International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-4)

Research Article | **April 2014**

UHCF: Updated Hop Count Filter Using TTL Probing and Varying Threshold for Spoofed Packet Separation

Mr. Govind M Poddar
Research Scholar, Dept. of CSE
JDCT, Dhar Road
Indore (M.P), India

Mr. Nitesh Rastogi
Asst. Prof & Head,Dept. of CSE
JDCT, Dhar Road
Indore (M.P), India

Abstract-

Ad-Hoc network supports short duration communication which establishes connection for limited time period only and later on gets terminated. In such network mobility is termed as key issues because the topology of network is continuously changing. MANET is a well known example of these ad-hoc category in which each node will works as a router for transmitting information. These networks suffer from various issues related to performance, complexity and security. As the users need is growing day by day the security phenomenon is also getting denser. IP Spoofing is the one of the known category in which the original packet gets maliciously affected by attacker's node somewhere in the network. Now the aim is to detect this affected spoofed packet from normal traffic. This discrimination is provided by tradition protocols using Hop Count Filter (HCF) mechanism. It calculates the difference of current and initial TTL values of operating systems port. The existing HCF mechanism will only measures the maximum TTL length value up to 30 which is an assumption. It can be larger than that and even multiple routes is also feasible for transmission. Hence this situation is not taken and hence there solution is not available with existing approaches. Even the approaches are not measured computationally as an effective and light weight.

This paper proposes a novel Updated Hop Count Filtering (UHCF) mechanism using probing and variable threshold for accurately measuring the affected packets from the normal traffic. Somewhere at the initial stages the work is proving its efficiency and giving better results which later on prove its authenticity and accuracy.

***IndexTerms*—MANET, IP Spoofing, DDoS (Distributed Denial of Service), TTL (Time-To-Live), UHCF (Updated Hop Count Filter), (VT) Varying Threshold;**

I. INTRODUCTION

Intrusion detection system is the mechanism for detecting the unconventional traffic form the network which is degrading the performance or performing the unnecessary data losses. They analyses users activities from source, destination or some networked devices and updates their traffic summaries which lets the network drops in near future. In MANET is play a crucial role because in this the node movements makes the rapid changes in networking topologies from which measuring the authenticity of data and nodes is a critical issue. Mainly the network is attacked by different types of attack and their removal is planned in such systems. Their primary aim is to provide security and assures data availability, confidentiality and integrity for continuity in data transmission. The general categorization of intrusion detection system is of two categories: misuse detection and anomaly detection and deployed as a network based system or a host device based system [1].

Among the most massive affected category IP spoofing has been exploited mot by denial of service (DoS) attacks and Distributed Denial of Service (DDoS) attacks. They deals with flooding traffic and analyses them and let the service rejected. IP spoofing is normally associated with malicious activity which blocks legitimate access. It occupies the resources and denies the actual request from transmission. Thus the ability to clarify the spoofed IP packets from the legitimate ones at senders or receivers is taken as avoiding mechanism. Most of the time the attacker can falsify the senders or receivers information by modifying the number of hops (Hop Count) by which packet is unable to reach its destinations node. This hop count information is taken in the form of its TTL (Time to Live) values available in IP Header. Here a mapping is performed from its TTL value to its IP Header and Hop Counts [2]. Thus servers may distinguish the actual data and spoofed packet by analyzing the difference in hop count values.

To apply the above detection of difference in TTL field various methods is been proposed over the last few years. These methods are totally based on measuring the hop count values and designing the filters in accordance to that so as to identify the misbehaving nodes with spoofed packets. This function is called as Hop Count Filter (HCF) [3]. The inclusion of the TTL value is also a potential vulnerability as intermediate node will not forward packets if the TTL value in a received packet is 1 or less. Since the TTL mechanism is not protected, a malicious node could reduce the TTL in received packets to an artificially low value [4]. Result of which packet may not reach to its destination address and cause successful execution of DoS category of attacks. This paper gives a novel approach of performing this filtration

using Updated HCF function as suggested with the help of some novel assumption which is not taken over by previous researchers.

II. BACKGROUND

Examining the type of attack required the analysis of its affects as per the communication is needed. The traditional route discovery Hop count filtering is the validation of source IP address of packets which is passing through routing devices. The malicious node aims at disrupting the actual operations of the routing protocols and denies the network services. They usually modify the sensitive information for triggering the attack events. Attacks are mainly involved in routing mechanism and analyze the packets passing through network. The categorization of most of the attacks according to their vulnerabilities and affects are given as:

- Denial of service,
- Modifying the packet header,
- Flooding attacks, and
- Replaying and reordering data packets.

Denial of service attacks include intentionally dropping packets instead of forwarding them and will also interfere the communication of its neighbour nodes. The affect of it is the loose of internal information and malicious behaviour. Thus a better approach would be required to find the actual identity of router without allowing them to participate in data transfers. Also the fabrication and modification of reply packets is preempted for correct route guidance and availability. This is managed by the receivers reply messages or probe messages of acknowledgements. Thus, even though the attacker can launch the directed attack due to the lost of acknowledgment packets, the sender and receiver can continue the communication by reinitializing the protocol [5].

Spoofing is the intentional reading or updations of actual packet for some attack triggering. IP spoofing is based on spoofed information of IP Header to apply the various attack categories like DoS attacks. It varies from complex algorithms to light weight calculations based on TTL Fields. The hop count field is indirectly related to the Time to Live (TTL) field of the IP Header. The existing mechanism works at the receiver end where the Time to Live (TTL) value can be inferred and can check for consistency. If the TTL field gives different values for different packet in a single session then irregularity prevails and one cansuspect of an intruder attempting to make connection with the receiver.

TTL Value-Based Features

Time to Live (TTL) measures the total number of Hops required to traverse from source to destinations. For multicast routing it should be more than a specific range limit of Nodes. For normal single it path it is near about 30. It specifies how long the corresponding response for a domain name should be cached in the network. Setting lower TTL values is useful for the attackers. Below is some of the TTL conditions [6]:

- Average TTL {simple TTL average, used in various detection methods.
- Standard deviation of TTL.
- Number of distinct TTL values.
- Number of TTL changes.
- Percentage usage of specific TTL ranges {malicious traffic tends to set their TTL values to lower values}

Hop Count Filter (HCF) is based on this TTL calculation and runs in two states. In the learning state, HCF watches for the abnormal TTL behavior without discarding any packets. On detection of an attack, HCF switches to the filtering state, where it discards those IP packets with mismatching hop counts [7]. The aim of this work is to design novel HCF mechanism having updated fields to handle existing issues. Thus some new mechanism is required for better results and on the basis of which some new criteria is required.

III. RELATED STUDY

The existing work contains the various problems related to security and data drops. Out of those a large numbers of authors had worked with packet dropping and suggest numerous techniques to overcome those. Mainly the developed mechanism till now suffers from the problem related to higher computational time and low detection rate of illegitimate packets. Likewise the approach given in the paper [8], in which the author proposed a Distributed Probability based Hop Count Filtering using RTT (DPHCF-RTT) technique to improve the above said limitations by maximizing the detection rate of malicious packets and reducing the computation time. The given approach has some of the positive aspects for resolving the bandwidth issues and resource consumption using Round Trip Time (RTT). This inclusion of RTT provides useful information which improves the efficiency of probabilistic DHCF technique which totally depends on Hop Count. The result of proposed scheme is proven through its significant detection rates.

Carrying forward the above suggested concept of HCF and RTT some of the authors had h\give more secure mechanism against each and every communication mechanism. This can be achieved by using covert channel. Thus, the paper [9], gives a novel covert channel inside the IP header's Time to Live (TTL) field. In this the sender can updates or change the TTLs of consequent packets transmitting covert information to the receiver side. Now for improved security this TTL updating information needs to analyze effectively for early and accurate detection. The author had also

discussed methods to eliminate and detect this covert channel through a novel IP header's Time to Live (TTL) field. Early calculations and identification proves the authenticity and efficiency of suggested approach.

Now after the above consideration the packet level analysis and monitoring is an compulsory act for more security. This ability to filter spoofed IP packets nears the users server gives an evolutionary approach for DDoS attack identification. The aim is to watch IP Header and time related fields to calculate the hop counts.An attacker can update any field of IP Header but he cannot modify the hop count filed up to destinations. More importantly, since the hop-count values are diverse, an attacker cannot randomly spoof IP addresses while maintaining consistent hop-counts. Based on this observation, the paper [10] present a novel filtering technique, called Hop- Count Filtering (HCF)—which builds an accurate IP-to-hop-count (IP2HC) mapping table—to detect and discard spoofed IP packets. HCF is easy to deploy, as it does not require any support from the underlying network.

In the paper [11], the author gives a approach for detecting packet mishandling in MANET. In this a solutions is given using an unobtrusive monitoring technique to identify and locate the malicious packet dropping from attacker's node.The approach utilizes the information from different network layers to detect malicious activity as a result of trace processing. Any single node can use above suggested unobtrusive monitoring without relying on cooperation from other nodes which make its implementation an easy task. The technique can be used to detect Byzantyne faults such as dropping or misrouting packets and giving better results than any existing approach.

Some of the papers had also focused their intensions towards the reputation based techniques as suggested by [12] for wireless mesh networks which avoids the routes selections. It uses link state routing with a trusted gateway for performing the computations of node trust value for the routers. The computation of the Node Trust Values is based on packet counters maintained in association with each route and reported to the gateways by the routers in repetitive process through a feedback mechanism having limited scope flooding scenario. Later on the new aggregate trust value of the router determines the probability with which that router is kept in the topology graph used for route identification. The results show the proposed mechanism can be able to detect misbehaving routers reliably, and thanks to the feedback and the exclusion of the accused nodes from the route selection which decreases the drop ration and increases the route length.

The above approach is later on extended by the author's approach in [13] given as Securing pAcket Forwarding in ad hoc nEtworks (SAFE)which addresses the malicious packet dropping problem using a trust model based reputation concept. It provides two main primary functionalities:

(i) Monitoring the behaviour of the neighboring nodes in the network and
(ii) Computing their reputations values based on the information provided by the monitoring.

It also discusses in details how the reputation information is managed within the network in an effective manner. The authors had also evaluated the proposed approach on various network parameters. At the initial level of work the approach is detecting the packet level frauds.They were continuously monitoring the behavior of each other for identification of intruder's node.

Spoofing can also be used to detect the malicious IP packets and addresses. Hence some mechanism needs to be designed so as to improve such packet dropping situations and hacking. Thus in the paper [14] a novel mechanism is proposed which give a technique to identify traffic verification and filtering. The proposed system is capable of monitoring the network and its traffic to detect any misbehaviour of uneven activities. IP Spoofing is incomplete without port scanning of the servers. The Port Scanning identifies whether all ports are active at a particular time and can validate the existence of an attack with the packet tracing feature. The suggested technique can be applied for host as well as network also and gives te good results at both the end.

Thus HOP Count and TTL counts will play a very important identification role for DDoS analysis and intruders identifications. As given in the paper [15], focuses on the methodology for modeling a DDoS UDP flood with an IP spoofing attack and hop count defense using OPNET Modeler network simulation software. The authors use counting mechanism of probe messages of originators node which attempts to discover the actual hop distance. Both the probe and probe reply messages carry no data except for the IP header. It uses the protocol field in the IP header to identify the probe and probe reply messages. The actual hop distance to the source node is computed as being equal to 255 minus the value of the TTL field in the probe reply message.

After analyzing the various works the this paper will discusses some of the concerns points required and will take Hop Count and TTL entry as a base of designing new mechanism to reduces the packet drops due to malicious devise or attackers. It gives an preemptions and recommendations that an Internet server can easily infer the hop-count information from the Time-to-Live (TTL) field. The above field sis from IP Header and detection of which server can differentiate the Spoofed IP Packet from the legitimate user or node.

IV. Problem Identification

After studying the different research papers it is identified that Denial of service (DoS) and Distributed DoS (DDoS) is a well known type of attack and affecting the market regularly causes the huge amount of data losses due to their Spoofed packets. These malware packets affecting the performance of network by forged IP addressing. It comes under the IP Spoofing attacks in which the devices is unable to make discriminations between the actual packet (legitimate) and the spoofed (malware) packet. Although, an attacker can forge any field in the IP header,he cannot falsify the number of

hops an IP packet takes to reach its destination.It is solely determined by the Internet routing infrastructure. The hop-countinformation is indirectly reflected in the TTL field of the IP header, since eachintermediate router decrements the TTL value by one before forwarding it tothe next hop.Previously anti-spoofing mechanism HCF (Hop Count Filter) is being developed which is providing great results is various cases. But as of now the usage of internet is increasing and hence the load on devices and routes is also getting denser, this detection mechanism is been affecting from various other issues. The HCF works on the basis that the attacker cannot misrepresent the Hop count (HC), the number of hops an IP packet takes to reach the destination.

*Scenario of Attack:*Due to various surveys and works on HCF designs and mechanism it is been found that most of the time the value of TTL is in between 30 for all the routes. This value is reducibility changed but not more than the maximum limit. According to the observations of [16], some IP packets have an abnormal time-to-live (TTL) value that is decreased by more than 30 increments from the initial TTL. These packets are likely to be generated by special software. It assumes that IP packets with strange TTL values are malicious.

This HC value can be inferred from the TTL(Time to Live) field in the IP packet. However, the working of HCF hasthe following problems which remain unsolved [17]:

(i) Multiple path possibility is ignored.
(ii) The method of building the HC tables must be more secure.
(iii) Lack of good renews procedure which can detect network changes.
(iv) Less number of packet filtration and verification after prelim filter functions so as to reduce computation cost [18].
(v) Light and Easy detection for less overhead.

Thus all the above problems are unsolved and open the area of work for various researchers. Out of those this work is getting its concern deeper about designing the updated HCF mechanism which is lighter in computational load and size. The suggested approach will improves the quality ofservice of the network by minimizing the number of false positives.

V. PROPOSED WORK

This paper gives a novelmethod for detecting malicious packets by observing their time to live (TTL) field values and the mapping with internet protocol (IP). It work on simple assumption of maximum time an IP packet passes through less than 30 routing devices to reach the destination nodes. However this is not in each case, sometimes the TTL value may exceeds more than 30 because of multicast routes or some long routes. In such cases the existing HCF methods are unable to consider those cases and the detection of spoofed packet is misguided. The key concern about taking the HCF method is that TTL value reflects the total number of hops a data had to pass from. Thus taking this as a base thing the suggested approach give a unique solution which improves different issues of existing approaches. It performs the packet discrimination as a legitimate or spoofed.

In this proposed work a novel updated hop count filtering (UHCF) mechanism is proposed which is used to identify the spoofed packet out of numerous legitimate packets. It has four components:

(i) Source Node
(ii) Destination Node
(iii) Network
(iv) Updated Hop Count Filter (UHCF) Mechanism

Whenever source wants to assess the authenticity of any packets then it initiates the verification modules. Initially source wants to communicate with the destinations node then it checks its routing table. It the entry is found then TTL field is updated in initial message. If the entry is not found then it as sends the Multicast Probe RREQ message to destination. Destinations reply with its IP Address, mapping and required details in Probe RREP message. This entry of multicast route is getting updated in routing table. Total number of hops is the number of devices traversed during this data communications. A timer counter is attached with probe message so as to get the validity on time which verifies the route existence.

Each device reduces the TTL value by 1 when a packet is transferred from it to any other device. Now the hop count table is created at source end. Now the filtering is applied according to which hop count is calculated as current measured TTL value is subtracted from initial TTL value. Here Initial TTL value is taken from the OS service port number which is fixed (Seen from the Table-I). Now the filter selects the TTL value from the table which is just above the measured value.

Hop Distance to Source Node= 255 (Default Initial Value or Passed form Table-I)-Current TTL Value

The hop count of received packet is calculated as t_0-t. After the hop count is calculated then the path is checked by condition:

Check Path Length (TTL of Stored Hop Count Calculated by Probe Message- TTL of Measured Hop Count by Current Message) = Variable Threshold Value (0 to Number of Multicast Path) &&<=30;

This condition is verifying the TTL value in which if the differentiated value is lesser than 30 than it is a legitimate route. But in some cases route can of more hops than an average variable threshold is also calculated which lies in between each hops of multicast path. So if the multicast reply came then this condition gets activated which should be above a threshold. From this multipath solution to larger hops is also feasible form up[dated HCF mechanism. Now if the

above condition is found to be correct than the packet is taken as a legitimate packet of else it is a spoofed packet. This information is then forwarded to each neighbor so that routing table and HCF value is updated at each nodes and devices.

TABLE I: OS PORT BASE INITIAL TTL VALUE

OS	Protocol	Initial TTL
Linux 2.4 kernel	ICMP	255
BSDI BSD/OS 3.1 and 4.0	ICMP	255
Windows Server 2008	TCP, UDP, ICMP	128
Windows7	TCP, UDP, ICMP	128
Windows XP	TCP, UDP, ICMP	128
Linux RedHat 9	TCP, ICMP	64
FreeBSD5	ICMP	64
MacOS X (10.5.6)	TCP, UDP, ICMP	64
AIX	TCP	60

The proposed approach is capable of identifying the spoofed packet out of larger number of normal packets. Now the task is to improve the accuracy of approach. For than various experiments is been performed on which regular results is generating. At the primary level of this research the approach seems to provide better results than any existing approaches.

VI. APPLICATIONS AND OUTCOMES

As the proposed approach beeng implemented, lots of As the proposed approach gets implemented, lots of benefits and integration availability with existing security mechanisms can be make available to network. Detection and prevention approach uses in wide domain of network uses.

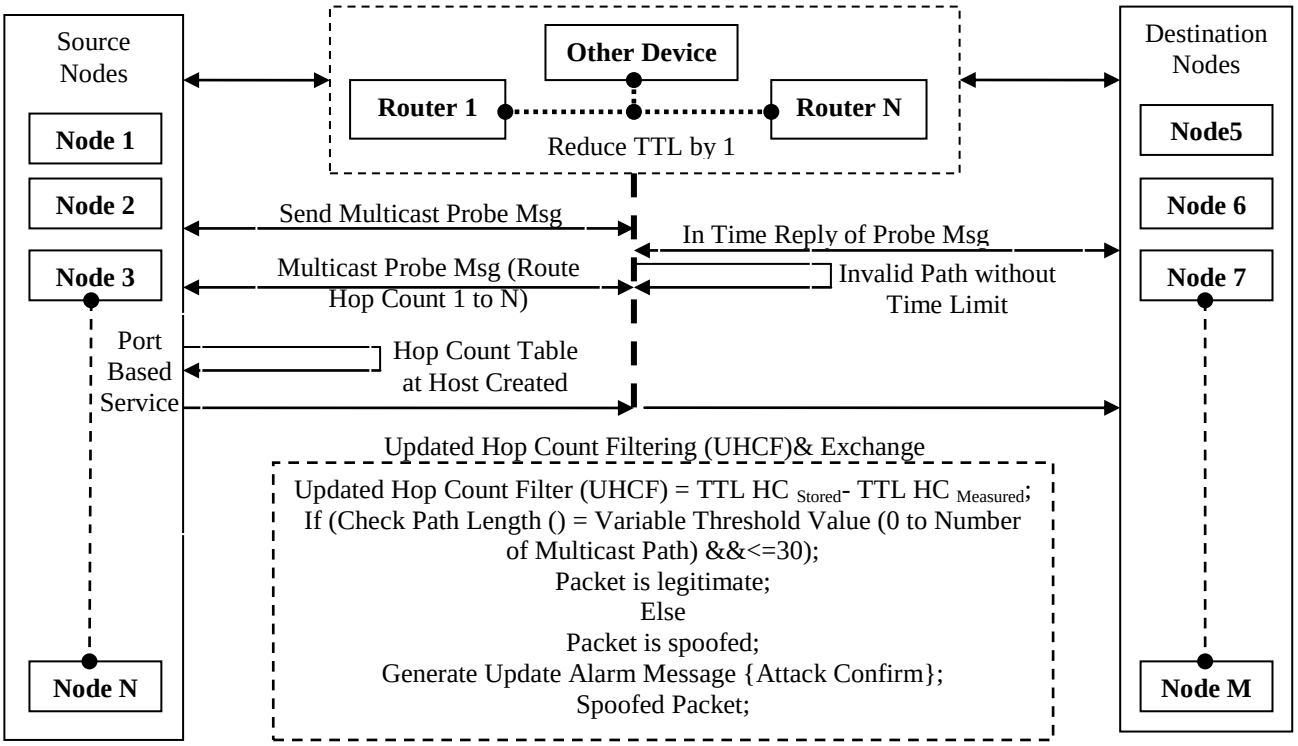

FIGURE 1: UPDATE HOP COUNT FILTER (UHCF) BASED SPOOF PACKET IDENTIFICATION

Some of them described as: Fraud detection and investigation, Filtering and monitoring company network activities, Social network and on banking sector which is most demanded thing today. Primarily the work categorizes itself in the area of IP Spoofing in MANET. IP spoofing is commonly associated with malicious network activities, such as

Distributed Denial of Service (DDoS) attacks which block legitimate access by either exhausting victim servers or saturating stub networks access links to the Internet.Using a mapping between IP addresses and their hop-counts, the server can distinguish spoofed IP packets from legitimate ones. Based on this observation, a novel filtering technique, called Hop-Count Filtering (HCF)which builds an accurate IP-to-hop-count mapping table to detect and discard spoofed IP packets is presented here.

After the implementation and experimental analysis of approach, various relevant results will be expected.

- The system is resistant to Distributed Denial of service attack (DDoS), Replay attack and blind spoofing.
- Enhanced malicious routing packets detection approach
- Prevents networks from misbehaviour activity.
- Offers fraud detection and investigation in the network
- Improves the lifetime of the network.
- Imrpoved detection rates
- Early detection with numerosity
- Less Overhead

VII. Performance Evaluation Factors

To analyze the result of proposed approach actual network traffic needs to be monitored according to designed experiments. It should contain the traffic movement having large number of legitimate and malicious traffic. Out of the all identified factors port numbers, TTL values, behaviour of packet had to calculate and the quantity of alert generated at the normal and abnormal traffic. Packets are measured and analyzed on the suggested parameters from which traffic categorization can be made as Normal or Abnormal.

- *Port numbers:* well-known port numbers are more likely to be used in malicious connection attempts.
- *TTL values:* It measures between the initial value (*t0*) and a value that has been reduced by 30 increments (*t0 – 30*).
- *Packet Behaviour:* They are produced by popular OSs and classified as *normal*. If a packet has a TTL value less than *t0 – 30*, it is classified as an *abnormal* TTL.
- *Number of Alerts per Traffic Type:* It is the number of alerts generated when the traffic is normal and when it is showing some malicious or intruders behaviour.
-

VIII. Constraints & Assumptions

At this level of work the research is not complete. The authors are working on the real implementation and are clear that in near future the approach is quite effective while detecting intruders at very early stages of data transfer. Initially the simulation environment is considered is getting better result than existing approaches.

IX. Conclusion

In this work a novel Updated Hop Count Filtering (UHCF) method is proposed overcome the issues generated due to inferred and spoofed IP packets. The designing of HCF filtering function follows the conditions of discriminations of actual packets from the spoofed packets. The suggested approach is capable of identifying the DDoS attacks and its variants at the early stages of data transfers and hence reduces the probability of losses and attacks occurrences. The approach is taking TTL considerations as a key parameter for work and improves the existing problems such as multicast routes, fabrications etc. Here the hop count value is the difference of final TTL value and initial TTL value. But at this point few of the issues remains unsolved whose solution is been suggested by the proposed approach. At the initial level of work the approach seems to be capable of detecting Spoofed IP packets with higher accuracy and lower computational complexity.

Future Work

Some problems and concepts that remain unaddressed can be performed in future. This system can further be extended to implement HCF in real-time networks where it has to deal with real-time requests.Such as with the help of pre-emptive approach more information can be added for exact timely analysis of intrusion, more conditional UHCF, lower overheads with high accuracy. We are also working towards embedding the developing source code of our proposed scheme in NS2. In our proposed scheme so as to use the benefits of approach like open source.

Acknowledgment

This research work is self financed but recommended from the institute so as to improve the security breaches with current techniques in MANET using IDS, HCF and TTL work. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. The authors also wish to acknowledge _____administration for their support & motivation during this research. They also like to give thanks to Mr. _____& Dr._____for discussion regarding the situational awareness system & for producing the approach adapted for this paper.

References

[1] C. Jin, H. Wang and K.G. Shin, "*Hop-Count Filtering: An Effective Defense against Spoofed DDoS Traffic*", in ACM, doi: 1581137389/ 03/0010, Oct 2003.

[2] S. S. Rana1 and T. M. Bansod, "*IP Spoofing Attack Detection using Route Based Information*", in International Journal of Advanced Research in Computer Engineering & Technology, ISSN: 2278 – 1323, Volume 1, Issue 4, June 2012.
[3] P. W. Wah, S. Hu and C. J. Mitchell, "*Malicious attacks on ad hoc network routing protocols*", in Royal Holloway, University of London.
[4] B. R. Swain and B. Sahoo, "*Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method*", IEEE International Advance Computing Conference (IACC 2009, doi: 978-1-4244-1888-6/08/, 2008.
[5] P. Sanjeevi, M.K.Nallakaruppan and U. Senthil Kumaran, "*Detection of Denial of Service attacks on Mobile Internet Protocol Nodes*", in IJARCSSE, ISSN: 2277 128X, Volume 3, Issue 5, May 2013 .pp 214-217
[6] E. K. John and S. Thaseen, "*Efficient Defense System for IP Spoofing in Networks*", in ICAIT, doi: 0.5121/csit.2012.2416, 2012. Pp 185-193
[7] V. Keermic, "*Inspecting DNS Flow Traffic for Purposes of Botnet Detection*", as GEANT3 JRA2 T4 Internal Deliverable, 2011.
[8] R. Maheshwari and Dr. C. R. Krishna, "*Mitigation of DDoS Attacks Using Probability Based Distributed Hop Count Filtering and Round Trip Time*", in International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 7, July – 2013.pp 1135-1140
[9] S. Zander, G. Armitage and P. Branch, "*Covert Channels in the IP Time To Live Field*", in Swinburne University of Technology.
[10] H. Wang, C. Jin and K. G. Shin, "*Defense against Spoofed IP Traffic Using Hop-Count Filtering*", IEEE/ACM Transaction of Networks, doi: 10.1109/TNET.2006.890133, Volume. 15, No.. 1, Feb 2007. Pp 40-53
[11] S. Medidi, M. Medidi and S. Gavini, "*Detecting Packet Mishandling in Mobile Ad-hoc Networks*", in Washington State University, NSF Grant number CNS 0454416.
[12] A. Gergely, L. Buttyan, and L. Dora, "*Misbehaving Router Detection in Link-state Routing for Wireless Mesh Networks*", in IEEE Transaction, doi:978-1-4244-7265-9/10, 2010.
[13] Y. Rebahi, V.E Mujica, C. Simons and D. Sisalem, "*SAFE: Securing pAcket Forwarding in ad hoc nEtworks*", at Fraunhofer Fokus, Berlin, Germany.
[14] S. J. Templeton, K. E. Levitt, "*Detecting Spoofed Packets*", in DARPA IA&S Grant number:30602-00-C-0201, Department of Computer Science U.C. Davis.
[15] S. Akhter, J. Myers, C. Bowen, S. Ferzetti, P. Belko, and V. Hnatyshin, "*Modeling DDoS Attacks with IP Spoofing and Hop-Count Defense Measure Using OPNET Modeler*", in Department of Computer Science, Rowan University.
[16] R. Yamada and S. Goto, "*Using abnormal TTL values to detect malicious IP packets*", in Proceedings of the Asia-Pacific Advanced Network (APAN), ISSN 2227-3026, doi:10.7125/APAN.34.4 ,Volume 34, 2013.p. 27-34.
[17] S. Lagishetty, P. Sabbu, and K. Srinathan, "*DMIPS - Defensive Mechanism against IP Spoofing*", in Springer-Verlag, ACISP, Berlin Heidelberg, 2011. pp. 276–291,
[18] R. Chen, J. M. Park and R. Marchany, "*TRACK: A Novel Approach for Defending Against Distributed Denial-of-Service Attacks*", as Technical Report TR-ECE-06-02, Dept. of Electrical and Computer Engineering, Feb. 2006.