of how systems work, intruders have become skilled at determining weaknesses in systems and exploiting them to obtain such increased privileges that they can do anything on the system. Intruders also use patterns of intrusion that are difficult to trace and identify. They rarely indulge in sudden bursts of suspicious or anomalous activity. They also cover their tracks so that their activity on the penetrated system is not easily discovered. Access control therefore does not model and cannot prevent unauthorized information flow through the system because such flow can take place with authorized accesses to the objects.

They are useful not only in detecting successful breaches of security, but also in monitoring attempts to breach security and provides important information for timely countermeasures. Thus, intrusion detection systems are useful even when strong preventive steps taken to protect computer systems and enhance the degree of confidence in their security. Furthermore, preventive steps such as repairs of system software faults may not always be preferable to detection of their exploitation from a practical cost-benefit consideration. Fixing bugs may not be possible without adequate software resources and requisite expertise.

Large scale deployment of patches may require more cumbersome installation procedures than updating the intrusion detection database, especially when software is customized for local use at individual sites. In the case of large complex programs, such as send mail, it may not be possible at all when its source code is available in a network node. Monitoring generic methods of exploiting vulnerabilities can be very useful in such large networks. Intrusion detection starts with instrumentation of a computer network for data collection. Pattern-based software ‘sensors’ monitor the network traffic and raise ‘alarms’ when the traffic matches a saved pattern. Security analysts decide whether these alarms indicate an event serious enough to warrant a response.

Traditional protection techniques such as user authentication, data encryption, avoiding programming errors and firewalls are used as the first line of defense for computer security. If a password is weak and is compromised, user authentication cannot prevent unauthorized use. Firewalls are vulnerable to errors in configuration and suspect to ambiguous or undefined security policies. Intrusion detection is required as an additional wall for protecting systems despite the prevention techniques and also in monitoring attempts to break security. Intrusion detection systems are classified as:

- Misuse intrusion detection system
- Anomaly intrusion detection system

Misuse intrusion detection systems use well-defined patterns which are encoded in advance and used to match against user behavior to detect intrusions. Alternatively detecting policy violations allows administrators to identify areas where their defenses need improvement such as identifying a previously unknown vulnerability, a system that wasn’t properly patched, or a user who needs further education against social engineering attacks. The problem is that current NIDS are tuned specifically to detect known service level network attacks. Attempts to expand beyond this limited realm typically results in an unacceptable level of false positives. At the same time, enough data exists or could be collected to allow network administrators to detect these policy violations.

III. METHODOLOGY

Sensor hubs are arbitrarily dispersed in the detecting field. In this system, the hubs are static and settled. The sensor hubs sense the data and after that send to the server. On the off chance that the source hub sends the parcel, it will send through the middle of the road hub. The hubs are imparts just inside the correspondence go. In this way, we need to discover the hub's correspondence extend. we have presented authentication method and data filtration method to tackle both outsider and insider DDoS attacks. Authentication is the best way to keep the outsider attackers stay away from the network. Route request flooding (outsider attack) is one of the frequent attacks in WSN because attackers attack the legitimate nodes by bombarding the route request or authentication packets in the network; in that case data filtration method plays an important role to prevent this attack. Insider attacks are also frequent in WSN because of their deployment in remote areas with lesser maintenance and thus leading to node capturing. Insider attacks can also be prevented by the data filtration method.

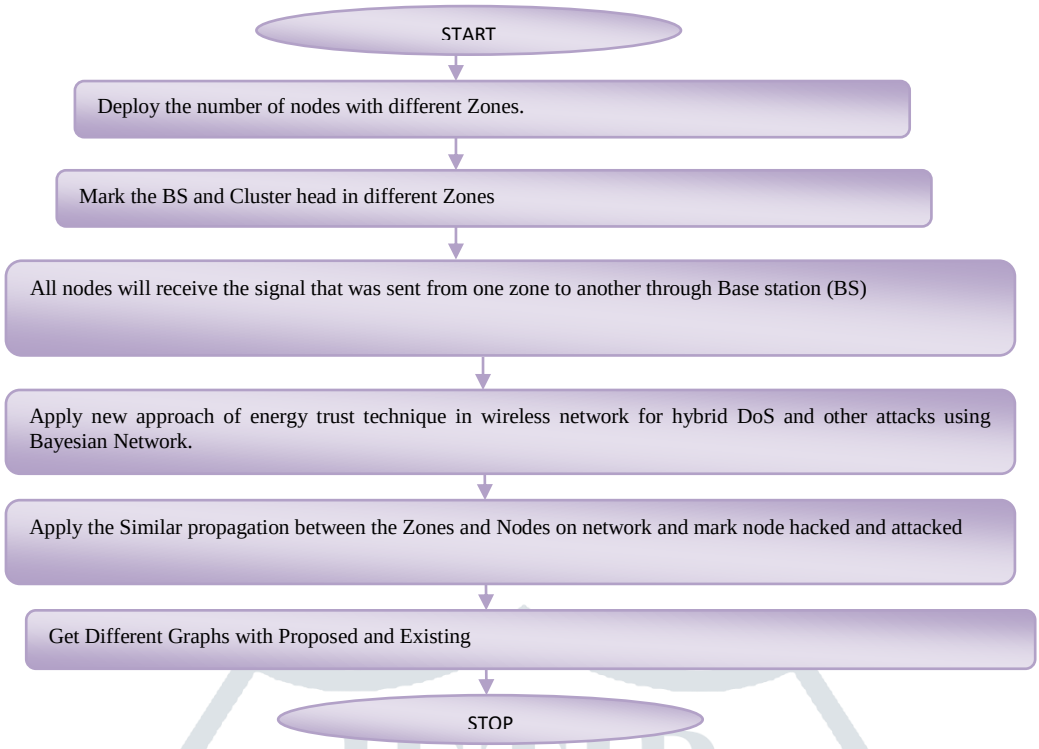

figure 1.1: flow chart of the work

IV. **RESULT & DISCUSSION**

These snap shorts are given below:

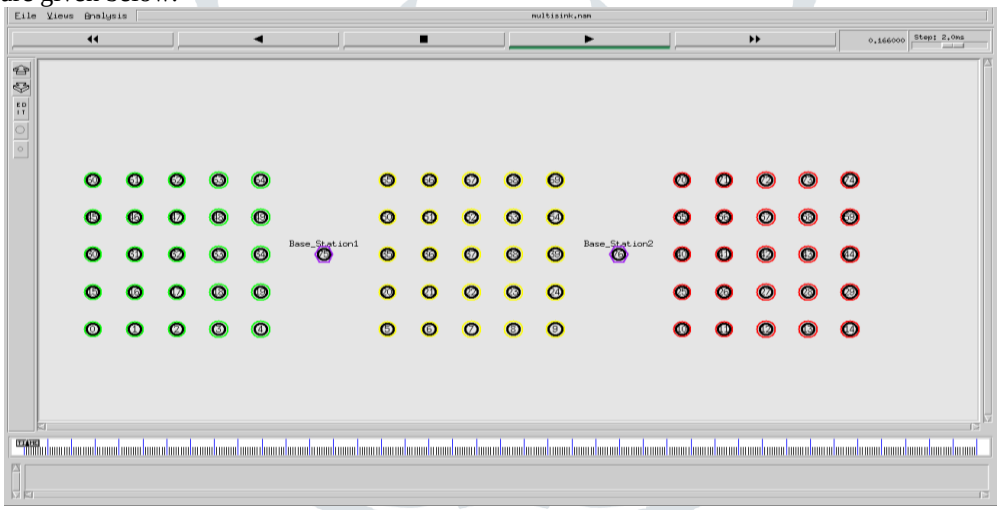

figure 2: node with base station

The figure 2 displays the different color nodes with different base stations. In this figure two base stations are defined i.e. is used to transfer the data from one zone to another zone.

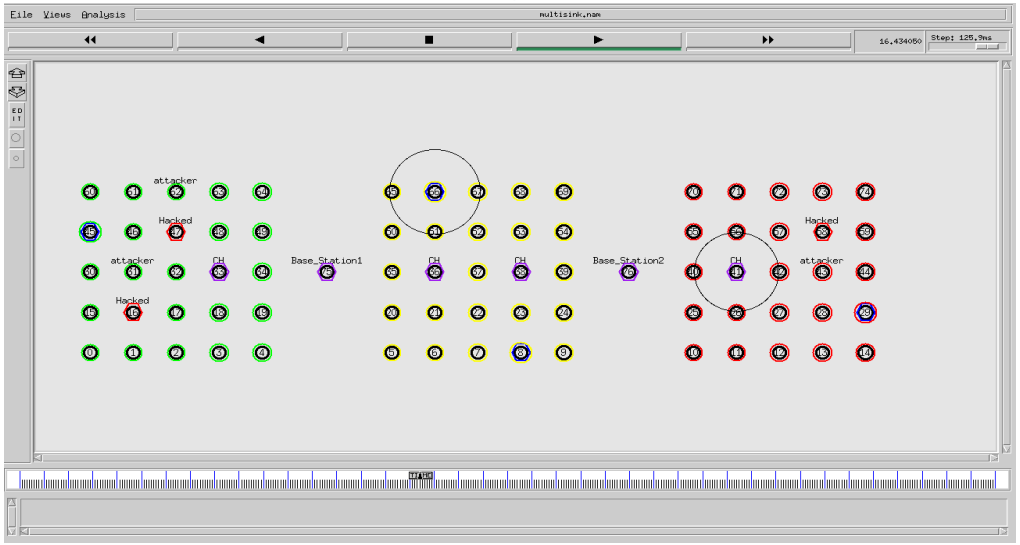

figure 3: data transferred through ch

The figure 3 is the Nodes with hacked and attacked, here hacked node is marked with red color and CH is marked with purple colors. In the figure 5.6 active nodes are akso marked with purple colors. All these nodes are used to transfer the data between nodes.

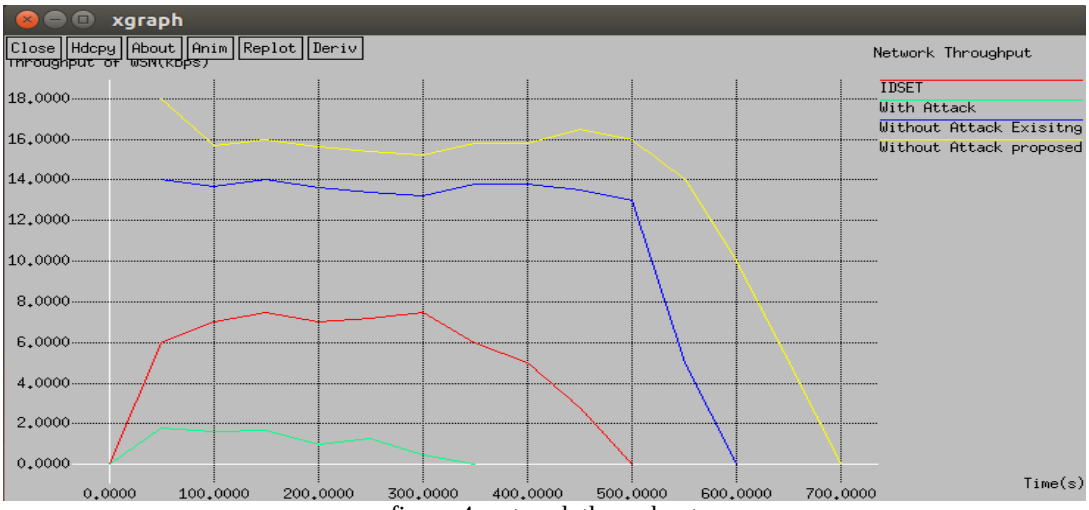

figure 4: network throughput

The figure 4 is the network throughput of different Intrusion detection systems with attack and without attacks is displayed. The IDSET is defined with red line and with attack is explained with green line and other are defined with blue and yellow line.

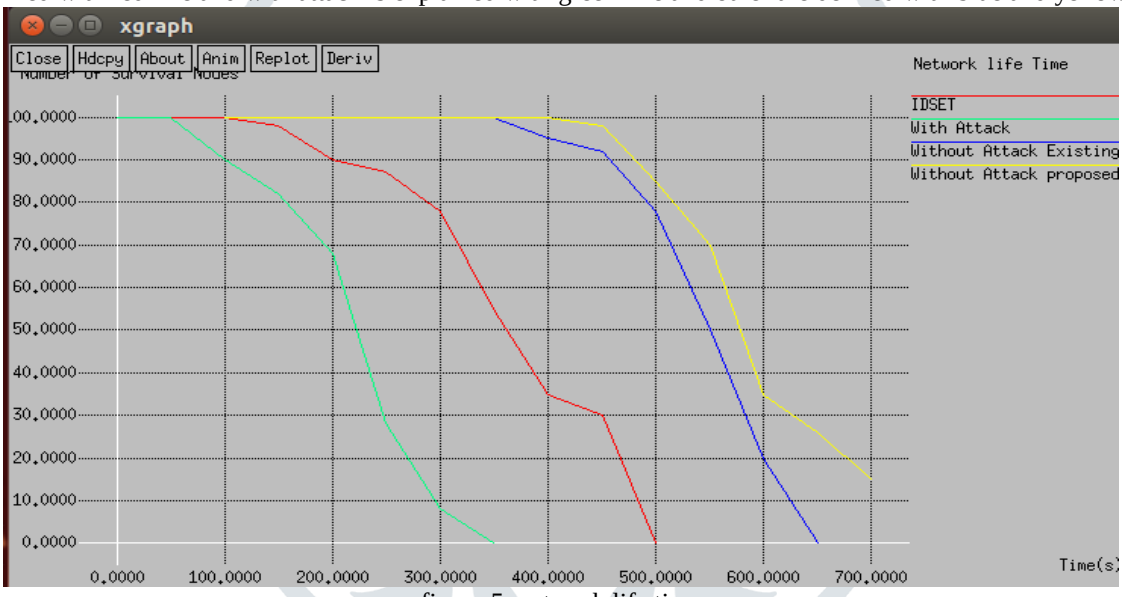

figure 5: network life time

The figure 5 is the network life time of different Intrusion detection systems with attack and without attacks is displayed. The IDSET is defined with red line and with attack is explained with green line and other are defined with blue and yellow line.

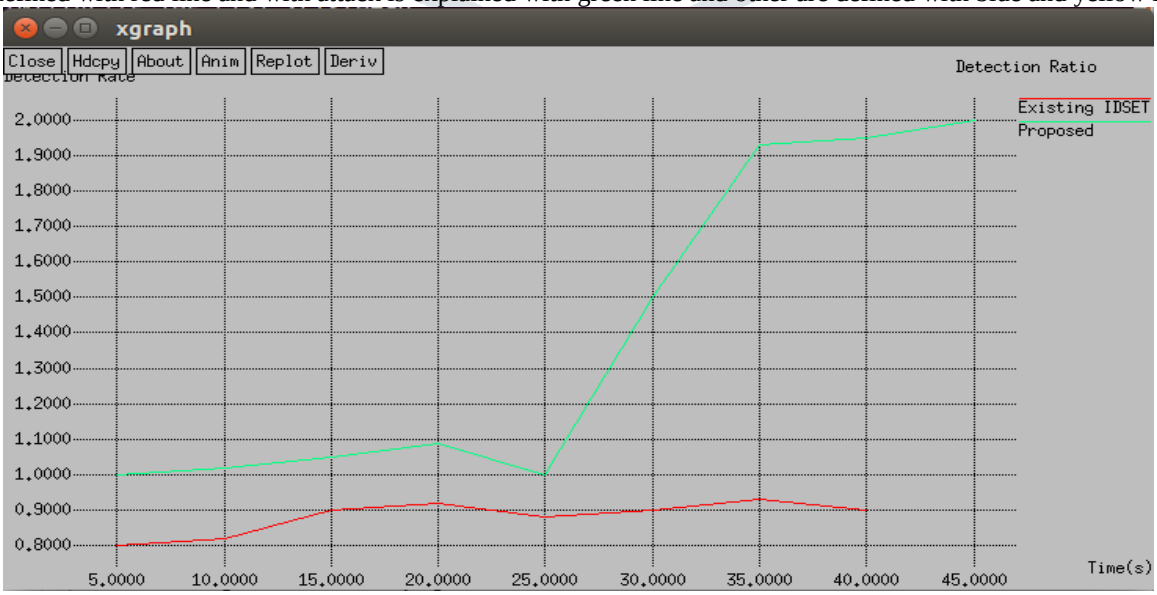

figure 6: detection ratio

The figure 6 is the detection ratio of different Intrusion detection systems In this figure detection ration of IDSET is defined with red line and proposed detection ration is defined with green line.

Table 1: network throughput

IDSET		With Attack		Without Attack Existing		Without Attack proposed	
0	0	0	0.0	0	0	0	0
50	6	50	1.8	50	14	50	18
100	7	100	1.6	100	13.7	100	15.7
150	7.5	150	1.7	150	14	150	16
200	7	200	1.0	200	13.6	200	15.6
250	7.2	250	1.3	250	13.4	250	15.4
300	7.5	300	0.5	300	13.2	300	15.2
350	6	350	0.0	350	13.8	350	15.8
400	5			400	13.8	400	15.8
450	2.8			450	13.5	450	16.5
500	0			500	13	500	16

Table 2: network life time

IDSET		With Attack		Without Attack Existing		Without Attack proposed	
50	100	0	100	100	100	100	100
100	100	50	100	150	100	150	100
150	98	100	90	200	100	200	100
200	90	150	82	250	100	250	100
250	87	200	68	300	100	300	100
300	78	250	28	350	100	350	100
350	55	300	08	400	95	400	100
400	35	350	0	450	92	450	98
450	30			500	78	500	85
500	0			550	50	550	70
				600	20	600	35
				650	0	650	26
						700	15

Table 3: detection ration

IDSET		Without Attack proposed	
5	0.8	5	1.0
10	0.82	10	1.02
15	0.9	15	1.05
20	0.92	20	1.09
25	0.88	25	1.00
30	0.9	30	1.50
35	0.93	35	1.93
40	0.9	40	1.95
		45	2.00

V.CONCLUSION AND FUTURE WORK

Intrusion prevention mechanisms, such as authentication, key management, security, routing protocols, and so on, can stop the deceptive attacks launched by external attackers, but it is difficult to confront the DOS attacks which have stronger concealment and destructive power and difficult to confront the deceptive attacks launched by captured node, these attacks must be found and handled through intrusion detection mechanism. In this paper, an intrusion detection method based on Energy Trust in wireless sensor networks is proposed. It is based on the prediction of energy consumption and increased the correlation calculation of energy consumption to evaluate the security state of nodes. In this work a new technique is being proposed in this research work that is used for energy trust technique in wireless network for hybrid DoS and other attacks. To design Hybrid Energy Efficient data transmission using BS and CH on WSN and analyze the result being obtained with different parameters like Network lifetime, Network throughput and Detection ratios. In this research work network life time is 98, throughput is 16.5 and detection ratio is 1.0 that is calculated in this work.

In the future work other different types of network attacks are prevented with the help of different protocols and different techniques. It is also further implemented with the help of other tools like data mining or NS3 with the help of different algorithms like C4.5, decision tree etc.

REFERENCES

[1] A.Anna lakshmi, Dr.K.R.Valluvan "A survey of Algorithms for Defending MANETs against the DoS Attack," International Journal of Advanced Research in Computer Science and Software Engineering, vol.2, Issue 9, pp.155-164, Sep 2012.
[2] Akash Mittal, Prof. Ajit Kumar Shrivastava, Dr. Manish Manoria "A Review of DOS Attack and its Countermeasures in TCP Based Networks" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.
[3] Antonio Challita, Mona El Hassan, Sabine Maalouf, Adel Zouheiry," A Survey of DDoS Defense Mechanisms, "The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.
[4] Anurekha, R.,K. Duraiswamy, A. Viswanathan, V.P. Arunachalam, K. Ganesh Kumar, A. Rajivkannan" Dynamic Approach to Defend Against Distributed Denial of Service Attacks Using an Adaptive Spin Lock Rate Control Mechanism," Journal of Computer Science, pp.632-636, 2012.
[5] Christos Douligeris and Aikaterini Mitrokotsa, "DoS Attacks And Defence mechanisms: A Classification," in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, (ISSPIT'03), pp. 190-193, Dec 2003.
[6] Darshan Lal Meena, Dr. R. S. Jadon " Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches" International Journal of Advance Research in Computer Science and Management Studies , Volume 2, Issue 4, April 2014.
[7] Divya Kuriakose,V.Praveena "A Survey on DDoS Attacks and Defense Approaches" International Journal of Innovative Research in Computer and Communication Engineering ,Vol. 1, Issue 8, October 2013.
[8] Elinor Mills, "Radio Free Europe DOS attack latest by hactivists," Online at http://news.cnet.com/8301-10784_3-9933746-7.html, CNET News, May. 2008.
[9] Guangsen Zhang, Manish Parashar,"Cooperative Defense against DDoS Attacks," Journal of Research and Practice in Information Technology, pp.1-6, 2006.
[10] Guangsen Zhang, Manish Parashar,"Cooperative Defense against DoS Attacks," Journal of Research and Practice in Information Technology, pp.1-6, 2006.
[11] Haining Wang Cheng Jin Kang G. Shin" Defense Against Spoofed IP Traffic Using Hop-Count Filtering," Networking, IEEE/ACM Transactions on Networking, vol. 15, pp 1-13, 2007.
[12] J. Amudhavel, V. Brindha, B. Anantharaj "A Survey on Intrusion Detection System: State of the Art Review" Indian Journal of Science and Technology, Vol 9(11), DOI: 10.17485/ijst/2016/v9i11/89264, March 2016.
[13] Liang Hu, Xiaoming Bi, "Research of DDoS Attack Mechanism and Its Defense Frame,"Computer Research and Development (ICCRD), 3rd International Conference, pp. 440–442, March 2011.
[14] Monika Sachdeva, Gurvinddr Singh, Krishnan Kumar, Kuldip Singh, " A comprehensive Survey of Distributed Defense Techniques against DoS Attack," International Journal of Computer Science and Network Security, Vol.9, No.12, pp.7-15, Dec 2009.
[15] Nisha H. Bhandari, "Survey on DoS attacks and its detection defense approach," International Journal of Science and Modern Engineering,Vol.1, Issue.3, pp.67-71, Feb 2013.
[16] Puneet Zaroo," A Survey of DoS attacks and some DoS defense mechanisms," Advanced Information Assurance (CS 626), 2003.
[17] Raksha Upadhyay, Uma Rathore Bhatt, Harendra Tripathi "DOS Attack Aware DSR Routing Protocol in WSN" International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015.
[18] Robert Vamosi, "Study: DoS attacks threaten ISP infrastructure," Online at http://news.cnet.com/8301-1009_3-10093699-83.html, CNET News, Nov. 2008.
[19] S. Vimala,Dr. V. Khanna,Dr.C.Nalini "A Supervised Learning Approach Using Support Vector Machine For Intrusion Detection System In Manet" International Journal of Pure and Applied Mathematics Volume 117 No. 21 2017, 947-952.
[20] S.A.Arunmozhi, Y.Venkataramani,"DoS attack and Defense in wireless ad-hoc Network," International Journal of Network Security & Its Applications Vol.3, No.3, pp.182-187, May 2011.
[21] Saurabh Ratnaparkhi , Anup Bhange " Protecting Against Distributed Denial of Service Attacks and its Classification: An Network Security Issue" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013
[22] Shenam Chugh, Dr. Kamal Dhanda " Denial of Service Attacks" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 8, August 2015
[23] Wei Ren, Dit-Yan Yeung, Hai Jin, Mei Yang, "Pulsing RoQ DoS Attack and Defense Scheme in Mobile Ad Hoc Networks," International Journal of Network Security, Vol.4, No.2, pp.227-234, Mar. 2007.
[24] Xie Jinhu , Tao Yang, Yang Feiyue "Intrusion Detection System for Hybrid DoS Attacks using Energy Trust in Wireless Sensor Networks" 8th International Congress of Information and Communication Technology (ICICT-2018), Procedia Computer Science 131 (2018) 1188–1195.