HITH: Hybrid IP Traceback for Heterogeneous Wireless Networks

Ikbel Daly[1], Faouzi Zarai[1], M. S. Obaidat[2], K.F. Hsiao[3] and Lotfi Kamoun[1]
[1]*LETI Laboratory, University of Sfax, Sfax, Tunisia*
[2]*Department of Computer and Information Science, Fordham University, NY, U.S.A.*
[3]*Dep. of Information Management, Ming-Chuan University, Taoyuan County 333, Taiwan*

Keywords: Heterogeneous Wireless Network, Security, Hybrid IP Traceback, Marking Packet, Logging Packet, Denial of Service Attack.

Abstract: The Denial of Service attack becomes increasingly vulnerable with heterogeneous wireless networks. Thus, it is fundamental to identify the source of attack by the execution of an IP traceback technique. There are two major categories: packet marking and packet logging. The first approach moderates the problem of overhead, but requires a large amount of packets to reconstruct the attack path. In packet logging, saving packets in digest tables enables the identification of attack source through a single packet but necessitates a huge storage space. In this paper, we propose a novel Hybrid IP Traceback for Heterogeneous wireless networks, which is called HITH (Hybrid IP Traceback for Heterogeneous wireless network). Our solution presents a precise IP traceback method with low overhead storage and improved accuracy. Indeed, the mathematical analysis and the comparison with existing solutions prove the capacity to trace a single IP packet while reducing storage overhead and data access time.

1 INTRODUCTION

The infrastructure of communication becomes increasingly heterogeneous following the integration of several technologies in order to meet the growing needs of the users' community. This heterogeneity has several mechanisms and techniques that are characterized by a specific composition and precise services and features.

To ensure this connectivity, we use several methods and strategies. Indeed, interoperability depends on the network topology, traffic pattern, interference, etc. According to Ren et al., 2011, the connectivity of low-priority network component depends on the characteristics of high-priority component, in order to ensure the diversity of techniques and to reduce infrastructure complexity.

In order to ensure the networks' heterogeneity, we must first procure the interworking between existing technologies from the third generation (3G) to the fifth generation (5G). Figure 1 illustrates an example of Heterogeneous Wireless Networks (HWN) which integrates two technologies; LTE (Long Term Evolution) and Wireless Mesh Network (WMN).

In heterogeneous wireless network, characterized by the integration of multiple network types and wireless technologies, the problem of security is becoming more critical. Consequently, this issue may deserve urgent and effective solutions to ensure secure communications and maintain the confidence between network equipment.

DoS (Denial of Service) (Houle and Weaver, 2001) and DDoS (Distributed DoS) (Phatak et al., 2013) attacks present the most spread vulnerability in the Internet, which can affect multiple targets, even critical, in a very short duration.

To prevent networks against these attacks, we can apply some traceability techniques, known by IP Traceback. This mechanism allows tracking packets and ensures the identification of the real source of attack.

The remaining part of this paper is organized as follows. In section II, we introduce some related works, which treat the existing IP traceback techniques. Section III describes our proposed hybrid IP traceback approach for Heterogeneous wireless Networks in details. Section IV evaluates the performance of our approach. Finally, Section V gives the conclusion.

Daly, I., Zarai, F., Obaidat, M., Hsiao, K. and Kamoun, L.
HITH: Hybrid IP Traceback for Heterogeneous Wireless Networks.
DOI: 10.5220/0006042500840093
In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 6: WINSYS*, pages 84-93
ISBN: 978-989-758-196-0

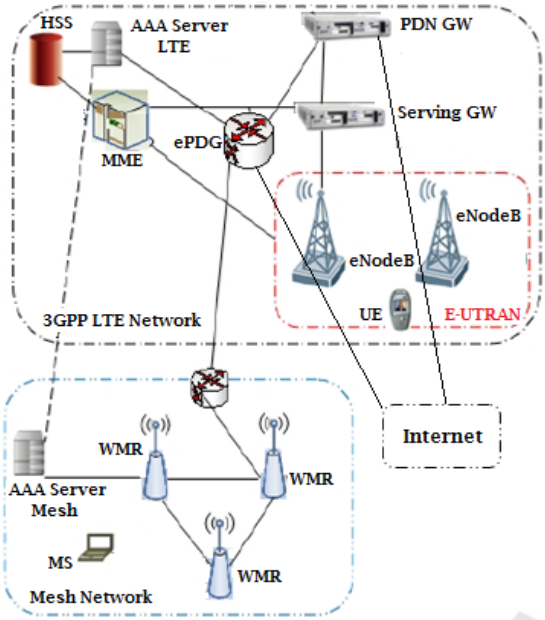

Figure 1: Example of Heterogeneous Wireless Networks topology (LTE-Mesh).

2 RELATED WORKS

The knowledge of the origin of vulnerability serves to protect the network from different types of attacks and even those which may occur in the future.

For this reason, researchers do not stop treating this topic by proposing new solutions and techniques.

A. IP Traceback Techniques

Therefore, there is a variety of IP traceback methods including primarily:

- Probabilistic Packet Marking (PPM) (Savage et al., 2001)
- ICMP traceback (ITrace) (Bellovin, 2000)
- Hash-based IP traceback (Packet logging) (Sager, 1998)
- Hybrid IP traceback (Choi and Dai, 2004)

1) Probabilistic Packet Marking (PPM)

This solution is based on the idea of marking the IP packets. This operation can be performed either by using some bits in the IP packet header, or by generating a new packet based on router's address or a part of its address. This approach has been improved in several works such as Sattari et al., 2010 and Yaar et al., 2005. The choice of marking packets depends on a probability value in the order of 0.04 (Savage et al., 2001).

The major constraint to this method is the need to collect a large amount of packets in order to identify the source of attack. But thanks to works done in Song and Perrig, 2001 as the number was reduced to 1000 packets. In addition, this method uses two additional functions; marking and path reconstruction. This addition, which requires the handling of packets, brings additional work with processor and therefore causes a processing overhead.

Furthermore, the packet can be transformed or modified in order to falsify the traceback results. For this reason, PPM supports different packets transformations within an environment without reflectors to ensure the sureness of IP traceback procedure results. Thanks to its efficiency, PPM can identify the source of majority of DoS and DDoS.

A variety of packets marking techniques have been proposed; we metion as examples the technical Probabilistic Packet Marking (PPM) (Song and Perrig, 2001) and Proactive Signaling Architecture for IP Traceback (PSAT) (Fadlallah and Serhrouchni, 2006).

2) ICMP traceback (ITrace)

This approach is based on the concept of adding a message named "ICMP traceback message" or "ITrace". This idea appeared with Bellovin, 2000. First, the router selects a packet from 20000 forwarding packets. Then, it generates a packet containing the ITrace message. Finally, this information will be forwarded to the same destination.

In order to handle this method, routers must be improved with the aim of designing new services. The scalability is assured because this addition does not affect the operation of other network equipment.

To execute this approach, we need a huge number of packets for the construction of path and the implementation of some additional functions such as the generation of ITrace message. Concerning memory storage, ICMP traceback method does not require a large quantity of additional memory. As with PPM, this method supports the transformation and modification of packets except with reflectors.

3) Hash-based IP Traceback (Packet Logging)

This technique is known as SPIE (Source Path Isolation Engine) (Sager, 1998). The idea is based on saving parts of packets as a digest or a packet signature. The main drawback for this IP traceback solution is the huge amount of resources reserved for storing packet digests. In order to reduce the

required storage space, routers operate a space-efficient data structure technique called Bloom filter (Bloom, 1970).

Concerning the network infrastructure, the packet Logging approach requires the addition of new equipment to ensure the storage packets procedure and to upgrade routers software. Consequently, packet logging approach does not provide the scalability needed in heterogeneous wireless network.

On the other hand, the primary advantage of this technique is the ability to establish the attack path through a single packet. Moreover, even with packet modification or transformation, packet logging is able to provide reliable and effective results for most DoS and DDoS attacks.

4) Hybrid IP Traceback (HIPT)

This method is based on two techniques: Packet Marking and Packet Logging. This alliance benefits from the advantages provided by each approach. Indeed, hybrid IP traceback is characterized by the reduction of reserved resources for packet marking and the utilization of a small number of packets to identify the attack source by using saved digests (Yang and Yang, 2012; Sai Priyanka and Srihari Rao, 2013; Gong and Sarac, 2005). Despite the multiplicity of advantages, this combination does not eliminate the drawbacks brought by the two used techniques.

B. Evaluation of IP Traceback Techniques

This subsection involves a comparative study between the different IP traceback techniques mentioned in the previous subsection (A). Based on Murugesan et al., 2014, a representative method in each category was evaluated. Indeed, the proposed scheme in Goodrich, 2008 was selected to represent the Probabilistic Packet Marking technique. The work in Bellovin, 2000 is chosen as a representative ICMP based traceback technique, SPIE (Snoeren et al., 2002) represents the Packet Logging method and RIHT (Yang and Yang, 2012) is chosen under Hybrid Traceback scheme.

The comparative study of IP traceback techniques is based on the following evaluation metrics:

- ISP Involvement: In order to trace the attack route, in some IP traceback schemes, we call for ISP (Internet Service Provider) intervention to provide some additional information aimed to identify the source(s) of attack.
- Number of attack packets: The number of packets required to determine the source of attack.
- Processing overhead: It represents the additional processing related to the traceback scheme. It can take place in two levels, either in ISP's devices or in the part of victim.
- Protection: To address this matter, we should consider the non-belonging of equipment to its network if this device becomes subverted.
- Scalability: In some traceback schemes, we need to add some new devices in the network. Such complementary equipment may require an independent configuration or with others devices. Thus, minimizing the dependency improves the scalability of the scheme.
- Memory requirement: This represents the quantity of additional storage needed at the network equipment. This metric can be computed in two levels: at the network components (routers and servers) and at the victim levels.
- Accuracy : This metric evaluates the precision of IP traceback method by defining the false positive and the false negative parameters.
- Knowledge of Network : This decides if the IP traceback scheme requires a prior knowledge about the topology of studied network.
- Ability to handle major DDoS attacks: This metric proves the capacity of the scheme to perform the traceback of DDoS attacks under rigorous circumstances such as IP spoofing, and manipulation of reflectors (Mölsä, 2005).

Based on these selected evaluation metrics, Table I illustrates a comparison between different IP traceback techniques.

3 PROPOSED SOLUTION

After studying the different IP traceback approaches, we can conclude that hybrid method is the most suitable approach for the studied network, which is characterized by the variety and the heterogeneity of technologies. On the other hand, this IP traceback technique has proved its efficiency and feasibility.

Table 1: Comparison of IP traceback techniques.

Evaluation Metrics	PPM	ITrace	Packet logging	Hybrid Scheme
ISP Involvement	Fair	Good	Poor (Huge memory requirement)	Fair
Number of attack packets	Large number of packet	Number of ICMP messages and huge number of attack packets	One packet	One packet
Processing overhead (Router)	Medium	Low	High	Low
Protection	Good	Good and practically feasible	Poor	Poor
Scalability	Poor	Good	Fair	Fair
Memory requirement (Network)	Not required	Not required	Very High	Low
Memory requirement (Victim)	Very High	Medium	Not required	Not required
Accuracy	Medium (Huge false positive rate in case of DDoS attack)	Good for less numbers of attackers	Medium with high false positive and false negative	High (less false positive and false negative rate)
Knowledge of Network	Not needed (Faster traceback and low false positive if known)	Not needed	Not needed	Not needed
Ability to handle major DoS attacks	DoS/DDoS flooding attacks	DoS/DDoS network layer attacks	DoS/DDoS flooding attacks	DoS/DDoS flooding attacks

A. Main Idea

In this subsection, we describe the principle of our proposed solution named HITH (Hybrid IP Traceback for Heterogeneous wireless network). This approach needs to meet several specifications related to the studied environment and the conditions of traceback process implementation.

HWN is characterized by a variety of wireless networks in which each category has its own properties. On the other hand, the proposed model allows encompassing the notion of mobility by studying the interworking between different networks and the handover procedure in layer 3.

In order to ensure reliability and robustness of our proposed IP traceback solution and in particular sureness of the established attack paths, the traceback model is based on a set of assumptions:

- Network routers are trusted,
- The attacker does not know in advance the traceback mechanism,
- The IP header can be changeable.

HITH is a hybrid IP traceback method, which owns the packet marking capabilities and the storage of some network information. This combination of two traceback techniques ensures the effectiveness of the proposed approach and the reduction of storage overhead problem.

The principle of HITH method is based on the identification of the first packet for each new connection crossing a new router. Indeed, following the receipt of a packet, the router checks a field called “LogMark”. If it is set to 0, the router proceeds with the logging operation. Otherwise (i.e. the value of “LogMark” is different to 0), the router proceeds by packet marking method.

1) Marking Procedure

In this part, we describe in details the packets marking mechanism at routers for the studied network. First of all, we must point out that our proposed solution is valid for IPv4 packets. And for IPv6 packet, more research and improvements should be procured to HITH since this new version includes new features that should be considered by our method in future work.

The majority of marking approaches use the 3 fields of IP header; “Identification”, “Reserved flag” and “Fragment offset”. Similarly, HITH uses these three fields to perform the marking operation and logging digests at network routers.

- **Identification**

This field is carried on 16 bits. It is useful in the case of packets’ fragmentation, since it designates the fragment number. A study in Stoica and Zhang, 1999 performed in the Internet environment, shows that less than 0.25% of packets crossing the network is fragmented. Therefore, the research community in the field of IP traceback processes the ability to reuse this field for other functionalities.

Indeed, a study of feasibility of this proposal and also of incompatibility problems of that field introduces a topic of discussion in Savage et al., 2001. Ultimately, the obtained results confirm the hypothesis of “Identification” field reusing.

As illustrated in Figure 2, HITH replaces the “Identification” field by two new fields; “LogMark”

and “Router ID”. For “LogMark”, this first element is carried on 2 bits and is used to define the operation to be performed by the router either marking or logging.
A logical combination of two bits can compose four possible values; 00, 01, 10 and 11. This field is initialized to (00) by the first router. Then, it undergoes an incrementation until reaching the last value (11). Afterwards, it returns to the first value (00) and increments once again till the attainment of destination. This value reveals the operation to perform at router level.

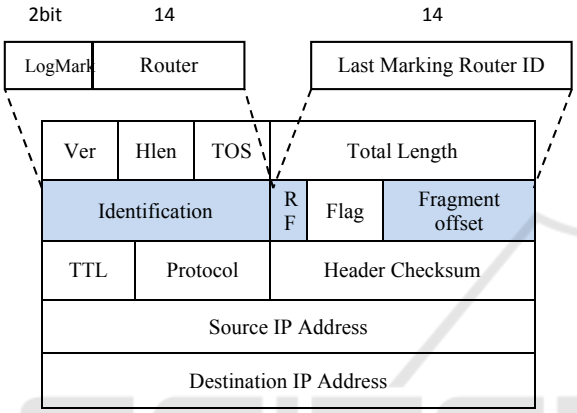

Figure 2: Structure of IP packet Header in marking procedure with HITH.

The second part of “Identification” field indicates the router identifier (Router ID). This information may be fixed to a length of 14 bits based on Muthuprasanna et al., 2006, which illustrates a study performed on the Internet and also the concept of routers neighborhood. Reference Muthuprasanna et al., 2006 asserts that the allocation of 14bits allows identifying routers uniquely.

- **Reserved Flag**

This field is carried on one bit, which is not yet assigned. In the domain of IP traceback, Dean et al., 2002 proposes the use of this field to execute the marking operation.

- **Fragment Offset**

In the IP header and following the packet fragmentation, this field is used to specify the offset of the fragment from the original datagram (64 bit words). But because of the elimination of the “Identification” field, “Fragment offset” becomes useless. This facilitates its exploitation in favor of IP traceback approaches Gao and Ansari, 2005 and Gong and Sarac, 2009.

Indeed, HITH operates these two fields (“Reserved flag” and “Fragment offset”) to denote the identifier of the previous marking router (Last Marking Router ID). This identifier is generated by the network administrator for each traceback-enabled router.

2) Logging Procedure

To pursue and rebuild the attack path and minimize the storage space at routers, various traceback approaches apply hash functions on the data set from the IP packet to extract the digests.

With hash-based approach, digests are derived from the integration of different IP header fields (except TTL “Time To Live”, TOS “Type Of Service” and checksum) with the first 8 bytes of payload. These fields are still operated in the hybrid traceback approach with the addition of a new field named "Logging flag" which introduces the innovation brought by this type of traceback mechanism.

In our solution, HITH calculates the packet digest in the same way as PPIT (Precise and Practical IP Traceback) approach presented in Yan et al., 2012 by integrating diverse parts of the IP header stated in the hybrid approach excluding the TTL field.

- **TTL Integration in Digest**

In this part, we show through an illustrative example the utility behind the addition of TTL field in the input of digests and subsequently in the reconstruction of attack path. In Figure 3, we present a sample network topology exploiting HIPT (Hybrid IP Traceback) approach, composed of 14 routers. The attack path is exposed through continuous red arrows and dotted arrows show the returned path to identify the source of attack.

Since this network adopts our hybrid IP traceback approach, routers (R1, R7, R10 and R14) executes packet digests storage procedure, known by logging and the other routers (R2, R3, R4, R5, R6, R8 R9, R11, R12 and R13) carried out the marking procedure. Following the detection of an attack, the traceback approach begins with the reconstruction of the attack path by identifying the concerned routers. Firstly, the hybrid approach recognizes the first router R14 since it is directly related to the victim.

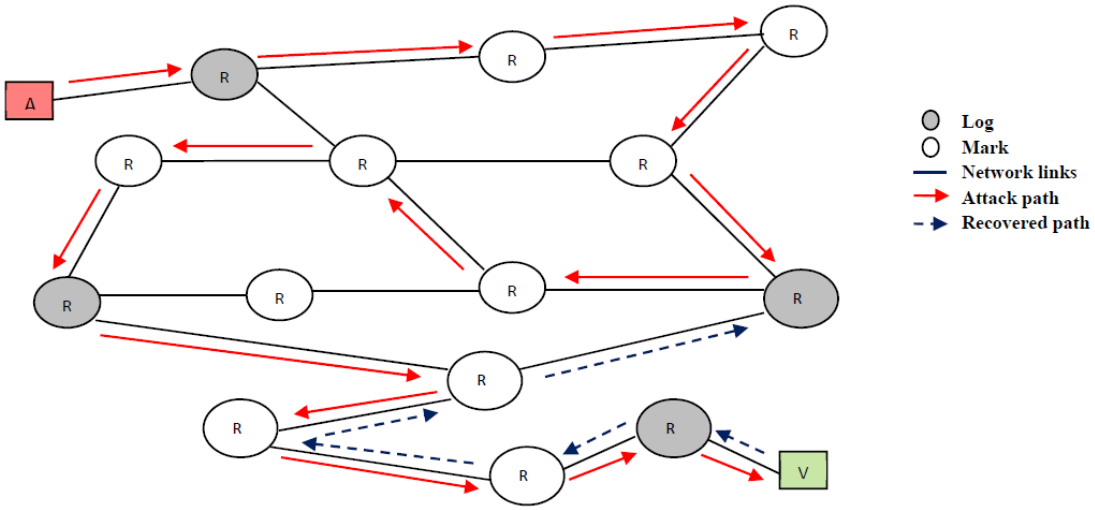

Figure 3: Example of false attack path reconstruction with HIPT.

Thanks to the implementation of the logging operation, we can identify the next router by referring to the router identity recorded in the packet digest. Then, the packet marking provides information on the previous router in the field "Last Marking Router ID" filled in place of “Fragment offset”. On arrival at R11 router, this latter sends queries to its neighbors (R7 and R10), which are both included in the attack path. And since the responses to requests will be received randomly, it can be considered the case where the path is continued with the router R10. Consequently, that may falsify the construction of the attack path.

To remedy this problem, we must differentiate between the two responses received from R7 and R10 by a time reference which may be presented in the IP header by the TTL field. In this case, by comparing the TTL fields from digests of R7 and R10 packets, we find that the TTL value of R7 is lower than that of R10. Thus, this comparison proves that the attack packet has traversed R10 before reaching R7. This scenario can be executed only if we include the TTL field in the logging process as a part of packet digest.

- **Digest Table**

The HITH approach saves packet digests in a digest table implemented with Bloom Filter method (Song and Perrig, 2001), which reduces the storage overhead and makes the storage procedure more convenient. As illustrated in Figure 4, Bloom Filter uses (k) hash functions to calculate (k) distinct packet digests, each one is composed of (n) bits. These results are indexed in a list of (2^n) bits, initialized to 0.

To ensure the rapidity of the reconstruction process of the attack path, we have adopted the idea of multiplying digest tables between neighbors, which is exposed in HIT (Hybrid single-packet IP Traceback) approach (Gong and Sarac, 2008). The routers in this approach are characterized by the management of different digest tables at the same time. Each table is associated with one or more routers identities (Router ID) used in the packet marking procedure.

After extracting the packet digest, this latter will be recorded in digest tables, which are necessarily associated with the router identity supported by the concerned IP packet. Indeed, when a router decides to execute the logging operation, it looks first at the router identity on the contemplated packet (Router ID). Then, it stores the resulting digest in the corresponding table.

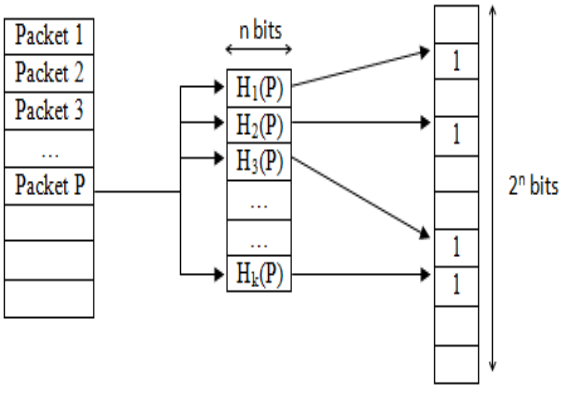

Figure 4: Bloom Filter procedure.

In this context, we note that the existence of a given table depends on the router vicinity, which can find a table with its identity in each of its neighbors.

Therefore, packets from different routers can undergo the logging operation and be stored in different tables simultaneously. This may cause the reduction of access time to digest tables because this parameter is no longer proportional to the packet arrival rate, but also to the maximum rate of arrival packets from the whole neighborhood router.

Despite this reduction, the results of the adopted traceback mechanism remain depending on the capacity of each router essentially the memory access time. Indeed, if a router is characterized by a bad memory access time, it cannot take advantage of traceback mechanism benefits. To remedy this problem, this category of low-speed router profits from access to digest table associated with all neighboring routers, carrying all identities instead of giving each router its own table.

In case of table saturation, packet digests will be archived for a period of time that depends on the configuration and the requirements of the studied network. Thanks to Bloom Filter procedure, the storage overhead of these tables for each router is still negligible and does not affect the network quality of service or the performance of the adopted traceback mechanism.

B. Traceback Process

In order to clarify the steps of identifying attack path by applying our IP traceback approach HITH, we adopt the same network topology mentioned in Figure 3. The studied network has four logging routers (R1, R7, R10 and R14) and the other entities constitute marking routers. First, the HITH procedure identifies R14 since it is directly related to the victim.

Then, it joined to the attack packet the value of R14 router identity, its own TTL value and the different values of the neighboring routers identities. After calculating the digest by exploiting the same hash function as in the logging process, we proceed by comparing the obtained results with the entries in the digest table. In case of correspondence, the concerned router presents the next hop in attack path reconstruction.

After identifying the router R13, the next step is to broadcast queries to all routers' neighbors. Upon receiving this request, each router examines all digest tables referring to the time interval of packet reception to carry on with correspondence. Thanks to the exploitation of TTL value, we avoid the risk of false paths. Therefore, R12 then R11 routers are identified for the attack path reconstruction. Then, we proceed in the same manner to achieve the router R1 in order to rebuild the path leading to the source of attack.

4 PERFORMANCE EVALUATION

In this section, we evaluate our proposed approach HITH with analytical methods by comparing it to some existing solutions: HIT (Hybrid single-packet IP Traceback) (Gong and Sarac, 2008) and SPIE (Source Path Isolation Engine) (Snoeren et al., 2002).

A. Traceback Accuracy

Traceback accuracy presents a very important criterion in the evaluation of IP traceback mechanisms. Indeed, it defines the success rate of attack path reconstruction and subsequently the sureness of the obtained sources. However, a traceback mechanism, which does not ensure this specification, may give false results, incorrect paths, and finally the failure of the traceback procedure.

On the other hand and owing to the adoption of existing techniques in such a traceback mechanism, some imperfections can be inherited from these procedures. For example, we quote the Bloom Filter technique for the management of packet digests in the logging phase. Therefore, we cannot completely eliminate all its problems, but we try to control the selected parameters in order to reduce the resulting anomalies.

In our study, we focus on two parameters: false-positive rate and IP traceback precision.

1) False-positive Rate

Bloom Filter introduces a space-efficient data structure that is used to organize elements and then to check membership in this set. During the phase of membership test, Bloom Filter can produce false-positive results and never false-negative results. We suppose the set of Bloom Filter parameters which is listed in Table II.

The false-positive rate (P) depends on the memory size of Bloom Filter as well as the size of the stored digests. Therefore, it is exponentially related to the value of memory efficiency factor (a / b) (Broder and Mitzenmacher, 2005).

Table 2: Bloom Filter parameters.

Parameter Symbol	Description
A	Number of elements (packets)
B	Number of bits
a/b	Memory efficiency factor
P	False-positive rate
K	Number of hash functions

$$P = \left(1 - \left(1 - \frac{1}{b}\right)^{ka}\right)^{k} \approx \left(1 - e^{-ka/b}\right)^{k} \quad (1)$$

From equation (1), the false-positive rate (P) can be managed and controlled by the right choice of the factor (a / b) (Snoeren et al., 2002) and the (k) hash functions. In our approach, HITH uses Bloom Filter procedure with the addition of the TTL field. This addition does not affect the rate (P) because we use (k) hash functions with the same management of digest table.

2) IP Traceback Precision

This parameter must be taken into account since the design phase of such an IP traceback mechanism to achieve precise and accurate results. Therefore, this precision presents an essential factor in ensuring the success of traceback by tracing the attack path perfectly and identifying the true source of intrusion.

According to the example mentioned in Figure 3, we can conclude that HIT approach still suffers from some problems and precision vulnerabilities that cause the uncertainty of the obtained results. In HITH, this problem is solved by the introduction of TTL field in the packet digest in order to reduce the risk of erroneous and incorrect paths.

B. Storage Overhead

In this part, we borrow the evaluation methods from HIT. Indeed, we evaluate the storage overhead criterion following two parameters:

- Digest Table Storage (DTS): It reveals the quantity of memory required for the registration of packet digests in a router.
- Digest Table Access time (DTA): It designates the number of packet digests stored in a table per time unit.

Similar to SPIE, hybrid traceback approaches can resort to a single packet or transformed packet in order to identify the source of attack. During the design phase of traceback approaches, we must not neglect the case of packets transformation. Indeed, IP packets may undergo various transformations, such as fragmentation and tunneling, crossing the network.

Table 3: Percentages of different types of IP packets.

Type de paquet IP	Pourcentage
1) IP fragments	α
2) Non-fragmented packets to be logged at the router (includes 2.a, 2.b et 2.c)	$(1-\alpha)Y$
2.a) Non-fragmented packet not logged in the two upstream routers.	$(1-\alpha)(1-Y)(1-Y)$
2.b) Non-fragmented packet logged at the upstream router but transformed at the current router.	$(1-\alpha)\,Y\,\beta$
2.c) Non-fragmented packet logged in the upstream router two-hop away and transformed in the current router.	$(1-\alpha)(1-Y)\,Y\,\beta$

In this context and for our HITH approach, stored packets in routers can be:

1) IP fragments.
2) Non-fragmented packets to be logged at the router, comprising the following sub-cases:
   a. Non-fragmented packet not logged in the two upstream routers.
   b. Non-fragmented packet logged at the upstream router but transformed at the current router.
   c. Non-fragmented packet logged in the upstream router two-hop away and transformed in the current router.

Similar to HIT approach, we consider (P_l) the percentage of packets to be logged at a router. We assume (α) to be the percentage of fragmented IP pack.ets and (β) the percentage of transformed packets in the router. In addition, we set (Y) to the percentage of packets to be logged at router without fragmentation. A consolidated list of these percentages is shown in Table III.

According to the parameters listed in Table III, the percentage of all of IP packets to be logged at the router is expressed by:

$$P_l = \alpha + (1 - \alpha)\,Y \quad (2)$$

The percentage of packets to be logged without fragmentation is:

$$Y = \frac{P_l - \alpha}{1 - \alpha} \quad (3)$$

And

$$1 - Y = \frac{1 - P_l}{1 - \alpha} \quad (4)$$

Since the second case of fragmentation includes three possible scenarios, (Y) can be expressed by the following equation:

$$Y = (1-Y)^2 + Y\beta + Y(1-Y)\beta \quad (5)$$

We replace the value of (Y) by (3) and $(1-Y)$ by (4) in (5), we obtain:

$$P_l = 1 - \frac{(1-\alpha)\left(\sqrt{1+4(1-\beta)^2}-1\right)}{2(1-\beta)} \quad (6)$$

Some measurement studies have proved that $\alpha \leq 0.25\%$ (McCreary and Claffy, 2000) and $\beta \leq 3\%$ (Broder and Mitzenmacher, 2005), (Stoica and Zhang, 1999). Therefore, we observe that:

$$0.382 \leq P_l \leq 0.392 \quad (7)$$

The obtained result demonstrates that 39% of packets crossing a router require the execution of logging operation. On the other side, with HIT approach and according to (Gong and Sarac, 2008), the result is expressed by:

$$0,50 \leq P_l \leq 0,51 \quad (8)$$

This means that 50% of IP packets must be logged in the current router. In SPIE approach, all packets crossing the router require the execution of logging operation.

If we consider DTS_H, DTS_I and DTS_S the values of DTS in HITH, HIT and SPIE approaches can be given by:

$$DTS_H = P_l \times DTS_S \approx \frac{2}{3} DTS_I \approx \frac{2}{5} DTS_S \quad (9)$$

In addition, for our approach, logging packets can be performed in multiple neighboring routers simultaneously as detailed in digest table part. Therefore, the rate of access to a digest table may be reduced with the number of existing neighbors in network. We suppose that a router has (n) neighbors. In the ideal case where the traffic arrives to router in a balanced way from each neighbor, and:

$$DTA_H = P_l \times \frac{1}{n} DTA_S \cong \frac{2}{5} \times \frac{1}{n} DTA_S \quad (10)$$

$\mathrm{DTA_H}$ and $\mathrm{DTA_S}$ represent the access time to digest table with HITH and SPIE approaches, respectively.

In the worst case, where all the traffic is derived from a single neighbor $(n = 1)$, we note that:

$$DTA_H = P_l \times DTA_S \cong \frac{2}{5} \times DTA_S \quad (11)$$

5 CONCLUSION

To ensure a more effective and precise IP traceback technique, the research community resort to combine the two existing approaches; packet marking and packet logging to establish a hybrid approach. Although this method inherits the benefits provided by each category, it still suffers from some vulnerability. Indeed, the hybrid IP traceback approach can cause incorrect paths due to accuracy problems. In addition, overhead storage remains high because of the inefficient use of the marking space.

In this paper, we have proposed a novel Hybrid IP Traceback approach for Heterogeneous wireless networks, which is called HITH. Our solution is based on some supplementary information added in the reconstruction of the attack path to avoid incorrect results. Moreover, HITH defines an efficient mechanism to reduce storage overhead by distributing the marking and logging roles between routers. Besides, in order to decrease the digest table access time, we have gathered the log information in multiple routers taking into account the notion of neighborhood and the limitation of some network equipment capacities. The effectiveness of the proposed IP traceback approach is proved by mathematical analysis. Indeed, HITH incurs little overhead at routers, improves accuracy and reduces overhead storage and data access time. As a future work, we will evaluate HITH by simulation analysis.

REFERENCES

Ren, W., Zhao, Q. and Swami, A., "Connectivity of Heterogeneous Wireless Networks". *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4315-4332, July 2011.

Houle, K. J. and Weaver, G. M., "Trends in Denial of Service Attack Technology". *Computer Emergency Response Team (CERT) Coordination Center, technical report v1.0*, October 2001.

Phatak, D., Sherman, A. T., Joshi, N., Sonawane, B., Relan, V. G., Dawalbhakta, A., "Spread identity: A new dynamic address remapping mechanism for anonymity and DDoS defense". *Journal of Computer Security*, vol. 21, no. 2, pp. 233-281, 2013.

Savage, S., Wetherall, D., Karlin, A. and Anderson, T., "Network Support for IP Traceback". *IEEE/ACM Transactions on Networking (TON),* vol. 9, no. 3, pp. 226-237, June 2001.

Bellovin, S. M., "ICMP Traceback Messages", *IETF draft*, 2000,

http://www.research.att.com/smb/papers/draftbellovin-itrace-00.txt.

Sager, G., "Security Fun with OCxmon and cflowd". Internet2 Working Group Meeting, November 1998, http://www.caida.org/funding/ngi/content/security1198.

Choi, K. H. and Dai, H. K., "A marking scheme using Huffman codes for IP traceback". *7th International Symposium Parallel Architectures, Algorithms Networks (I-SPAN'04)*, pp. 421–428, Hong Kong, China, May 2004.

Sattari, P., Gjoka, M. and Markopoulou, A., "A network coding approach to IP traceback". *IEEE International Symposium on Network Coding (NetCod'10)*, pp. 1-6, Toronto, Canada, June 2010.

Yaar, A., Perrig, A. and Song, D., "FIT: Fast internet traceback". *IEEE Conference on Computer Communications (INFOCOM'05), vol. 2*, pp. 1395-1406, March 2005.

Song, D. X. and Perrig, A., "Advanced and Authenticated Marking Schemes for IP Traceback". *IEEE Conference on Computer Communications (INFOCOM'01), vol. 2,* pp. 878-886, Arkansas, USA, April 2001.

Fadlallah, A. and Serhrouchni, A., "PSAT: Proactive signaling architecture for IP traceback". *IEEE 4th Annual Communication Networks and Services Research Conference (CNSR'06)*, pp. 293-299, Washington, DC, USA, May 2006.

Bloom, B. H., "Space/time trade-offs in hash coding with allowable errors". *Communications of ACM, vol. 13*, no. 7, pp. 422-426, July 1970.

Yang, M. H. and Yang, M. C., "RIHT: A Novel Hybrid IP Traceback Scheme". *IEEE Transactions on Information Forensics and Security, vol. 7*, no. 2, pp. 789-797, April 2012.

Sai Priyanka, B. and Srihari Rao, N., "IP Traceback Techniques – A Selective Survey". *International Journal of Computer Science and Mobile Applications, vol. 1*, no. 3, pp. 40-44, September 2013.

Gong, Ch. and Sarac, K., "IP Traceback based on Packet Marking and Logging", *IEEE International Conference on Communications (ICC'05), vol. 2*, pp. 1043-1047,16-20 May 2005.

Murugesan, V., Shalinie, M., Neethimani, N., "A Brief Survey of IP Traceback Methodologies". *Acta Polytechnica Hungarica, vol. 11*, no. 9, pp. 197-216, 2014.

Goodrich, M. T., "Probabilistic Packet Marking for Large Scale IP Traceback". *IEEE/ACM Trans. Networking, vol. 16*, no. 1, pp. 15-24, February 2008.

Snoeren, A. C., Partridge, C., Sanchez, L., Jones, C., Tchakountio, F., Schwartz, B., Kent, S. and Strayer, W., "Single-packet IP traceback". *IEEE/ACM Transactions on Networking, vol. 10*, no. 6, pp. 721-734, 2002.

Mölsä, J., "Mitigating denial of service attacks: A tutorial". *Journal of Computer Security, vol. 13*, no. 6, pp. 807-837, 2005.

Stoica, I. and Zhang, H., "Providing guaranteed services without per flow management". *ACM conference on Applications, technologies, architectures, and protocols for computer communication (SIGCOMM'99), vol. 29*, no. 4, pp. 81-94, Cambridge, MA, USA , October 1999.

Muthuprasanna, M., Manimaran, G., Manzor, M., and Kumar, V., "Coloring the internet: IP Traceback". *12th International Conference on Parallel and Distributed Systems (ICPADS'06)*, pp. 589-598, Minneapolis, USA, August 2006.

Dean, D., Franklin, M. and Stubblefield, A., "An algebragic appproach to IP traceback". *ACM Transactions on Information and System Security, vol. 5,* no. 2, pp. 119-137, 2002.

Gao, Z. and Ansari, N., "Enhanced probabilistic packet marking for IP traceback". *IEEE Global Telecommunications Conference (GLOBECOM'05), vol. 3,* pp. 1676-1680, 28 November - 2 December 2005.

Gong, C. and Sarac, K., "Toward a practical packet marking approach for IP traceback". *International Journal of Network Security, vol. 8*, pp. 271-281, 2009.

Yan, D., Wang, Y., Su, S. and Yang, F., "A Precise and Practical IP Traceback Technique Based on Packet Marking and Logging". *Journal of Information Science and Engineering, vol. 28*, pp. 453-470, 2012.

Gong, Ch. et Sarac, K., "A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking". *IEEE Transactions on Parallel and Distributed System, vol. 19*, no. 10, pp. 1310-1324, October 2008.

Broder, A. and Mitzenmacher, M., "Network applications of Bloom filters: A survey". *Internet Mathematics, vol. 1*, no. 4, pp. 485-509, 2005.

McCreary, S. and Claffy, K., "Trends in wide area IP traffic patterns: A view from Ames internet exchange". *13th ITC Specialist Seminar on IP Traffic Modeling, Measurement and Management*, pp. 1-25, Monterey, CA, USA, 2000.