Analysis of Algorithm design in the Fast Internet Traceback scheme

Ngo Tien Dung ○, and Choong Seon Hong

Department of Computer Engineering, Kyung Hee University

dungnt@networking.khu.ac.kr ○, cshong@khu.ac.kr

Abstract

The rising threat of cyber attacks, especially DDoS, makes the IP traceback problem very relevant to today's Internet security. The Fast Internet Traceback (FIT) [1] is a novel scheme which just use only 1 bit to derive the distance from the receiver and the last marking FIT enabled router, so it significantly decreased number of received packets needed for victim to reconstruct the attack path, and could derive the actual legacy hops between the receiver and the last marking FIT enabled router. In this paper, we make the analysis to know how the algorithm in the FIT scheme is designed.

1. Introduction

Denial of Service (DoS) attacks has been a major threat to the Internet for a long time now. Tracing the source of the attack has been seen as one of the solutions to DoS. Probabilistic Packet Marking [2] has been proposed for the identification of the source of DoS attack. This scheme is based on the idea that routers mark packets that pass through them with their addresses or a part of their addresses. Packets for marking are selected at random with some fixed probability of being selected. As the victim gets the marked packets, it can reconstruct the full path, even though the IP address of the attacker is spoofed. However, the PPM scheme which is proposed by Savage [2] seemed to wasteful bits for representing the distance between the receiver and the last marking router. In order to solve that problem, the Fast Internet Traceback (FIT) scheme [1] is proposed, which did not use 5 bits increment distance field to calculate the distance. This scheme used less space for representing how the receiver is far from the last marking router. It leaded to the improvement in the IP Traceback such as: the expected number of needed packet for victim to reconstruct the attack path is reduced and calculate the numbers of hops between the receiver and the last marking router. In this paper, we will analysis the algorithm design of FIT scheme.

2. FIT scheme

In the FIT scheme, as in all other PPM schemes, routers encode on the 16 bit IP Identification (IPID) field of the IPv4 header as they decide to mark on the received packets before forwarding. The global constant q among all FIT enabled routers is set to 0.04 that is the marking probability on packets passing through. 1/d is the optimal value of probability q to reduce the average number of received packets for the victim to reconstruct the attack path [2]. q=0.04 is optimal for markings from routers at a distance of 25 hops from the reconstructing endhost. The mark field contains three subfields, as shown in Figure 1. The first field, denoted as b, is the 1-bit distance field. The second and third fields involve the router's hash. Each FIT router pre-calculates a hash of its IP address and splits the hash into n fragments of b_{frag}-bits each, where n is a global constant. The size of each fragment, b_{frag}, is set as $15-b_{fnum}$. As marking, a router randomly selects a fragment number to mark into the frag# field, and the hash fragment field will be assigned with the corresponding fragment's bits.

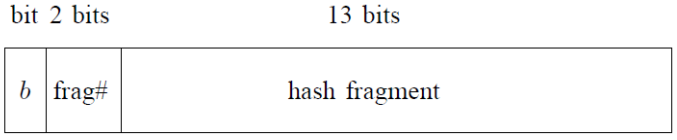


Figure 1. FIT marking field diagram. The distance field b is one bit. In this

This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2010-(C1090-1031-0005))

Dr. CS Hong is the corresponding author

example, the fragment number field is two bits ($b_{fnum} = 2$ bits) allowing four distinct fragments, and the remaining 13 bits are used for the hash fragment ($b_{frag} = 13$ bits).

Unlike other PPM schemes, FIT router makes the marking decision from the result of calculating *marking predicate* based on the packet's TTL field and distance bit. The received packet would be automatically marked by the forwarding router if the packet was not marked for the past 32 hops. The *marking predicate* is computed as: $\left(b \mid c - TTL_{[5..0]}\right) \bmod 64 > 32$, where $b \mid c$ denotes the concatenation of the distance bit b in the packet with the global constant c, and $TTL_{[5..0]}$ denotes the six least significant bits of the TTL field.

As marking a packet, a router chooses a fragment number randomly, then write to the *frag#* field and the hash fragment field will be marked with the corresponding hash fragment's bits. a global constant c will be assigned to the 5 least significant bits of the packet's TTL , and the distance field b contains the 6th bit of the TTL. The purpose is helping the receiver to identify the distance from the last marking router.

FIT packet marking algorithm:

FOR each packet P
  $r \xleftarrow{R} [0,1)$
  IF $(r \le q)$
  OR (P.*dist_bit*$|c - TTL_{[5..0]} \mod 64) > 32$ THEN
    $\alpha \xleftarrow{R} [0,n)$
    P.*frag_num* $\leftarrow \alpha$
    P.*fragment* $\leftarrow H(IP)_{[(\alpha+1)\cdot b_{fnum}-1..\alpha\cdot b_{fnum}]}$
    P.*dist_bit* $\leftarrow TTL_{[5]}$
    $TTL_{[4..0]} \leftarrow c$
  ELSE
    $TTL \leftarrow TTL - 1$

Figure 2. The FIT Marking Algorithm

$r \leftarrow [0,1)$ means that we select a number from the interval [0, 1) uniformly at random. The notation $TTL_{[5]}$ selects bit 5 of the TTL (the LSB is $TTL_{[0]}$, and $TTL_{[5..0]}$ selects the six least significant bits.

4. Analysis of algorithm design

In order to understand the FIT Marking Algorithm in Figure 2, we need to calculate the value of $\left(b \mid c - TTL_{[5..0]}\right) \bmod 64$ corresponding to all possible received values of $\left(TTL_{[5]}, P.dist\_bit\right)$ as router R_2 (FIT enabled router) received from any neighbor router R_1.

R_1		R_2 (FIT enabled router)
$P.dist\_bit$	$TTL_{[5]}$	$\left(b \mid c - TTL_{[5..0]}\right) \bmod 64$
0	0	$\left(c - TTL_{[4..0]}\right) \bmod 64$
1	0	$\left(\left(c - TTL_{[4..0]}\right) + 32\right) \bmod 64$
0	1	$\left(\left(c - TTL_{[4..0]}\right) - 32\right) \bmod 64$
1	1	$\left(c - TTL_{[4..0]}\right) \bmod 64$

As we can see from the table above, If $TTL_{[5]}$ and $P.dist\_bit$ has the same value, that is, $\left(P.dist\_bit, TTL_{[5]}\right) = (0,0)$ or $\left(P.dist\_bit, TTL_{[5]}\right) = (1,1)$ then $\left(b \mid c - TTL_{[5..0]}\right) \bmod 64 = \left(c - TTL_{[4..0]}\right) \bmod 64$ $= c - TTL_{[4..0]}$ (Because $0 \le c - TTL_{[4..0]} \le 31$) . Else if $TTL_{[5]}$ does not equal $P.dist\_bit$, $\left(P.dist\_bit, TTL_{[5]}\right) = (1,0)$ or $\left(P.dist\_bit, TTL_{[5]}\right) = (0,1)$ then $\left(b \mid c - TTL_{[5..0]}\right) \bmod 64 = \left(c - TTL_{[4..0]}\right) + 32$ (Because $0 \le c - TTL_{[4..0]} \le 31$). Note that in the case of $\left(P.dist\_bit, TTL_{[5]}\right) = (0,1)$, then $\left(b \mid c - TTL_{[5..0]}\right) \bmod 64$ $= \left(\left(c - TTL_{[4..0]}\right) - 32\right) \bmod 64$

$= \left(\left(c - TTL_{[4..0]} \right) - 32 \right) + 64 \mod 64$

$= \left(c - TTL_{[4..0]} \right) + 32 \quad (> 32)$. Thus if

$\left(P.dist\_bit \neq TTL_{[5]} \right)$, the

$\left(b \mid c - TTL_{[5..0]} \right) \bmod 64 > 32$ will always happen.

Hence, the condition of marking on the received packet could be state as follows: if $\left(P.dist\_bit \neq TTL_{[5]} \right)$, or $\left(\left(P.dist\_bit = TTL_{[5]} \right) \& \left(\left(c - TTL_{[4..0]} \right) > 32 \right) \right)$, the current FIT router will decide to mark on the received packet.

Next, we would consider all situations of marking decision of the FIT enabled router R_2. There are two cases:

1) R_2 marks on the packet randomly regardless of the value of $\left(b \mid c - TTL_{[5..0]} \right) \bmod 64$:

   Then, R_2 will update $P.dist\_bit$ field: $P.dist\_bit \leftarrow TTL_{[5]}$ and reset $TTL_{[4..0]}$ in the TTL field. When receiver receives a packet from R_2, it could know how far from the nearest marking router R_2 by computing $d = c - TTL_{[4..0]} + 1$.

2) R_2 decides to mark on the packet if it exists the event $\left(P.dist\_bit \neq TTL_{[5]} \right)$ in the received packet :

   We want to know why R_2 will make the marking decision with this case in the FIT marking algorithm.

   In the normal way, If there is no attacker/compromised router between 2 consecutive FIT routers R_a and R_2

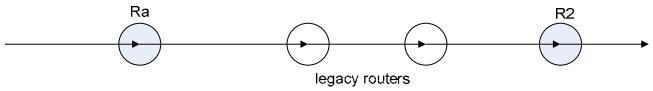


Figure 3. No compromised router between 2 consecutive FIT routers

then $P.dist\_bit$ is always the same as $TTL_{[5]}$ in the process that packet traverses from R_a and R_2 due to the marking mechanism (algorithm) involving the assignment $P.dist\_bit \leftarrow TTL_{[5]}$ of FIT enabled routers.

However, if R_2 receives a packet and check that $P.dist\_bit \neq TTL_{[5]}$ then there are 2 clear possibilities: Received packet has not traversed any FIT enabled router yet, or there is at least a compromised router on the attack path from R_a to R_2

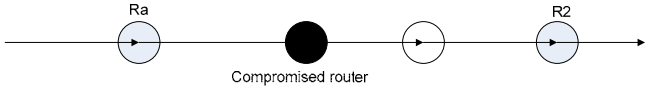
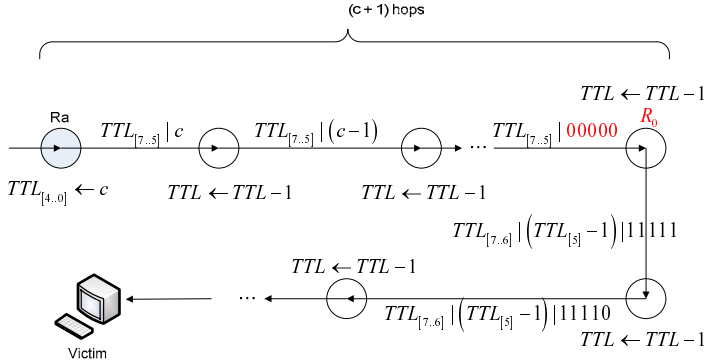


Figure 4. Compromised router in the middle

In other words, the packet that R_2 received was faked. Therefore R_2 should decide to mark on the received packet in this case.

3) The current FIT router would decides to mark on the packet if it exists the event $\left(\left(P.dist\_bit = TTL_{[5]} \right) \& \left(\left(c - TTL_{[4..0]} \right) > 32 \right) \right)$ in the received packet:



As we can see from the figure, since a packet

traversed the marking router R_a, its TTL value has been decreased each time going through one legacy router on the attack path. The value $TTL_{[4..0]}$ will be decreased down to zero just before reaching R_0 whose distance > c. For any receiver which has distance from R_0 $\leq c$, it will see the event $\left(P.dist\_bit = TTL_{[5]}\right)$ of the received packet. In other words, if the receiver see that event, it could believe that the received packet ever traversed one marking router whose distance from the receiver < c. If R_0 is a legacy router, it will decrease the TTL field of packet 1 unit before forwarding to the next router, so R_0 is the router that makes a change from the event $\left(P.dist\_bit = TTL_{[5]}\right)$ to $\left(P.dist\_bit \neq TTL_{[5]}\right)$. In other words, If the distance of 2 consecutive FIT routers that packet traverse through is $> c$, the $TTL_{[5]}$ values of them do not equal . That is the reason why the FIT scheme must use the $P.dist\_bit$ to store the $TTL_{[5]}$ value of the last traversed marking router in order for the receiver to check whether the received packet ever traversed through the last marking router which distance is $> c$ or not. Generally, if the receiver receives one packet which has the event $\left(P.dist\_bit \neq TTL_{[5]}\right)$, it will confuse and could not know which is the actual reason that made the event $\left(P.dist\_bit \neq TTL_{[5]}\right)$ of the following 3 reasons: received packet has not traverse any FIT enabled router yet, or there is at least a compromised router on the attack path from marking router R_a to the receiver, or d (distance between the receiver/current FIT enabled router and the nearest marking router R_a) $> c$.

In order to avoid the change of event from $\left(P.dist\_bit = TTL_{[5]}\right)$ to $\left(P.dist\_bit \neq TTL_{[5]}\right)$, if the current FIT enabled router check that $\left(\left(P.dist\_bit = TTL_{[5]}\right)\&\left(TTL_{[4..0]} = 00000\right)\right)$, then it should decide to mark on the received packet

From the above analysis, we could state the condition of marking for the current FIT router on the received packet as follows: If the event $\left(P.dist\_bit \neq TTL_{[5]}\right)$, or $\left(\left(P.dist\_bit = TTL_{[5]}\right)\&\left(TTL_{[4..0]} = 00000\right)\right)$ happens, the current FIT router will decide to mark on the received packet. In other words, from the received packet, if the current FIT router see that the event $\left(P.dist\_bit \neq TTL_{[5]}\right)$ or the final event $\left(P.dist\_bit = TTL_{[5]}\right)$ before being changed to the event $\left(P.dist\_bit \neq TTL_{[5]}\right)$ by doing $TTL \leftarrow TTL - 1$, it will mark on it.

6. Conclusion

Our analysis explored the FIT scheme and pointed how the FIT marking algorithm is designed. Actually, FIT scheme could not avoid using 5 bits to represent or calculate the distance between the receiver and the last marking router, but it exploited available 5 bits $TTL_{[4..0]}$ in the TTL field and one more bit $P.dist\_bit$.

References

[1] A. Yaar, A. Perrig, D. Song, “FIT: Fast Internet Traceback,” In Proc. Of IEEE INFOCOM’05, vol. 2, pp. 1395-1406, 2005.

[2] Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson. Practical network support for IP traceback. In Proceedings of ACM SIGCOMM 2000, August 2000.

[3] R. L. Carter and M. E. Crovella, “Dynamic server selection using dynamic path characterization in wide-area networks,” in Proc. IEEE INFOCOM, vol. 3, Apr. 1997, pp. 1014–1021.

[4] W. Theilmann and K. Rothermel, “Dynamic distance maps of the Internet,” in Proc. IEEE INFOCOM, vol. 1, Mar. 2000, pp. 275–284.

[5] Skitter analysis (2000). [Online]. Available: http://www.caida.org/ Tools/Skitter/Summary/