Volume 5, Issue 11, November 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The End to End Active Packet Loss Measurement in Computer Network

[1]K. Sangetha, [2]B. S. Sangeetha, [3]R. Umamaheswari, [4]M. Sathya, [5]M. Mujeeb

[1]M.Sc., M.phil., Sri Saradha Nekthan College, Salem, Tamilnadu, India

[2, 3, 4] M.Sc., M.Phil., Shri Sakthi Kailassh Women's College, Salem, Tamilnadu, India

[5] MBA (IT)., M.Phil., AVS Arts & Science College, Salem, Tamilnadu, India

***Abstract:** Measurement and estimation of packet loss characteristics are challenging due to the relatively rare occurrence and typically short duration of packet loss episodes. While active probe tools are commonly used to measure packet loss on end-to-end paths, there has been little analysis of the accuracy of these tools or their impact on the network. The objective of our study is to understand how to measure packet loss episodes accurately with end-to-end probes. We begin by testing the capability of standard Poisson- modulated end-to-end measurements of loss in a controlled laboratory environment using IP routers and commodity end hosts. Our tests show that loss characteristics reported from such Poisson-modulated probe tools can be quite inaccurate over a range of traffic conditions. Motivated by these observations, we introduce a new algorithm for packet loss measurement that is designed to overcome the deficiencies in Evaluate the capabilities of our methodology experimentally by developing and implementing a prototype tool, called BADABING. The experiments demonstrate the trade-offs between impact on the network and measurement accuracy. We show that BADABING reports loss characteristics far more accurately than traditional loss measurement tools.*

The objective of our study is to understand how to measure packet loss episodes accurately with end-to-end probes. We begin by testing the capability of standard Poisson-modulated end-to-end measurements.

Motivated by these observations, we introduce a new algorithm for packet loss measurement that is designed to overcome the deficiencies in standard Poisson-based tools.

Standard Poisson-based tools. Specifically, our method entails probe experiments that follow a geometric distribution to enable an explicit trade-off between accuracy and impact on the network, and enable more accurate measurements than standard Poisson probing at the same rate.

Keywords: BADABING, TCP, UDP, LTCIP

I. INTRODUCTION

Measuring and analyzing network traffic dynamics between end hosts has provided the foundation for the development of many different network protocols and systems. Of particular importance is under-standing packet loss behavior since loss can have a significant impact on the performance of both TCP- and UDP-based applications. Despite efforts of network engineers and operators to limit loss, it will probably never be eliminated due to the intrinsic dynamics and scaling properties of traffic in packet switched network. Network operators have the ability to passively monitor nodes within their network for packet loss on routers using SNMP. End-to-end active measurements using probes provide an equally valuable perspective since they indicate the conditions that application traffic is experiencing on those paths.

Our study involves the empirical evaluation of our new loss measurement methodology. To this end, we developed a one-way active measurement tool called BADABING. BADABING sends fixed-size probes at specified intervals from one measurement host to a collaborating target host. The target system collects the probe packets and reports the loss characteristics after a specified period of time. We also compare BADABING with a standard tool for loss measurement that emits probe packets at Poisson intervals.

The results show that our tool reports loss episode estimates much more accurately for the same number of probes. We also show that BADABING estimates converge to the underlying loss episode frequency and duration characteristics. Our observations about the weaknesses in standard Poisson probing motivate the second part of our study: the development of a new approach for end-to-end loss measurement that includes four key elements. First, we design a probe process that is geometrically distributed and that assesses the likelihood of loss experienced by other flows that use the same path, rather than merely reporting its own packet losses. The probe process assumes FIFO queues along the path with a drop-tail policy. Second, we design a new experimental framework with estimation techniques that directly estimate the mean duration of the loss episodes without estimating the duration of any individual loss episode. Our estimators are proved to be consistent, under mild assumpt ions of the probing process.

II. ALGORITHM

A Probabilistic Packet Marking Scheme With Lt Code For Ip Trace Back

Cybercrime has become an important issue in the cyber-society. Distributed Denial of Service attack is the most popular attack, which uses many zombies to attack the victim, makes victim crashed and interrupt services. We propose the LT Code IP Trace back scheme to reconstruct the attack graph and find the source of attacker. LTCIP overcomes the collision problem in traditional packet marking scheme. It uses fewer packets to reconstruct the attack graph. Finally, our LTCIP is a reliable IP Trace back scheme, which can find the source of DDoS and avoid the attack.

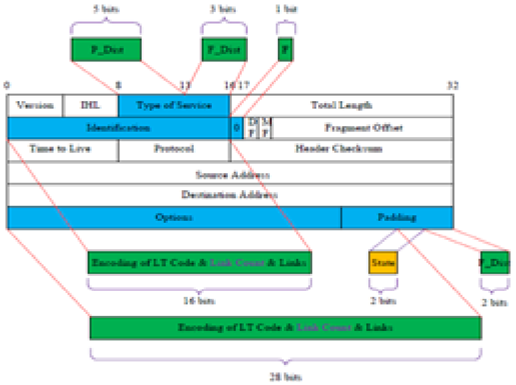
Distributed Denial of Service (DDoS) attack is one of the popular attacks and causes damage severely. DDoS attack sends large amount of packets to the victim and let the victim cannot serve legitimate users.

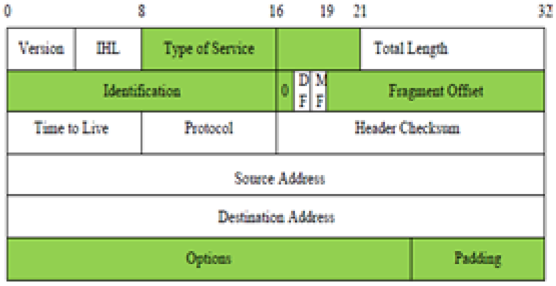
DDoS have affected many famous companies such as Yahoo, eBay and Twitter…etc. Nowadays, finding the true source of DDoS attack is difficult. DDoS attack is easy to implement and hard to defend due to the stateless behaviour of the internet. Many business products such as intrusion detection system or firewall can detect the DDoS attack, but they could not find the attack source.

In order to find the DDoS source, IP Traceback is proposed to tracing back to the source address of the attacker by overcoming IP spoofing . Probabilistic Packet Marking (PPM) is an efficient marking scheme, which marks part of router's information into IP Header. It uses constant probability to decide whether the packet should be marked or not. This scheme can reconstruct the attack graph with enough packets, which means that PPM needs many packets to complete the reconstruction. LT Code IP Traceback (LTCIP) scheme is based on Dynamic Probability and Luby Transform Code (LT Code) to complete the marking procedure. It uses link list to collect the marked packets and decode the received packets. Dynamic Marking Probability uses this method to receive every router's partial information with the same probability. LT Code can be used in the IP Trace back, which reduces the collision of the packets. Thus, LTCIP uses fewer ackets to trace back the DDoS attacking source accurately.

Proposed It Code Ip Trace Back Scheme

We propose a LTCIP by considering LT Code and Dynamic Marking Probability. There are three procedures in the LTCIP: 1) marking procedure, 2) collection procedure and 3) reconstruction procedure. The marking procedure finds the source of the attacker. The marking procedure uses LT Code encode 32-bits IP Address primitively. Finally, we use ink list to store the marked packets. The reconstruction procedure decodes the collected packets and extracts the attack paths.





We use the 8-bits ToS Field, 16-bits ID Field, 1-bit Reserved Field and 32-bits Option and Padding Field to store mark information. It overcomes 25 hops count and uses 5 bits to represent it. Then, we divide ToS Fields into two parts.

The 2 bits of Padding Field to assist to complete the 10-bits distance field in order to store the hop count and the information of beginning and terminated router. TABLE I shows the purpose of each used fields, defines the variables of marking algorithm

.

Dynamic Marking Procedure of LT Code

```
BEGIN
For each packet P at router R
Find initial TTL value of P;
TDistance := initial TTL value – current value of TTL;
LTCode ltc := NULL; Integer i :=0;
p := 1 / TDistance;
Degree distribution d is 1 or 2;
Let r be a random number from [0,1)
IF r < p THEN
IF F = 0 THEN
Initialize the Marking Fields;
```

LT Code Encoding Procedure

```
Choose d distinct bits b[i] from 32 bits IP Address of current router randomly;
IF d = 2 THEN
```

```
            ltc := b[i] ⊕b[i+1]; LC := 1;
        ELSE
            ltc := b[i]; LC := 0;
        END IF
        ELC := ltc; L := 1 or 2 links; F :=1; P_Dist := TDistance;
    ELSE
        z := CheckEmptyField();
        IF z = 0 THEN
            Execute LT Code Encoding Procedure;
            ELC := ltc; L := 1 or 2 links;
        ELSE
            Execute (F = 0) step;
        END IF
    END IF
ELSE
    IF F = 1 THEN
        F := 0; F_Dist := TDistance - 1;
    END IF
END IF, Forward P to the next router; END
```

DYNAMIC MARKING PROCEDURE OF DETERMINATION OF LT CODE

```
BEGIN
    For each packet P at router R
    Find initial TTL value of P;
    TDistance := initial TTL value – current value of TTL;
    LTCode ltc := NULL; Integer i :=0;
    p := 1 / TDistance;
    Degree distribution d is 1 or 2;
    Let r be a random number from [0,1)
    IF state = 00 THEN
        IF r < p THEN
            Initialize the Marking Fields;
            //LT Code Encoding Procedure
            Choose d distinct bits b[i] from 32 bits IP Address of current router randomly;
            IF d = 2 THEN
                ltc := b[i] ⊕b[i+1]; LC := 1;
            ELSE
                ltc := b[i]; LC := 0;
            END IF
            ELC := ltc; L := 2 links; state := 01; P_Dist := TDistance;
        END IF
    ELSE IF state = 01 THEN
        Execute LT Code Encoding Procedure;
        ELC := ltc; L := 2 links; state := 10;
    ELSE IF state = 10 THEN
        Execute LT Code Encoding Procedure;
        ELC := ltc; L := 2 links; state := 11;
    ELSE
        Execute LT Code Encoding Procedure;
        ELC := ltc; L := 2 links; state := 00; F_Dist := TDistance;
    END IF
    Forward P to the next router;
END.
```

III. MARKING PROCEDURE

We propose two types of LTCIP. The first LTCIP uses dynamic storing method to store the encoding symbols into the marking fields of the packet, that is to say higher storage. It uses 1 bit to represent the encoding symbol and uses 5 or 10 bits to represent the links which represent the positions of encoding symbols and are decided by the random degree distribution between 1 and 2. It uses 1 bit to represent the link count.

The storing order of marking information is encoding symbol, link count and the last is maybe one link position or two link positions. The best performance of the first LTCIP is that it could store at most six encoding symbols of the routers. The following will show the first LTCIP marking algorithm and steps. The steps of Dynamic Marking Procedure of LT Code.

Step1: Finding initial TTL value and computing dynamic marking probability.
Step2: Decide whether the packet should be marked or not through dynamic marking probability.
Step3: Checking the flag of packet. If the flag is 0, using LT Code encoding method and saving hops count to the Previous Distance Field and storing specific information to the marking fields.
Step4: If the flag is 1, checking the marking field whether it is full or not. If it is not full, storing specific information. If it is full, executing the step which the flag is 0.
Step5: If the packet is not marked by the router, storing previous hops count to the following distance field and forward the packet to the next router.

The marking procedure of the second LTCIP is called Dynamic Marking Algorithm of Determination of LT Code, which its marking method is a little bit different with the first LTCIP. It uses state field to check the packet whether the marking field is full or not. Its marking method also uses dynamic marking probability to decide whether the current packet will be marked or not. It uses fixed storing method and the storing order of marking information is encoding symbol, first link and the last is second link. If the router decides to mark the packet, the encoding symbols of the following three routers will be marked into the packet too. The best performance of the second LTCIP is that it could store at most four encoding symbols of the routers and ensure saving four encoding symbols invariably.

The second LTCIP marking algorithm and steps are shown as follows: The steps of Dynamic Marking Algorithm of Determination of LT Code.
Step1: Finding initial TTL value and computing dynamic marking probability.
Step2: Checking the packet state.
Step3: If the packet state is 00 and the dynamic marking probability is greater than random number ,using LT Code encoding method and saving hops count to the Previous Distance Field and storing specific information to the marking fields.
Step4: If the packet state is 01 and 10, the router marks the packet determinately through the same method which is just like state of 00.
Step5: If the packet state is 11, this step is the same as step 4 and need to store the hops count into the Following Distance Field. Finally, forwarding the packet to the next router.

PACKET COLLECTION PROCEDURE

We create a Packet Collection List Table (PCLTbl) at the victim. It has two slots, the first slot will store the source IP Address of the attackers and the second slot will use the method of link list to store the marked packets by the upstream routers. When each packet forwards to the victim, the victim will check the table and insert the marking information to the appropriate place.

The marking information will sort dynamically when the packet enters into the victim. In order to decrease the amount of storage at the victim, we use the behavior of the link list to store the marking information dynamically. The Packet Collection algorithm and the steps are shown as follows: The steps of Dynamic Marking Algorithm of Determination of LT Code
Step1: Initializing Table Entry and Node Pointer variables.
Step2: Finding the table entry and checking the packet source which is sent by attacker.

Reconstruction Procedure

This finds the marking information of same distance and same source. It puts the marking information of the same features into the decoding box. The decoding box executes LT Code decoding. After decoding procedure, the result gets the IP Address from one router to the others. Finally, the procedure puts the decoded information into the stack. This method could get the full attack graphs and find the source of the attackers. The following will show the Reconstruction algorithm and steps. The steps of Reconstruction Procedure
Step1: Finding first table entry and first node.
Step2: Finding the same distance through node pointer.
Step3: Throwing the same distance node into Decoding Box and using LT Code decoding method to decode the symbols which are in the Decoding Box .
Step4: The IP Address which is decoded through LT Code decoding method will store into the stack.
Step5: Extracting the full attack path from stack through pop operation.

PACKET COLLECTION PROCEDURE

```
 BEGIN
 For each packet P from attacker
 Let PCLTbl to be the Packet Collecting List Table
TableEntry *te := NULL;
 NodePointer *nptr := NULL, *currptr := NULL;
 te := FindTableEntry(P.Source);
 IF te != NULL THEN
 nptr := head;
WHILE nptr != NULL DO
 IF nptr → data.P_Dist = P.P_Dist && nptr → data.F_Dist >=
P.F_Dist || nptr →link = NULL THEN
```

```
      newNode → link := nptr → link;
      nptr → link := newNode;
      BREAK;
    ELSE IF nptr → data.P_Dist > P.P_Dist THEN
      currptr := head;
      WHILE currptr != nptr DO
        IF currptr → link = nptr THEN
          newNode → link := currptr → link;
          currptr → link := newNode;
          BREAK;
        END IF
        currptr := currptr → link;
      END WHILE
      BREAK;
    ELSE
      nptr := nptr → link;
    END IF
  END WHILE
ELSE
  te := FindEmptyEntry();
  CreateTableEntry(te,PSource);
  nptr := head;  nptr → link := newNode; END IF, END.
```

RECONSTRUCTION PROCEDURE

```
BEGIN
  Let PCLTbl to be the Packet Collecting List Table
  TableEntry *te := NULL;
  NodePointer *nptr := NULL;
  DeconingBox *deb := NULL;
  Integer i;
  te := FindFirstRow();
  WHILE te != NULL DO
    nptr := head;
    WHILE nptr != NULL DO
      i := 0;
      p_dist := nptr → data.P_Dist;
      f_dist := nptr → data.F_Dist;
      Insert(deb,nptr → data);
      WHILE i != 1 DO
        nptr := nptr → link;
        cpr := Compare(p_dist,f_dist, nptr → data.P_Dist, nptr → data.F_Dist);
        IF cpr = TRUE THEN
          Insert(deb,nptr → data);
        ELSE
          i := 1
        END IF
      END WHILE
      ipaddr := Calculate(deb);
      Stack(ipaddr);
      Initialize(deb);
    END WHILE
    te := te + 1;
  END WHILE
  Extract
```

IV. RESULTS AND PERFORMANCE

A. Case Analysis

Case1: represents the worst situation;
Case2: represents the best situation; and
Case3: represents the state of full marking field.

Case 1

If the packet sent by the attacker and passes through the router R1, it calculates the hops count of the packet and get the dynamic marking probability which is 1. At first, R1 checks the Flag Field, then execute LT Code encoding procedure and write the specific information to the packet.

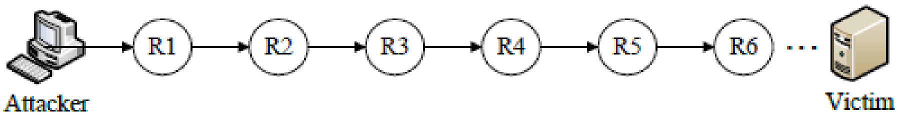
R1 forwards the packet to the next router R2. If R2 would not mark the packet through dynamic marking probability, R2 writes the previous hops count to the Following Distance Field and set the flag value to be 0. Finally, R3 to R6 would not mark the packet, victim receive only partial information of R1.

Case 2

If the packet is forwarded from R1 to R6, each router will mark the packet definitely and the degree distribution is always 1. When the packet is forwarded to the R6, the marking field of the packet will store the encoding bits of the router from R1 to R6. When the victim receives enough packets which take the marking information from R1 to R6, the Reconstruction Procedure could use these packets to reconstruct the IP Address of the router from R1 to R6.

Case 3

If R1, R2 to R4 mark the packet definitely and the degree distribution also is 2. The marking filed of the packet is full at the R4. When the packet is forwarded to the R5 and it decides to mark the packet, R5 checks the packet and finds out that the marking field of the packet is full. Thus, it initializes the marking fields and executes the process which flag is 0. At this moment, the marking field of the packet only has the encoding in formation of the R5.



V. CONCLUSION

In this thesis, we have studied the problem of combating Internet worms. To that end, we have developed a branching process model to characterize the propagation of Internet worms. Unlike deterministic epidemic models studied in the literature, this model allows us to characterize the early phase of worm propagation. Using the branching process model, we are able to provide a precise bound M on the total number of scans that ensure that the worm will eventually die out. Further, from our model, we also obtain the probability that the total number of hosts that the worm infects is below a certain level, as a function of the scan limit. The insights gained from analyzing this model also allow us to develop an effective and automatic worm containment strategy that does not let the worm propagate beyond the early stages of infection. Our strategy can effectively contain both fast scan worms and slow scan worms without knowing the worm signature in advance or needing to explicitly detect the worm. We show via simulations and real trace data that the containment strategy is both effective and non-intrusive.

REFERENCES

[1] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, “Next Century Challenges: Scalable Coordination in Sensor Networks,” Proc. ACM Mobile Computing. 263-270, Aug. 1999.

[2] B. Karp and H.T. Kung, “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks,” Proc. ACM MobiCom, pp. 243- 254, Aug. 2000.

[3] Yi Shang, Hongchi Shi and A. Ahmed, “Performance study of localization methods for ad-hoc sensor networks”, in proceedings of IEEE International Conference of Mobile Ad-hoc and Sensor Systems, Fort Lauderdale, FL, October 2004.

[4] Akkaya, K. and M. Younis, A survey on routing protocols for wireless sensor networks. Ad hoc networks, 2005. 3(3): p. 325-349.

[5] Son, D., B. Krishnamachari, and J. Heidemann. Experimental study of concurrent transmission in wireless sensor networks. in Proceedings of the 4th international conference on Embedded networked sensor systems, ACM, 2006.

[6] Lou, W., W. Liu, and Y. Zhang, Performance optimization using multipath routing in mobile ad hoc and wireless sensor networks, in Combinatorial optimization in communication networks, Springer, 2006. p. 117-146.

[7] Ganesan, D., et al., Highly-resilient, energy-efficient multipath routing in wireless sensor networks. ACM SIGMOBILE Mobile Computing and Communications Review, 2001. 5(4): p. 11-25.

[8] Felemban, E., C.-G. Lee, and E. Ekici, MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks. Mobile Computing, IEEE, 2006. 5(6): p. 738-754.

[9] A. Manjeshwar and D. P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks", in the Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing.

[10] Theodore S. Rappaport. Wireless communications principles and practice, Second edition 2003.

[11] Jiangping Jiang et.al. On distributed dynamicchannel allocation in mobile cellular networks. IEEE transactions on parallel and distributedsystem, 13(10): 1024-1037, 2002.