ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2014

Performance Evaluation of UHCF Using TTL Probing for Packet Spoofing Detection in MANET

Govind M. Poddar[1], Nitesh Rastogi[2]

PG Student, Dept. Of CSE, M.P., India [1]

Assistant professor, Dept. of CSE, JDCT, Indore, M.P., India [2]

ABSTRACT: Now days various types of network came into existence which supports medium based communication such as wired and wireless. Among them the network which works for temporary basis and gets disconnected after the time limit or connection expires. Ad hoc network supports short durational connection between movable nodes and gets terminated after the communication is over. Mobile ad-hoc network is one of the ad-hoc network having movable nodes communicating with the help of mobility aware routing protocols without any infrastructural elements such as router or switches. Here the mobile nodes itself serves the functionality of router. These network support dynamic environment and sudden changes which causes various unauthenticated devices and services starts operating in normal environment. It causes degradation in normal performance of the network and their behaviour changes as planned by these attacks. IP Spoofing is known as one of these attack in which the normal packets is gets changed or affected by some attacker's packet in network. Quantity of this spoofed packet somewhere had been lost in normal traffic and the detection methodologies needs to make a clear separation between normal and spoofed traffic. The above functionality is achieved by some traditional methods works on the concept of Hop Count Filter (HCF) mechanism. But the traditional HCF method only measures the TTL maximum up to 30 hops limit and the packet coming from larger hops will be taken to be spoofed but it was not the case all the time. Sometimes actual packet might come from more hops. Its solution is been drafted as UHCF (Updated Hop Count Filtering) mechanism suggested in [19]. Along with some modification this paper presents a complete evaluation of suggested approach and will also presents a comparison of the approach with existing mechanisms.

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

I. INTRODUCTION

Network is divided by its type of communication supported qualities i.e. wired or wireless medium. In wired communication, the network is dependent on fixed devices and locations of operations while the wireless communication is location free motion aware technology. Taking the device mobility as primary factor, now a day's different network gives distinctive utilities to end users. The system works as per their transmission medium like radio waves which is a short extend waves differing from 10 to a few 100s of meters/km. These are GSM, MANET, WSN, Bluetooth, Zigbee and so forth. A wireless mobile ad hoc network is formed by a group of mobile hosts that communicate through radio transmissions, without support of fixed routing infrastructure. Because of its simplicity of arrangement, it has a lot of requisitions in military and also in citizen situations.

These system which fills in as a short term communication for information exchange goes under the class of Ad-hoc systems. The ad hoc networks have been on the research desk for a long time but have recently gained more attention. The proliferation of a variety of wireless access technologies, flawless connectivity and everywhere, anytime computing are commonly used as the paradigms for serving mobile network users. Further, broadband wireless access is described as the panacea for the last-mile problem. While the vision of seamless connectivity and broadband wireless internet access is attractive, it is far from reality. For different administrative, specialized and efficient reasons, wireless access systems overall fails to satisfy the guarantee of constant, high-transmission capacity, and moderate administration.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2014

Interruption recognition or intrusion detection frameworks are the instrument for distinguishing the capricious activity structure and abnormal traffic which is degrading the systems executions or performing the unnecessary information misfortunes. They examines clients exercises from source, objective or some organized gadgets and redesigns their activity synopses which lets the system drops in not so distant future. In MANET is assume a vital part on the grounds that in this the hub developments rolls out the quick improvements in systems administration topologies from which measuring the legitimacy of information and hubs is a basic issue. Mostly the system is assaulted by diverse sorts of assault and their evacuation is arranged in such frameworks. Their essential point is to give security and guarantees information accessibility, secrecy and respectability for progression in information transmission. The general classification of intrusion detection and removal system is of two classifications: misuse detection and anomaly detection. They are deployed as a network based system or a host device based system as suggested by [1].

II. BACKGROUND

Considering the intruder's behaviour the most exploited attacks in this category is IP Spoofing. In this the normal traffic is maliciously modified by entering some diverging packets and the actual content of these packets might be modified. Now after these packets came into action of desiring events and actions the formal request or responses gets affected and starts denying the service. It also came into the category of the denial of service attacks. They manage flooding activity and dissect them and let the administration rejected. IP parodying is regularly connected with malevolent action which pieces real get to. It involves the assets and denies the genuine solicitation from transmission. Accordingly the capacity to illuminate the ridiculed IP bundles from the honest to goodness ones at senders or collectors are taken as evading system. More often than not the assailant can adulterate the senders or recipients data by changing the amount of jumps (Hop Count) by which parcel is not able to achieve its goals hub.

This jump include data is taken the type of its TTL (Time to Live) values accessible in IP Header. Here a mapping is performed from its TTL worth to its IP Header and Hop Counts [2]. In this manner servers may recognize the real information and the spoofed packet by analytically evaluating the difference in hop count values of normal condition. To achieve this functionality the function implemented or designed is known as hop count filter (HCF) [3]. But there are some issues which need to be resolved for complete solution. 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.

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 [5]. 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 can suspect of an intruder attempting to make connection with the receiver. 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.

The objective of this work is to generate a lightweight scheme that validates incoming network data packets at an mobile gateways without using any cryptographic methodology or router support. The objective is not to achieve perfect authentication, but to screen out most bogus traffic with little collateral damage. The fundamental idea is to utilize inherent network information—that each packet carries and an attacker cannot easily forge—to distinguish

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2014

spoofed packets from legitimate ones. It can be modelled as a problem of multi-commodity flows and easily be implemented. Simulation results show that the algorithm has a better performance and will provide an effective solution for realizing multimedia applications in mobile network.

III. RELATED STUDY

The current work holds the different issues identified with security and information drops. Out of those an expansive amounts of creators had worked with bundle dropping and propose various methods to defeat those. Principally the created component till now experiences the issue identified with higher computational time and low recognition rate of illegitimate parcels. Moreover the methodology given in the paper [8], in which the creator proposed a Distributed Probability based Hop Count Filtering utilizing RTT (DPHCF-RTT) strategy to enhance the above said limits by boosting the identification rate of malevolent bundles and diminishing the processing time. The given methodology has a portion of the positive perspectives for determining the transmission capacity issues and asset utilization utilizing Round Trip Time (RTT). This incorporation of RTT gives valuable data which enhances the effectiveness of probabilistic DHCF procedure which completely relies on upon Hop Count. The aftereffect of proposed plan is demonstrated through its huge recognition rates.

Convey forward the above recommended idea of HCF and RTT a portion of the creators had h\give more secure system against every single correspondence component. This could be attained by utilizing secretive channel. Accordingly, the paper [9], gives a novel secretive channel inside the IP header's Time to Live (TTL) field. In this the sender can upgrades or change the TTLs of subsequent parcels transmitting clandestine data to the collector side. Presently for enhanced security this TTL upgrading data needs to break down successfully for right on time and precise recognition. The creator had additionally talked about systems to dispense with and locate this clandestine channel through a novel IP header's Time to Live (TTL) field. Early figuring's and ID demonstrates the realness and productivity of recommended methodology.

Presently after the above thought the parcel level dissection and observing is a necessary represent more security. This capacity to channel satirize IP bundles nears the clients server gives an evolutionary methodology for Ddos assault distinguishing proof. The point is to watch IP Header and time related fields to compute the bounce tallies. An assailant can upgrade any field of IP Header however he can't adjust the bounce tally documented up to objectives. All the more significantly, since the jump number qualities are differing, an aggressor can't arbitrarily parody IP locations while keeping up reliable bounce tallies. In light of this perception, the paper [10] present a novel sifting procedure, called Hop- Count Filtering (HCF)—which manufactures an exact IP-to-jump tally (Ip2hc) mapping table—to discover and toss caricature IP bundles. HCF is not difficult to convey, as it doesn't oblige any backing from the underlying system.

The above methodology is later on stretched out by the creator's methodology in [13] given as Securing parcel Forwarding in impromptu systems (SAFE) which addresses the malevolent bundle dropping issue utilizing a trust model based notoriety idea. It gives two fundamental essential functionalities:

(i) Monitoring the conduct of the neighboring hubs in the system and
(ii) Computing their notorieties qualities focused around the data gave by the observing.

It additionally examines in points of interest how the notoriety data is overseen inside the system in a viable way. The creators had likewise assessed the proposed approach on different system parameters. At the introductory level of work the methodology is distinguishing the bundle level fakes. They were persistently observing the conduct of one another for distinguishing proof of gatecrasher's hub.

Caricaturing can additionally be utilized to identify the pernicious IP parcels and locations. Subsequently some component needs to be planned in order to enhance such parcel dropping circumstances and hacking. Subsequently in the paper [14] a novel component is proposed which give a procedure to distinguish activity check and separating. The proposed framework is equipped for checking the system and its movement to locate any bad conduct of uneven exercises. IP Spoofing is inadequate without port checking of the servers. The Port Scanning recognizes whether all ports are dynamic at a specific time and can approve the presence of an assault with the bundle following gimmick. The recommended procedure might be requisitioned have and additionally organize likewise and gives te great results at both the end.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2014

In the wake of examining the different works the paper will talks about a portion of the concerns focuses obliged and will take Hop Count and TTL entrance as a base of outlining new instrument to lessen the parcel drops because of malevolent devise or aggressors. It gives seizures and proposals that an Internet server can without much of a stretch gather the jump check data from the Time-to-Live (TTL) field. The above field sis from IP Header and recognition of which server can separate the Spoofed IP Packet from the true blue client or hub.

IV. PROBLEM IDENTIFICATION

During the last few years issues is addressed using the base of TTL values and hop counts. But still there are some which requires more focus. Let us take a look about the hop count values which is directly or indirectly reflected by the TTL fields of Internet protocol header (IP). Here the interdictory routing devices make the values decrements after forwarding the packet to the next hop. Till the packet reaches its destination this Hop count values gets decremented each time when they are transferred from one node or hop to other. Traditionally there is some anti spoofing mechanism available such as hop count filtering (HCF) scheme. But still there is a case where this method can't work.

Attack Situation

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 has the 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.
(vi)

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 of service of the network by minimizing the number of false positives

V. PROPOSED WORK

The implementation phase of UHCF after suggesting it in [19] involves in the actual construction and installation of a system. It is the process of converting design into an executable software system and gets stucked in different design issues. The work takes several iterations of the model to produce a working program. Implementation also affects the developed system. This work gives a novel method 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.

The updated hop count filtering (UHCF) mechanism is used to identify the spoofed packet out of numerous legitimate packets. It has four components:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2014

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

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. 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.

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.

To implement the desired system first a network is created using nodes and the above defined configurations required to simulate. System contents are the mobile nodes and they are free to perform communication with each other. Every time when Route discovery starts RREQ packets are sent and received by the nodes of the network to their neighbor nodes. First time node sends a RREQ packets to its neighbor node when the node sends a RREP packet to the node sending RREQ packet then first session is created. For implementing the above developed solution NS2 simulator is used and its detailed process wise algorithm is given below.

Algorithm

(i) Send Multicast Probe Message
(ii) Reply Multicast Probe Message (Route Hop Counts 1, Route Hop Count 2,…..Route Hop Counts 3)
(iii) Create Hop Count Table at Hosts (IP Address, Hop Counts, and Low level Interrupts Timers)
(iv) Probe message reply comes in a Time Limit (Path Exist) Else Invalid Path
(v) Apply Hop Count Filtering (Checks Spoofed Packet or Not)
(vi) Hop Count = Initial TTL value - Final TTL value
(vii) Checks Hop Count Based on Ports Service
(viii) Select the Port Number Having respective TTL Minimum Above Larger Value from the Current TTL
(ix) The hop count can be calculated for the received packet as follows: (*hop count*) = *t0* − *t*. For example, when a host receives a packet with a TTL value of 120 (*t* = 120), the minimum number in Table 1 that is larger than *t* is 128 (*t0* = 128). Therefore, the hop count is 8 (128 − 120 = 8).
(x) Hop Distance to Source Node= 255 (Default Initial Value)-Current TTL Value
(xi) 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 Muti Cast Path) && <=30; the packet is legitimate;
(xii) Else

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2014

(xiii) Packet is spoofed;
(xiv) Inform Other By Update Alarm Message (Attack Confirm)
(xv) If the difference <30 Packet is legitimate or else Spoofed
(xvi) Inform Other By Update Alarm Message (Attack Confirm)

VI. PERFORMANCE EVALUATION FACTORS

In order to measure and compare the performances of the proposed UHCF scheme, the work continue to adopt the three performance metrics, First is Packet delivery ratio (PDR) which defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node. Second is Routing overhead (RO) which defines the ratio of the amount of routing-related transmissions such as RREQ, RREP, ACK, 2ACK, S-ACK etc. Third is throughput which gives the effectiveness of the systems in transmitting the packets. The proposed mechanism can be able to identify the attacks based on their types. This can be prevented before any damage or packet drops. Further it can be extended to a few more parameters based upon the network density. The algorithm can also be extended to identify and prevent few more network layer attacks. To simulate proposed approach, scenario is created by writing TCL (Tool Command Language) script in which fifteen nodes are created with specified coverage and transmission power. Additional components are also defined in script file such as antenna type, routing protocol and queue type. Each node assigns hundreds percent energy.

Table-I: Simulation Environment

Number of nodes	19
Simulation time (seconds)	70
Radio range	300m
Traffic type	CBR, 3pkts/s
Packet size (bytes)	512
Number of traffic connections	4, 30
Transmission energy consumption	1.0J

In future the results will show the effectiveness of proposed scheme. For network simulation, there are several performance metrics which is used to evaluate the performance. In future simulation purpose this work will use seven performance metrics for showing the expected results. Results are plotted using Xgraph utility of NS2.

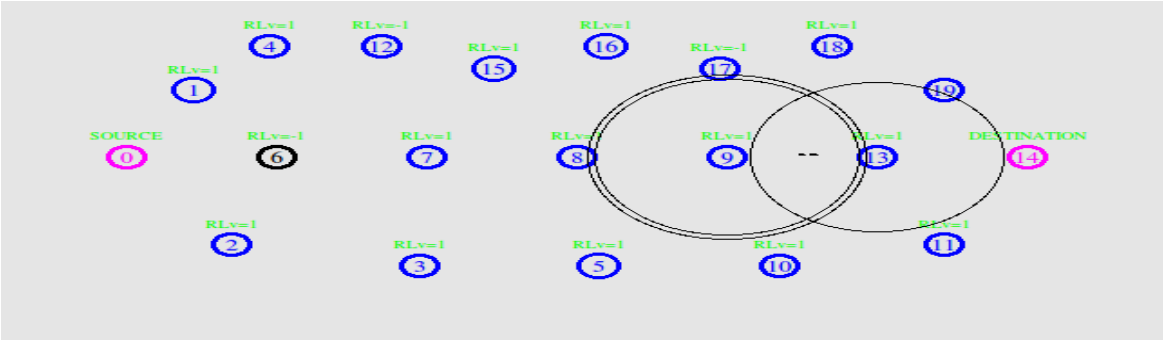


Figure 1: Simulation Environment and Scenario of UHCF

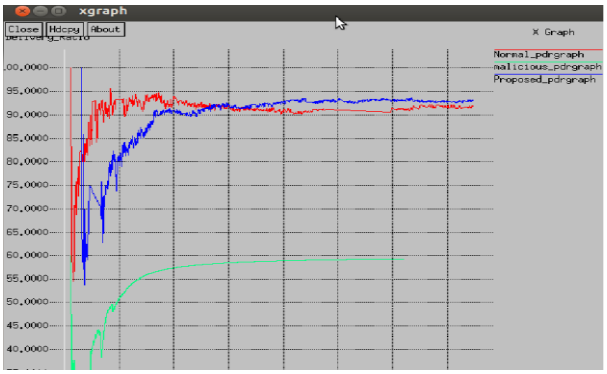
PDR (Packet Delivery Ratio) Graph
Packet delivery ratio is the ratio of number of packets received at the destination to the number of packets sent from the source. The performance is better when packet delivery ratio is high.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

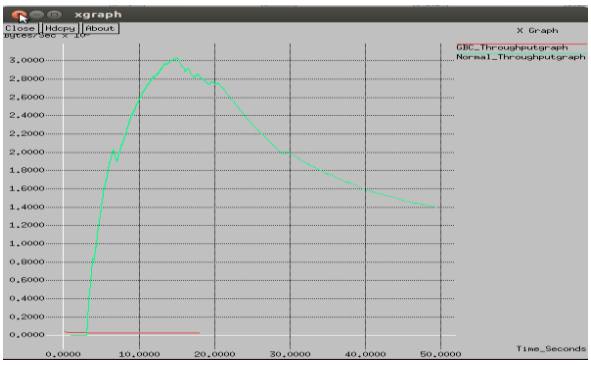
Vol. 3, Issue 8, August 2014



Graph 1: Comparison of PDR Ratio of UHCF Proposed and Existing

Graph Summary*:* As the PDR ratio is used to identify the performance of the approaches using the packet delivery ration. It is the ration of number of packet sent to the number of packet received. In ideal condition it should be high as possible. For comparing the suggested work of UHCF, the above graph interprets the result as an improved PDR ration than the existing approaches.

Throughput -It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation i.e., information whether or not data packets correctly delivered to the destinations.



Graph 2: Comparison of Throughput of UHCF Proposed and Existing AODV

Graph Summary: As throughput measure the transmission efficiency in terms of successfully delivered packets in unit time for a specified channel bandwidth. The above graph shows the effectiveness of the suggested approach while comparing it with the existing. The graph interprets the constant throughput for several cases which justify the approach.

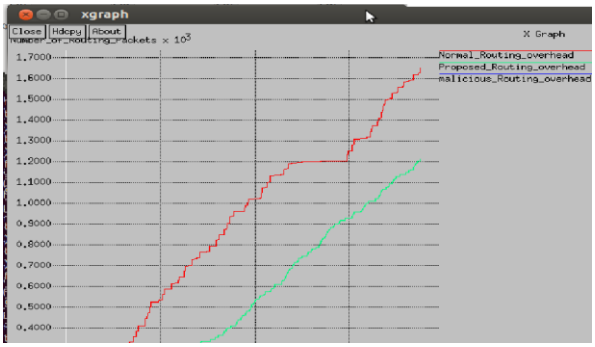
Routing Overhead Load- Routing Load is the ratio of total number of the routing packets to the total number of received data packets at destination. The amount of control traffic generated (in bits) per data traffic delivered (in bits). It should be taken in terms of the extra load started while executing the suggested approach than the normal protocol load for the system Considering the factors.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2014



Graph 3: Comparison of Routing Overhead of UHCF Proposed and Existing AODV

Graph Summary: The above graph verifies its results by minimum routing overhead associated with the suggested approach. It also shows that the complexity of using the proposed method is quite less in comparison with the existing.

By the above result based graph it is measured that the energy demands of the suggested approach is very less in comparison with the existing mechanism. Also the approach is proving the overall energy demands of the simulations. By less energy consumption the overall network lifetime is also increased.

Result Points

1. The detection rate of UHCF consistently swings around the optimum value of 99% which is a good sign of packet filtering technique. This result is the outcome of the combination of HCF and TTL which has prevented IP spoofing attacks up to the maximum.
2. Victim server cannot be overloaded with large number of packet flooding as it may lead to network jam and server bog down. But, UHCF technique can handle packet flooding, as the implementation can be done in a distributive manner using up to 30 numbers of intermediate Hops.
3. Not all packets have been checked at the victim server in the existing HCF technique. But, in proposed UHCF technique all packets have been checked on numbers of intermediate hops probabilistically.

behaviour.

VII. BENEFITS OF WORK

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 applying the above suggested approach there are some of the expected benefits measures are:

- Early and effective detection of malicious behaviour on the basis of identified parameters.
- Delay tolerant detection which reduces the probability of data losses.
- Timely triggered attack detection using performance check operations which decreases routing overhead.
- Behaviour analysis of new node in the network with no previous participation.
- Regular basis monitoring for sudden conversion identification and misleading node detections.
- The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process.

VIII. CONCLUSION

In this work a novel Updated Hop Count Filtering (UHCF) system is proposed defeat the issues created because of construed and ridiculed IP packets. The outlining of HCF separating capacity takes after the states of segregations of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2014

real bundles from the ridiculed parcels. The recommended methodology is equipped for distinguishing the DDoS assaults and its variations at the early phases of information exchanges and consequently decreases the likelihood of misfortunes and assaults events. The methodology is taking TTL contemplations as a key parameter for work and enhances the current issues, for example, multicast courses, manufactures and so forth. Here the bounce tally esteem is the distinction of last TTL esteem and starting TTL esteem. Anyway right now few of the issues stays unsolved whose result is been recommended by the proposed methodology. At the starting level of work the methodology appears to be equipped for recognizing Spoofed IP bundles with higher exactness and lower computational multifaceted nature.

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. 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.
19. G M Poddar and Prof N Rastogi, "*UHCF: Updated Hop Count Filter Using TTL Probing and Varying Threshold for Spoofed Packet Separation*", in International Journal of Emerging Research in Management &Technology ISSN: 2278-9359, Volume-3, Issue-4, April 2014.