Communications and Network, **2013, 5, 478-484**
http://dx.doi.org/10.4236/cn.2013.53B2088 Published Online September 2013 (http://www.scirp.org/journal/cn)

A Coding-Based Incremental Traceback Scheme against DDoS Attacks in MANET

Qiang Jiang, Yinan Jing*, Xiaochun Xiao, Xueping Wang
School of Computer Science, Fudan University, Shanghai, China
Email: jiangqiang@fudan.edu.cn, *jingyn@fudan.edu.cn, xxiaochun@fudan.edu.cn, wangxp@fudan.edu.cn

Received April 2013

ABSTRACT

Due to constrained resources, DDoS attack is one of the biggest threats to MANET. IP traceback technique is useful to defend against such type of attacks, since it can identify the attack sources. Several types of traceback schemes have been proposed for wired networks. Among all the existing schemes, probabilistic packet marking (PPM) scheme might be the most promising scheme for MANET. However its performance in MANET is not as good as that in Internet. In this paper, a new scheme based on the coding technique (CT) is proposed for traceback in MANET. Furthermore, a new idea of Incremental traceback is raised to cope with the situation of incremental attack (ICT). We present the protocol design and conduct theoretical analysis of this scheme. Additionally, we conduct experiments to compare it with the traditional PPM scheme. The experimental results show that the new coding-based traceback scheme outperforms the PPM scheme in MANET.

Keywords: IP Traceback; MANET; Coding; DDoS; Incremental Traceback

1. Introduction

A Mobile Ad hoc Network (MANET) is a collection of wireless nodes that is capable of keeping the network connected without the support of a predefined network infrastructure or any centralized administration. Beyond that, nodes in such a network are often mobile. MANET is an emerging research area with practical application, such as battlefield communication, emergency services, disaster recovery, environment monitoring, personal area networking, etc. However, MANET is particularly vulnerable to network attacks. That may be attributed to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, constrained bandwidth, and limited computing resource. These properties make it much easier to be subjected to attacks compared to wired networks [1].

Although several types of attacks in MANETs have been studied in the literature, the denial-of-service (DoS) attack may be the most serious attack. When the attack-traffic comes from multiple sources, it is called a distributed denial-of-service (DDoS) attack. By leveraging multiple attack sources, the power of a DDoS attack is amplified and the problem of defense becomes more complicated. Many facts show that DDoS attacks have brought serious financial losses to Internet [2]. Furthermore, with its constrained resources, MANET is deemed to be more vulnerable to DDoS attacks than wired networks [3]. Additionally, it is more difficult to defend against these DDoS attacks because of some inherent properties of MANET, including dynamic topology and autonomous principle.

IP traceback is one of the effective countermeasures against DDoS attacks. It allows the victim to identify the attack sources even in the presence of IP spoofing. [4] has shown traceback results which are helpful to defeat DDoS attacks. Furthermore, a well-established traceback system can play a key role in deterring attackers, so that it can curb the spreading of attacks to a certain extent. Currently, various schemes have been proposed for Internet [5]. However, these existing traceback schemes cannot be directly applied to MANET for various drawbacks.

Among all the existing traceback schemes, Probabilistic Packet Marking (PPM) schemes might be the most promising one for traceback in MANTE, because it is more lightweight on the network overhead and node overhead than other schemes. However, in MANET it does not work as well as in Internet, since it has some drawbacks. First, the marked information might be overwritten by downstream nodes, so that the upstream nodes' information cannot be easily conveyed to the victim. In other words, its traceback speed is not that fast to adapt

*Corresponding author.

to the dynamic changes of MANET. Second, it has to rely on a premise that the attacking paths are static, but this condition is hard to meet in MANET. If we are not able to take measures to defeat the attackers before the paths change, all the effects made are in vain. Even though we give a relative stable topology for PPM, we cannot ensure it work very well [6].

In this paper, a coding-based traceback (CT) scheme is proposed. By leveraging the coding technique, the node information of different attacking source nodes can be combined into one code by the intermediate nodes. Furthermore, we first propose a new idea of incremental traceback to solve the problem of incremental DDoS attack.

2. Coding-Based Traceback in MANET

The main idea of the CT scheme can be expounded as following steps. Firstly, every node in the network will play the role of monitor. They will monitor all the incoming data flows. When one suspects that its upper node is sending attack packets, it will encode its identity information (such as IP address) with a randomly generated coefficient. Secondly, it will send this encoded value to the suspected victim. Thirdly, the intermediate node will receive the coding information from different incoming links and store them into their coding cache. Then it will encode all those coding values. After that, it will send the new coding value to the downstream node. Finally, if the destination node (victim) has detected that it is under an attack, it will decode the source node information from those received coded values with the corresponding coefficients. Thus, it will be able to traceback the attackers. The above-mentioned traceback steps are illustrated in **Figure 1**.

2.1. Encoding Procedure

The encoding procedure is about two questions: what to encode and how to encode?

As for the first question, there are two situations. If the node is source node like x_i, it will encode its own identity. If the node is an intermediate node like m_i, it will encode all the codes coming from ingress edges. We first discuss Besides, we will consider what to be coded will be most suitable and when will be the best time. As for the second question, we propose to use the random linear coding method, which was first described in [7]. That is each link carries a linear combination of codes from incoming links. The linear coefficients for each link are independently and randomly selected from a finite field. Encoding with random numbers is a more efficient manner in a large distributed system than with determined ones. In determine coding, every node adopts determined encoding coefficients. Although it only requires a small set of coefficients and costs less in carrying coefficient information, determine coding needs to acquaint with the topological-structure of the whole network in advance, which makes it more complex. However, the topology of MANET is changing dynamically, making the encoding system to be updated with huge management overhead. Therefore, we adopt the random linear coding method and explain how it works in detail.

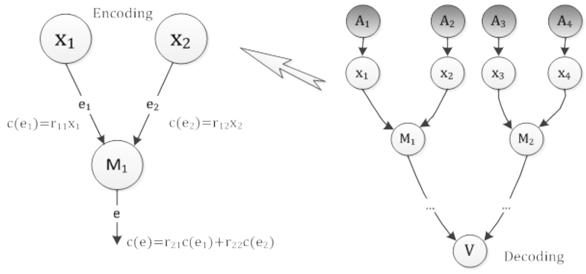


Figure 1. The process of CT.

Take a network $G = (V, E)$ as an example, where V is a set of vertices, and E is a set of edges. As for the source node, it will choose a random number as the encoding coefficient. For example, x_1, x_2 randomly choose r_{11}, r_{12} to encode with respectively and send to downstream nodes. As for the intermediate node, it will encode the codes from ingress edges together and generate a new code for the egress edge. For example, m_1 will encode the $c(e_1)$ and $c(e_2)$ from ingress edges $e_1$and e_2, and then get a new code $c(e) = r_{21}*c(e_1) + r_{22}*c(e_2)$ for the egress edge as shown in **Figure 1**.

Generally speaking, we assume there are k ingress edges (e_k) to a node, then the code generate by this node is: $c(e)=\sum_{i=1}^{k} r_i * c(e_i)$.

Making this coding-based scheme practical relies on three key ideas: random encoding, packet tagging, and buffering. Random encoding and tagging allow this scheme to proceed in a distributed manner. Buffering allows for asynchronous packet arrivals and departures with arbitrarily varying rates, delay, and loss. The CT scheme uses a Coding Hash Table (CHT) to record the coded information from upstream node. Every intermediate node has one CHT, storing the codes, with hashed MAC address of the upstream node as the key as **Figure 2** shows. Each of the table entry contains a timestamp to record the code's latest access time. The hash table can be cleaned regularly based on timestamp to make more space available for updated coded information.

In the encoding process, the intermediate node generates random numbers as encoding coefficients and encodes the code in the table with them. Encoding time is used to describe the proper time an encoding operation is triggered. Intermediate node receives a packet transmit-

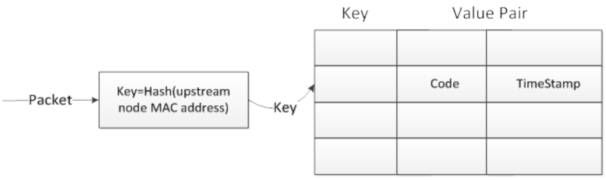


Figure 2. Code Hash Table.

ted from the upstream node and determines whether it has received information from this node or not. If it has received and has updated the CHT, the intermediate node will not encode this packet and does nothing to the table. If not, the received code will be written to the CHT in the form as "Key, Code, Time Stamp". Finally, the intermediate node encodes all the codes in the table with randomly selected coefficients.

The encoding algorithm is depicted in **Algorithm 1**.

Algorithm 1. CT encoding algorithm.

```
Procedure Encoding(n, w, v)
For each packet w to v, encoding in the node n
    if(w.code != null)   /*if the packet contains code */
    /*decide whetherCHT record the codefrom upper node*/
        bRecorded = SearchCHT(HashKey(w.MAC));
        if (bRecorded == Flase)  /*if not recorded*/
            Let   old= the last record in CHT for v;
            Let   new=CreateRecord(HashKey(w.MAC));
            Let r1, r2 be two nonzero random numbers;
            new.code = r1*old.code+r2*w.code;
            new.TimeStamp= old.TimeStamp= now();
            UpdateCHT();
            w.code = new.code;
    else
        Let r be a random number
        w.code = r*n.IP;
```

2.2. Decoding Procedure

In ad hoc networks, the generation and transmission of the coding information is not synchronized, and links are not stably connected. The application of random liner coding makes it possible to calculate the global coefficient for a source node and decode with enough coded information. The decoding can be done by Gaussian elimination [8].

We assume a single attack pathwith d hops between the attacker and the victim. $X = (x_1, x_2, \ldots\ldots, x_n)$ is a set of source nodes near to n attackers. $R_{ij} = (r_{i1}, r_{i2}, \ldots, r_{id})$ stands for the coefficient vectorwhich acts on x_i along the path in the j round of encoding. We can calculate the global coefficient a_{ij} in a recursion manner, and get final code value *yi*:

$$\alpha_{ij} = \prod_{h=1}^{d} r_{ih}, y_i = \sum_{i=1}^{n} \alpha_{ij} x_i \qquad (1)$$

For all the sources $(x_1, x_2, \ldots\ldots, x_n)$, we will get the global coefficient vector $(\alpha_{1j}, \alpha_{2j}, \ldots\ldots, \alpha_{nj})$. The victim receives $y_1, y_2, \ldots, y_n$ and get the matrix as follows:

$$\begin{bmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{bmatrix} = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix} \qquad (2)$$

The equation set can be solved with high possibility.

2.3. Incremental Traceback

In some situation that all DDoS attack won't occur at a same time. The cunning attackers may adopt the strategy to carry on their attack increasingly to confuse the target. Furthermore, more than one attacks may occurs in a period of time. It is a good idea if we can take advantage of the decoded sources to traceback the latest one. We propose a new idea of Incremental coding-based traceback (ICT) to achieve such goal.

Since the coding system is distributed, it is impossible to receive all necessary information at the same time and to decode all the attack sources in a multi-source attack. The coding procedure is asynchronous and the number of the sources is indeterminate. It will cost much more time and computing resources if solving out all of the sources simultaneously in the manner of Gaussian elimination. Hence, we require a more efficient method. It works as follows. First, we use a collector to store the coding coefficients and the corresponding codes in a queue. For that the encoding is incremental, we can easily get the first source node x with little information. Second, we store the resolved source x in another queue andsolve the following equations with the help of x. In this way, we can find out the sources gradually with fewer packets.

On the other hand, CT scheme make it possible for the intermediate nodes to store coding messages. The following occurred attacks which route to the same target through these intermediate nodes will benefit from the stored message stated above and gain a high performance. Thus realize incremental traceback.

3. Analysis

Before analyzing the performance, we do qualitative compare about CT and PPM. Firstly, they differ in what they mark. The intermediate nodes in CT will encode the received messages and mark them while PPM will mark the intermediate nodes' address and overwritten the previous ones. Thus PPM needs to cost a large number of packets to recover the attack path. Secondly, they differ in what they obtain. CT cares about the source address rather than the attack path. It is very important in MANET. With the change of topological structure, the attacking paths will change as well. If we fail to recover the paths before the change of routing, all works will be in vain. Finally, CT scheme has a better performance in multi-sources situation. According to the theory of Network Coding, there will be higher transmission efficiency. Therefore, the traceback speed of CT will be faster. Generally speaking, there is much difference between CT and PPM.

Definition 1. Convergence. It refers to the time when it is able to traceback all the sources.

Definition 2. Convergence Time (T). The convergence time of a traceback scheme is defined as the least number of packets required for convergence.

Convergence time reflects the traceback speed. Obviously, the less convergence time, the better traceback performance. We will compare the convergence time of PPM scheme and CT scheme by theoretical analysis.

We let *d* denote the length of one attack path, *i.e*. the number of intermediate nodes in a single attacking path. According to CT, the convergence time is:

$$T_{CT} \approx 1 + \left(d - 1\right) = d \tag{3}$$

According to the PPM scheme, the expected value of the convergence time of PPM [9] is:

$$E\left(T\right)_{PPM} \approx \frac{\ln\ln\left(d\right)}{p\left(1-p\right)^{d-1}} \tag{4}$$

Now let's prove that the convergence time of CT is less than that of PPM. Here, we try to find the minimum of $E\left(T\right)_{PPM}$ to compare with T_{CT}.

First, we calculate the derivative

$$\frac{dE\left(T\right)_{PPM}}{dp} = \ln\ln\left(d\right) p^{-2}\left(1-p\right)^{-d}\left(dp-1\right) \tag{5}$$

If $p = \frac{1}{d}$, we get the minimum of $E\left(T\right)_{PPM}$

$$\min(E\left(T\right)_{PPM}) = \frac{\ln(d)}{\frac{1}{d}(1-\frac{1}{d})^{d-1}} \tag{6}$$

We divide $\min(E\left(CT\right)_{PPM})$ by *d*.

$$\min(E\left(T\right)_{PPM})/d = \frac{\ln\ln\left(d\right)}{\frac{1}{d}\left(1-\frac{1}{d}\right)^{d-1}}/d = \frac{\ln\ln\left(d\right)}{\left(1-\frac{1}{d}\right)^{d-1}} \tag{7}$$

The length of the path (*d*) is certainlylonger than 1, *i.e.* *d* > 1. Obviously, the formula above would be greater than 1. That means $\min(E\left(CT\right)_{PPM}) > T_{CT}$. Therefore, we come to the conclusion that the convergence time of CT is less than that of PPM.

4. Simulation

In this section, we provide experiments to analyze the performance of the CT scheme as well as the PPM scheme on Glomosim 2.03 [10]. We implement PPM based on AODV routing protocol and IR-AODV (Identity Replacement based AODV) protocol [6] proposed by us, which is a routing protocol with stable topology support. **Table 1** shows some detailed experiment environment settings.

1) Performance of Traceable Ratio

Definition 3. Traceable Ratio. It is defined as the ratio of the number of successful traceback to the total number of traceback attempts.

Due to dynamic changes of topology, the traceback performance in MANET cannot simply be evaluated by the convergence time metric.Hence, we define a new metric called traceable ratio. **Figure 3(a)** illustrates the traceback ratio of CT, PPM on AODV and PPM on IR-AODV when the wireless node's transmission range varies from 150 m to 300 m. Moving speed is 10 m/s. **Figure 3(b)** shows the traceback ratio with different moving speed. Here each node has a transmission range about 250 m. The marking probability of the PPM scheme is set to 0.4. From both figures, we see that although PPM with stable topology support in MANET has a better traceable ratio, it still work more badly than CT. We can see that CT has a perfect performance. It can almost achieve a 100% traceable ratio.

2) Performance of Traceback Convergence Time

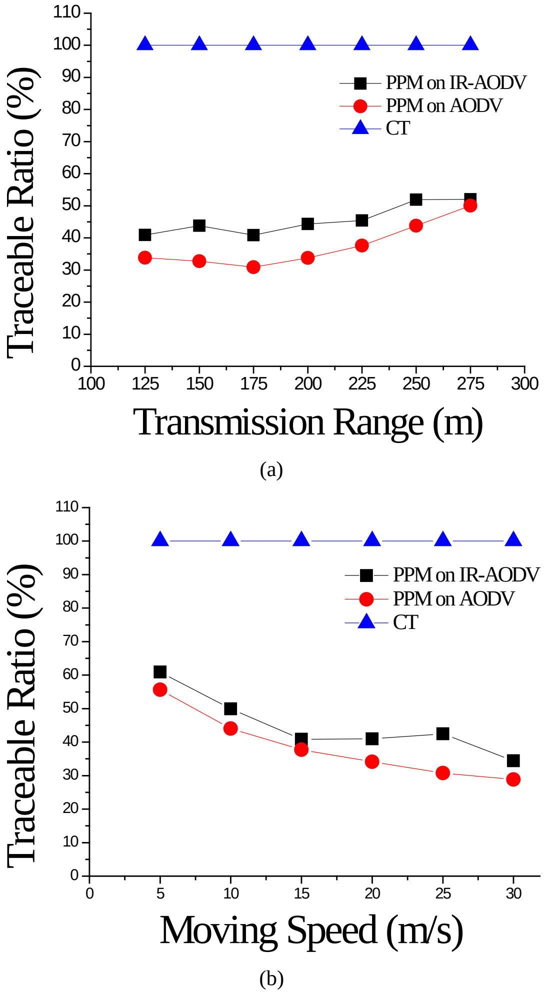
In the following experiments, we analyze the convergence time of the two schemes under different transmission ranges and different moving speeds.

Figure 4(a) depicts the variation of convergence time of PPM on AODV, PPM on IR-AODV and CT when we let the transmission range vary from 125 m to 325 m with the moving speed 10 m/s. **Figure 4** depicts the variation of convergence time of the three schemes when we let the moving speed changing from 5 to 30 m/s with the transmission range 250 m.

From **Figure 4(a)** we get the conclusion that the convergence time will get shorter as the transmission range getting larger, because there are fewer hops from the source to the destination when the transmission range becomes large. Furthermore, the performance of CT is

Table 1. Experiment Environment Settings.

Parameter	Value
TERRAIN	1500 m × 900 m
NODES	100
NODE-PLACEMENT	RANDOM
MOBILITY MODEL	Random Way Point (pause 30 sec)
MAC-PROTOCOL	802.11
ROUTING-PROTOCOL	AODV/IR-AODV
DATA-TRAFFIC	CBR (packet size = 512 B)



(a)

(b)

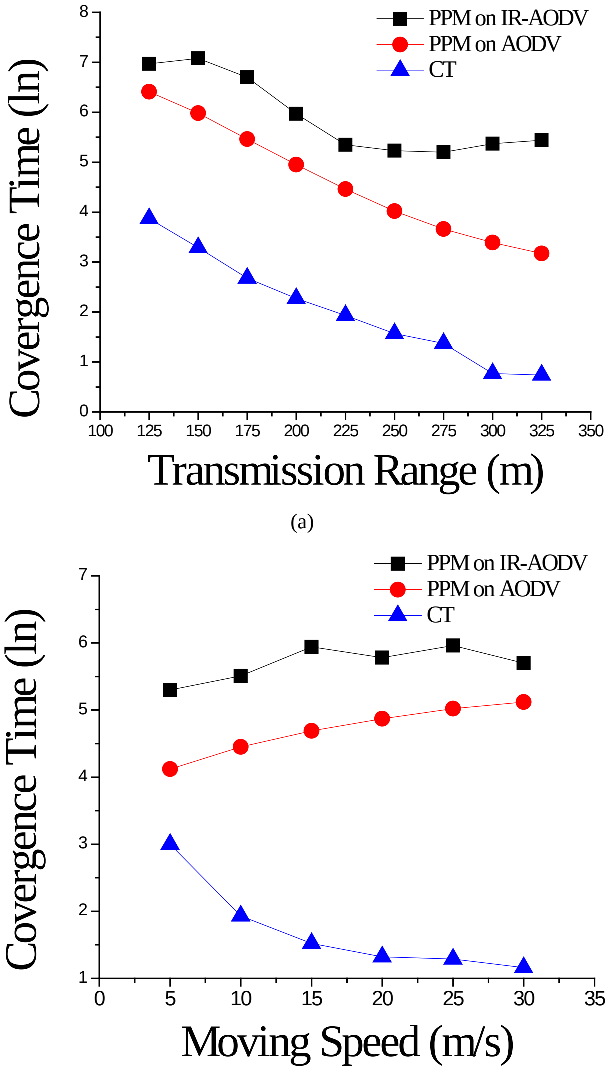
Figure 3. (a) and (b).

better than the other two. From **Figure 4(b)** we know the changing patterns of convergence time versus different moving speed are very much different. The convergence time is getting smaller in CT as the nodes moving faster and faster, while the others having adverse tendency. The moving speed is one of the factors affecting the topology stability. CT scheme is less affected. To the contrary, as source nodes or the intermediate nodes moves, they carry the related coding information as well, which may give it more chance to connect to the destination and leads to less consumption of necessary packets.

3) Performance of traceback for multi-source attacks

Figure 5 shows the convergence time of ICT in multi-source attack scenarios. The proportion of attack nodes to all the nodes change from 1% to 50% while the transmission range of each node is 250 m and the moving speed 10 m/s. Standard means the linear growth of convergence time.

We firstly elaborate the convergence time in multi-source condition. We suppose all the sources are attacking at the same time and we do trace at the same time as



(a)

(b)

Figure 4. (a) and (b).

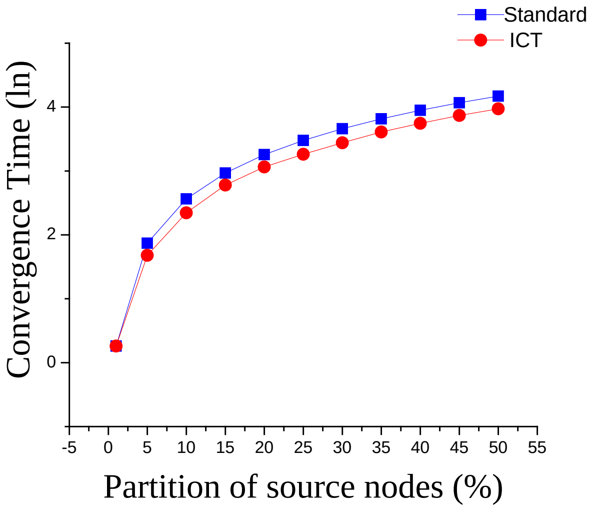


Figure 5. Convergence Time vs. Attack nodes proportion.

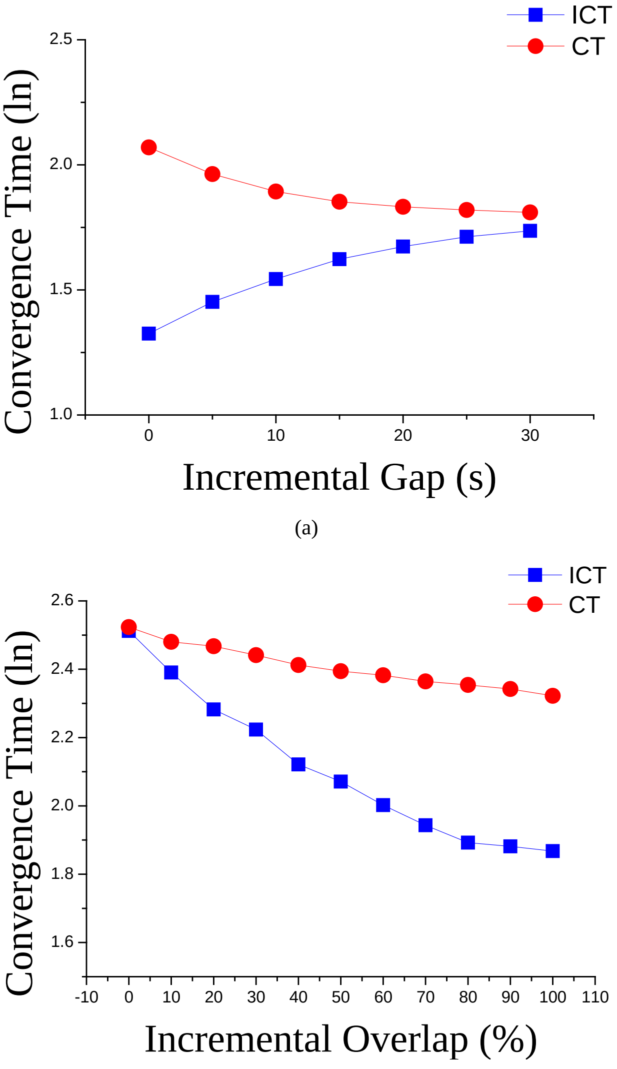
well. The sources will be traced gradually, and we define the packets needed to traceback the last attacker as the convergence time. We can see that when the number of sources increases several times above, the convergence time not increase at the same way. With the help of coding during the transmission, the intermediate nodes will combine the codes of different sources together. Therefore, the CT scheme can fully take the benefits of coding when tracing multiple attackers.

4) Performance of Incremental Traceback

Figure 6 depicts the convergence time of CT and ICT in an incremental attack situation. The simulation is conduct in the environment of 10 m/s moving speed, 250 m transmission range, based on AODV.

Figure 6(a) shows the situation of two phases attack with each phase 10 nodes. Incremental gap is the time gap of two attacks and it changes from 5 to 30 s. From the figure, we can come to the conclusion that the performance of ICT is much better than CT. CT shows a downward trend because when two attacks are to close, the network will be too crowd that leads to longer delay. ICT shows an upward trend because with the increasing of gap, the two attacks will tend to be independent.

Incremental overlap means the amount of sources of two phase attacks that are overlapped. **Figure 6(b)** indicates the relationship between incremental overlap and convergence time. The transmission range is 250 m and moving speed is 10 m/s. There are 20 nodes at the first attack. The incremental overlap changes from 0% to 100%. From the figure we can find that both CI and ICT performance better with the increase of incremental overlap and ICT is much better. ICT can achieve a good performance brought by Incremental Traceback. If the groups are more overlapped, better performance can be obtained with the storage of decoded sources.



(a)

(b)

Figure 6. (a) and (b).

5. Related Work

The traceback technology against DDoS attacks is well developed in Internet [6]. IP traceback techniques in wired network can be classified into three general categories. First are logging-based traceback schemes, such as CenterTrack [12] and Hash-based IP traceback [13]. Second are ICMP-based traceback schemes called iTrace [11]. Third are packet-marking schemes, such as the typical Probabilistic Packet Marking (PPM) [9]. However, due to different reasons, these schemes for wired networks are not suitable for resource constrained MANET directly.

The traceback problem in wireless ad hoc network is first addressed by Vrizlynn L. L. Thing *et al* [14]. The existing traceback schemes for wireless ad hoc networks are mostly inherited from Internet and further modified. They can also be classified into the same three categories as those for wired networks. Based on ICMP technique, besides iTrace-CP method proposed by Vrizlynn, Kim studied out a scheme researching on flow characteristic. Hotspot-based Traceback [15], CAPTRA [16], the scheme proposed by Kim *et al* [17] and SWAT [18] are logging-based traceback schemes for wireless network. The above-mentioned schemes [15-18] mainly inherit from the Hash-based approach. The researches on PPM in ad hoc networks mainly focus on the traceback performance. Cheng *et al* [19,20] try to minimize the convergence time to reduce the influence of dynamic topology. Jin proposed a new scheme called zone sampling-based trackback (ZSBT) [21] and Yang [22] use the recorded network topology snapshots to proofread the tracking results. Das *et al* [23] proposed an incremental computing method to reflect the change of the topology. However, it can only trace DoS attacks with a single attack source.

6. Conclusion

In this paper, we first analyze the existing problems when conducting traceback against DDoS attacks in MANET, and the problems when we apply PPM scheme to MANET. To achieve the goal of high tracing efficiency, we proposed a coding-based traceback scheme. We detail the encoding and decoding procedures of this scheme and analyze the traceback performance in a theoretical way. Furthermore, we compare the performance of CT with PPM and we can see that the performance of CT is better than PPM in both traceable ratio and convergence time.

REFERENCES

[1] H. Yang, H. Y. Luo, F. Ye, S. W. Lu and L. X. Zhang, "Security in Mobile Ad Hoc Networks," *IEEE Wireless Communications Challenges and Solutions*, Vol. 11, No. 1, 2004, pp. 38-47. http://dx.doi.org/10.1109/MWC.2004.1269716

[2] D. Moore, G. Voelker and S. Savage, "Inferring Internet Denial-of-Service Activity," 10*th ACM USENIX Security Symposium*, 2002, pp. 9-22.

[3] I. Aad, J. P. Hubaux and E. Knightly, "Impact of Denial of Service Attacks on Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, Vol. 16, No. 4, 2008, pp. 791-802. http://dx.doi.org/10.1109/TNET.2007.904002

[4] Y. Jing, X. Wang, X. Xiao and G. Zhang, "Defending Against Meek DDoS Attacks By IP Traceback-based Rate Limiting," 49*th GLOBECOM* 2006, San Francisco, November 2006.

[5] A. Belenky and N. Ansari, "On IP Traceback," *IEEE Communications Magazine*, Vol. 41, No. 7, 2003, pp. 142-153. http://dx.doi.org/10.1109/MCOM.2003.1215651

[6] Y. Jing, X. Wang, L. Zhang and G. Zhang, "Stable Topology Support for Tracing DDoS Attackers in MANET," 54*th GLOBECOM* 2011, Houston, December 2011.

[7] R. Ahlawede, N. Cai, S. R. Li and R. W. Yeung, "Network Information Flow," *IEEE Transactions on Information Theory*, 2000.

[8] Wikipedia. Gaussian Elimination. http://en.wikipedia.org/wiki/Gaussian_elimination

[9] S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Practical Network Support for IP Traceback," *ACM SIGCOMM Computer Communication Review*, Vol. 30, No. 4, 2000, pp. 295-306. http://dx.doi.org/10.1145/347057.347560

[10] GloMoSim Simulator. http://pcl.cs.ucla.edu/projects/glomosim/ography

[11] S. Bellovin, M. Leech and T. Taylor, "ICMP Traceback Messages," 2001. http://www3.ietf.org/proceedings/01dec/I-D/draft-ietf-itrace-01.txt

[12] R. Stone, "CenterTrack: An IP Overlay Network for Tracking DoS Floods," *Proceedings of the* 2000 *USENIX Security Symposium*, Denver, CO, July 2000.

[13] A. C.Snoeren, C. Partridge, L. A. Sanchez and C. E. Jones, "Hash-Based IP Traceback," *Proceedings of the* 2001 *Conference of Applications*, *Technologies*, *Architectures*, *and Protocols for Computer Communications*, August 2001, pp. 3-14.

[14] V. L. L. Thing and H. C. J. Lee, "IP Traceback for Wireless Ad-Hoc Networks," 60*th IEEE Vehicular Technology Conference*, Los Angeles, September 2004.

[15] Y. Huang and W. Lee, "Hotspot-Based Traceback for Mobile Ad Hoc Networks," *Proceedings of the ACM Workshop on Wireless Security*, 2005.

[16] D. Sy and L. Bao, "CAPTRA: Coordinated Packet Traceback," *Proceedings of the* 5*th International Conference on Information Processing in Sensor Networks*, April 2006, pp. 124-135.

[17] I.-Y. Kim and K.-C. Kim, "A Resource-Efficient IP Traceback Technique for Mobile Ad-hoc Networks Based on Time-tagged Bloom Filter," *International Conference on Convergence and Hybrid Information Technology*, 2008, pp. 549-554.

[18] Y. Kim and A. Helmy, "SWAT: Small World-Based Attacker Traceback in Ad-hoc Networks," *Proceedings of the* 2*nd Annual International Conference on Mobile and Ubiquitous System*: *Networking and Services*, San Diego, July 2005.

[19] B.-C. Cheng, H. Chen and R.-Y. Tseng, "A Packet Marking with Fair Probability Distribution Function for Minimizing the Convergence Time in Wireless Sensor Networks," *Computer Communications*, Vol. 31, No. 18, 2008, pp. 4352-4359. http://dx.doi.org/10.1016/j.comcom.2008.03.024

[20] B.-C. Cheng, H. Chen and G.-T. Liao, "FBT: An Efficient Traceback Scheme in Hierarchical Wireless Sensor Network", *Security and Communication Networks*, Vol. 2, No. 2, 2009, pp.133-144. http://dx.doi.org/10.1002/sec.88

[21] X. Jin, Y. X. Zhang, Y. Pan and Y. Z. Zhou, "ZSBT: A Novel Algorithm for Tracing DOS Attackers in MANETS," *EURASIP Journal on Wireless Communications and Net- working*, Vol. 2006, pp. 1-9.

[22] M.-H. Yang, C.-S. Chiu and S. Shieh, "Tracing Mobile Attackers in Wireless Ad-Hoc Network," ICIW 2008, pp. 7-12.

[23] A. K. Das, S. Agrawal and S. Vishwanath, "Algebraic Traceback for Dynamic Networks," 2009.