# A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking

Shui Yu, *Senior Member, IEEE*, Wanlei Zhou, *Senior Member, IEEE*,
Song Guo, *Senior Member, IEEE*, and Minyi Guo, *Senior Member, IEEE*

**Abstract**—DDoS attack source traceback is an open and challenging problem. Deterministic packet marking (DPM) is a simple and effective traceback mechanism, but the current DPM based traceback schemes are not practical due to their scalability constraint. We noticed a factor that only a limited number of computers and routers are involved in an attack session. Therefore, we only need to mark these involved nodes for traceback purpose, rather than marking every node of the Internet as the existing schemes doing. Based on this finding, we propose a novel marking on demand (MOD) traceback scheme based on the DPM mechanism. In order to traceback to involved attack source, what we need to do is to mark these involved ingress routers using the traditional DPM strategy. Similar to existing schemes, we require participated routers to install a traffic monitor. When a monitor notices a surge of suspicious network flows, it will request a unique mark from a globally shared MOD server, and mark the suspicious flows with the unique marks. At the same time, the MOD server records the information of the marks and their related requesting IP addresses. Once a DDoS attack is confirmed, the victim can obtain the attack sources by requesting the MOD server with the marks extracted from attack packets. Moreover, we use the marking space in a round-robin style, which essentially addresses the scalability problem of the existing DPM based traceback schemes. We establish a mathematical model for the proposed traceback scheme, and thoroughly analyze the system. Theoretical analysis and extensive real-world data experiments demonstrate that the proposed traceback method is feasible and effective.

**Index Terms**—Cybersecurity, IP traceback, packet marking, scalability

## 1 Introduction

DISTRIBUTED D S 5 (DD S) 5 . T 5 5 - 1`, 2`, 3`, 4`, 5 - 5`, 6`, 7`. T 5 5, 5 5 2`, 8` 5 9`. B 5- , 5 5 5 5, 5 5 5 5 5 . A 5 5 10`. D 5 5 5 5 5 2`, 11`, 12`, (5 - 5 ) 5 5 5 . F 5, 5 DD S 5 5. A F 1, 5 DD S 5 *T*, 5 5, *V*. T 5 5 ( ) 5 LAN , 5 *L* (*L* ). F *L* *V*, *attack path*, 5 $R_1, R_2, \ldots$. T 5 DD S 5 5 5 5 ( IP 5 5 5 5) 5 *L* ( *L*). I , IP 5 5 5 . S 5 5 DD S 5 5 5 5 . H , 5 5 5 5 . T 5 5 5 5 5 : P 5 5 (PPM) 13`, 14`, 15`, 16` 5 5 (DPM) 6`, 17`, 18`. T 5 5 5 IP 4 5 5 . C PPM 5 , DPM 5 5 5 , 55 , 5 5 5 . B 5 5 5 - , , 5 5 19`, 20`. H , 5 DPM 5 5 5 , 5 , 5 5 5 5 5. T , 5 5 5 DPM 5 . A 5 16`, I , 5 DPM 5 5 5 . D 5 5 2,048 5 DPM 5 17`. T , 5 262,144 5 5 DPM (FDPM) 5 6`. T 5 5 5 10 5 5 5 ( ) DPM 5 . T 5 . A 21`.

- *S. Yu and W. Zhou are with the School of Information Technology, Deakin University, Victoria 3125, Australia. E-mail: {syu, wanlei}@deakin.edu.au.*
- *S. Guo is with the School of Computer Science and Engineering, The University of Aizu, Aizuwakamatsu, Japan. E-mail: sguo@u-aizu.ac.jp.*
- *M. Guo is with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. E-mail: guo-my@cs.sjtu.edu.cn.*

*Manuscript received 4 July 2014; revised 17 Mar. 2015; accepted 8 May 2015. Date of publication 31 May 2015; date of current version 13 Apr. 2016. Recommended for acceptance by G. Min.*
*For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.*
*Digital Object Identifier no. 10.1109/TC.2015.2439287*

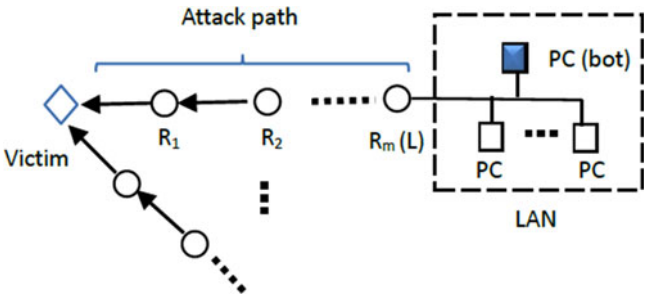



Fig. 1. An attack diagram and terms of distributed denial of service attack.

T 5 5 DPM 5 5 5 R 5 . A 5 DPM 5 R 5 : I DD S 5 . T , R 5ID 5 I . H , 5 IP 4 5 , 5 5 R I ID.

F DD S 5 , 5 5 5 5 DD S 5 : 1) I 5 , 5 DD S 5 R 2`, 11`, 12`, 5 , 22`. T 5 , , 5 R - . 2) I , DD S 5 , 5 5 23`. B 5 , R 5 R 5 R . I , 5 R 5 R 5 5 DPM 5 .

A , DD S 5 55 R 5 5 . D 5 , 5 5 DD S 5 5 5 5 5 . T R 5 5 5 , 5 R LAN . E 5 , - R R , 5 R , 5 , IP R 1`, 24`, 5 5 , 5 25`, - - 5 R 24`, 26`, 27`. T , 5 DD S 5 5 5 , 5 R - 5 DD S 5 .

I , R (MOD) 5 DPM 5 5 R R ID DD S 5 - 5 5 . I , R (MOD ). A 5 R 5 I , DD S 5 5 . W 5 , 5 ID MOD , R ID 5 . A , MOD IP R MOD , 5 . O 5 DD S 5 5 , 5 5 5 5 . W 5 5 MOD IP 5 5 R . W 5 - 5 5 5 , 5 MOD 5 5 . C R DPM 5 5 , - R , 5 R 5 , R 5 5 5 , R 5 R . O 5 5- 5 . M , 5 5 5 5 , 5 , - R, .

W 5 5 55 5 . I , 5 5 5 5 5 5 . T 5 :

- W 5 5 R 5 DD S 5 5 5 5 . C - R 5 5 , MOD 5 R . F , 5 - 5 DPM 5 , 5 5 5 5 5 . S 5 , 5 5 5 R 5 . T , - DD S 5 R R , R 5 .
- W 5 5 - 5 5 .
- T 5 5 5 5 , 5 5 R 5 .

T R . W S 5 2. I S 5 3, - MOD 5 5 - 5 R . S 5 5 5 5 5 S 5 4, - 5 MOD 5 S 5 5. F 5 MOD 5 S 5 6. F , 5 S 5 7.

## 2 Related Work

T R DD S 5 5 5 R R , 5 R R R 5 , 5 5 R R . E DD S 5 R 2000, - , 5 CNN, A , R 5 5 . T 5 5 5- . H , 5 5 5 5 R 5 - 5 5 5 1`.

C , DD S B .
H I , . A , ( ) , - , DD S 1`, 28`. A DD S , , . A DD S 10`.
T , , : PPM DPM. I IP 4 , , 16, 17, 19 24 6`. N ID . B , , - , 7`. A , .
T PPM 13`, , 16`. T PPM - , , , . A - , , , . I , 55 , , PPM , , . D PPM , DPM ( , LAN ). T B A 17`. T PPM , IP 17 (16 IP 1 ). A , . S55 DPM . J 29` ID IP . F IP , 0-13 , 9-22 , 18-31 , . T . T IP . F , . 6` DPM , FDPM . T , , 16, 19 24 . M , - - 55 . T FDPM . F , FDPM-19 FDPM-24 , 8,192 262,144 - , . W DPM 2,048 . A . W . 19` IP - . O , , , . J . 20` - . M . 30` - DD S I - , $\frac{1}{256}$ IP 4 . T DD S . B 22 , - 24.5/ . I I , 6,272 $(24.5 \times 256)$ . A , : 60 - 10 , 80 30 . A , (10.8 ) 10 (9.7 ). W . I DD S , . H , . S - T 182,800, T 49,272 48,532, 28`. O C 2,201,183. A , - , ( , , - ), . R . 22` . W .

## 3 The Proposed Traceback Method

I , , M D DPM .

### 3.1 The Marking On Demand Traceback Scheme

A , , , , .

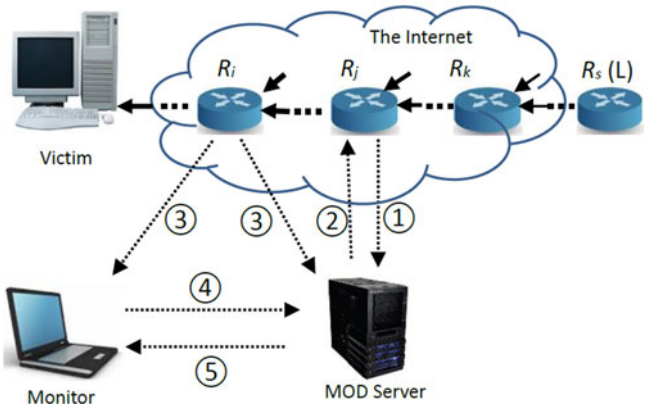



Fig. 2. The framework of the marking on demand scheme for DDoS attack traceback.

A 5 5 5 DD S 5 5 , 5 . O 5 , 5 5 5 5 , 5 5 5 5 .

F 5 , R , 5 *network flow* *flow*. W 5 DD S 5 *attack flow*.

B , 5 , 5 5 . D R R 5 5 , R 5 5 5 5 .

T R R F R 2. T 5 5 5 , $R_s$, $R_k$,$R_j$,$R_i$, 5 . I 5 5 5 5 . W $R_k$,$R_j$,$R_i$ 5 , DD S 5 5 , 5 5 R 5 5 5 5 . T 5 $R_s$ 5 5 5 5 . T R 5 5 5 5 $R_s$ 5 , , 5 5 $R_s$.

I , R MOD , 5 R R . M , MOD - , 5 - .

D 5 , $R_k$ 5 5 . W R R - R 5 ( 5 ), $R_j$ 5 R , 5 5 5 , , $R_j$ - 5 , 5 R 5 . W 5 R R 5 , , $R_i$ 5 5 ( 5 , 5 5 5 ).

O 5 5 5 , 5 R , R, $R_i$, MOD 5 5 ( 5 $R_s$ $R_j$). T MOD 5 R 5 R . T 5 5 5 5 5 5 .

A 5 5 .

1) W 5 R , 5 ( R, $R_j$ F R. 2) 5 5 R 5 5 5 . I , R . I , - MOD ( 1 R ).

2) T MOD , ( , 5 IP , ) ( 2 R ).

3) T 5 ( R, $R_j$ F R. 2) R 5 R R .

4) A R 5 R 5 , 5 ( R, $R_i$ F R. 2) 5 . T 5 $R_i$ MOD 5 . T MOD - . M , 5 - 5 5 . ( 3 R ).

5) W 5 5 , IP 5 ( 4 R ).

6) T MOD 5 5 , IP . I , 5 5 5 5 5 ( 5 R ).

I R 5 5 5 , R R DD S 5 5 R 5 , 5 5 5 5 5 R .

### 3.2 Comparison on the Marking Schemes

I 5 , 5 R 5 R . W DPM 5 , R DPM 5 18`, - 5 5 FDPM 5 6`.

T R R IP 4 5 DPM 5 . I R , IP 4 5 : F R ID (16 ), R F R (1 ), - 5 (TOS , 8 ). T R DPM 5 17 R (F R ID R F R), FDPM 5 24 (F R ID TOS) R , 16 (F R ID) R . W 17`, 18`, 6` 5 5 R.

F 5 , R R 24 16 MOD 5 5 . I R , $l$ R 5 .

A F 3, l, DPM FDPM : $d'$ ($d$ ID) ID , $a'$ ($a$ ) IP , $s'$ ($s$ ) IP . I

$$l = a' + d' + s'. \quad (1)$$

T (1)

$$\begin{cases} a' \geq 1 \\ d' \geq 1 \\ s' \geq 2 \\ 2^{s'} \geq a'. \end{cases} \quad (2)$$

T $N_{tr}$ $d'$ :

$$\max\{N_{tr}\} = 2^{d'} = 2^{l-a'-s'}. \quad (3)$$

F DPM , $l = 17$, $\max N_{tr} = 2,048$ $d' = 11, a' = 1,$ $s' = 5$ (2). I . A , 32 -

I MOD , , , F 3,

$$l = d. \quad (4)$$

T MOD $d$,

$$\max\{N_{tr}\} = 2^l = 2^d. \quad (5)$$

C (1), (4) (2), MOD $2^{a'+s'}$ .

A , MOD , DPM FDPM - T 1.

## 4 System Analysis on the MOD Scheme

I , , DD S . W .

### 4.1 Traceable Sources

T - $2^l$ . H , MOD , - . I , , - , - I .

F $t$,

TABLE 2
Statistics for Conficker Distribution in Terms of Domain Names at the Three Top Level Domains

| N | L | S |
|---|---|---|
| 462 | 2,201,183 | 1 |
| 1 20,104 | 1,718,306 | 1 |
| 2 96,756 | 1,714,283 | 1 |

. W

: , 1, 2, . S

T 2.

I , 34˜, 35˜. S

$n$ , -

. L $x$ ,

.

$$Pr\{x = i\} = C \cdot i^{-\alpha}, \tag{6}$$

$\alpha$ , $C$ . F

,

$$\sum_{j=1}^{n} C \cdot j^{-\alpha} = 1. \tag{7}$$

I , $\alpha$ $n$ .

B ,

$C$,

T 3.

A , $B(t)$

, $B_i(t)(1 \le i \le |K(t)|)$ .

C ,

. M ,

TABLE 3
The Approximation of $\alpha$ and $C$ in Three Top Level Domains

| T | L 1 | L 2 |
|---|---|---|
| $\alpha$ | 1.140 | 1.112 | 1.091 |
| $n$ | 462 | 20104 | 96756 |
| $C$ | 0.2164 | 0.1567 | 0.1320 |

T 3.

F F . E , F .

F , $M(t)$ , $|K(t)|$ - $K(t)$ $t$. F ,

$$Pr\{X = |K(t)|\} = C \cdot |K(t)|^{-\alpha} = \frac{M(t)}{B(t)}. \tag{8}$$

F (8),

$$|K(t)| = e^{-\frac{1}{\alpha}\ln\frac{M(t)}{CB(t)}}. \tag{9}$$

F T 2, $M(t) = 1$, (9)

$$|K(t)| = e^{\frac{1}{\alpha}\ln CB(t)}. \tag{10}$$

I , $|K(t)|$, $\alpha$ $M(t)$ , W -

:

$$B(t) = \frac{M(t)}{|K(t)|^{\alpha}} \cdot \sum_{i=1}^{|K(t)|} \frac{1}{i^{\alpha}}. \tag{11}$$

W I . F $t$, $A(t)$

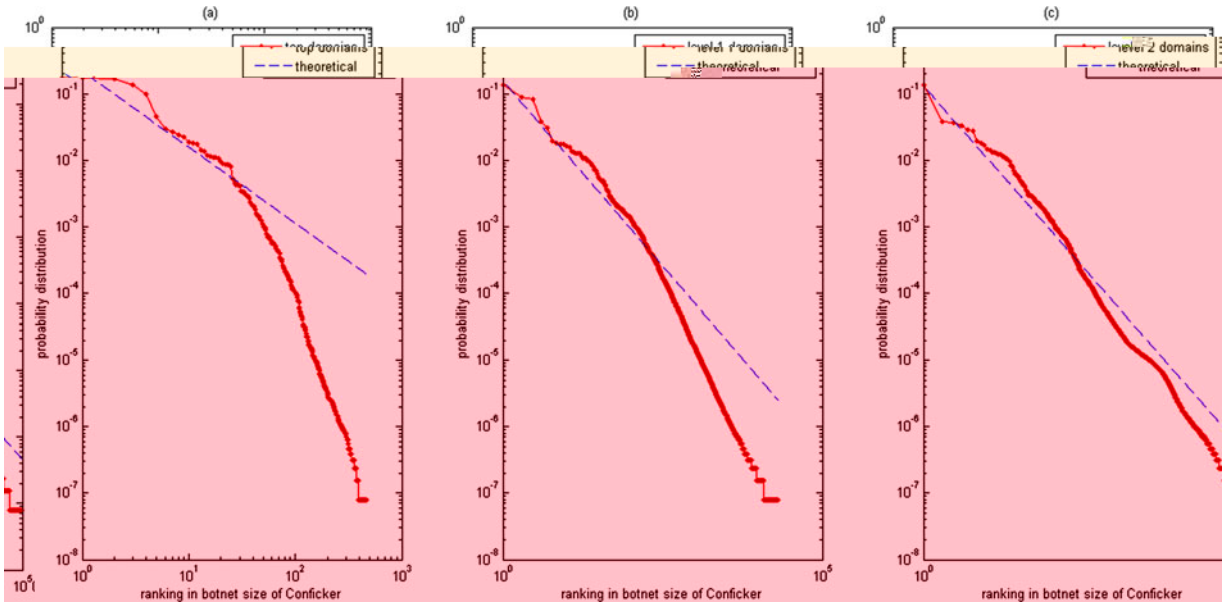



Fig. 4. Power law distribution of Conficker botnet in the top three levels of domain names with theoretical comparison.

[illegible] I , $D(t)$ [illegible] . T [illegible] $t$

$$N_{tr}(t) = A(t) \times K(t). \quad (12)$$

T [illegible]

$$T_I(t) = \frac{2^l}{A(t) \cdot K(t)} \cdot D(t) \quad (13)$$

B W T ,

$$E[T_I(t)] = \frac{2^l}{E[A(t)] \cdot E[K(t)]} \cdot E[D(t)], \quad (14)$$

$E[\cdot]$ [illegible] . A , - [illegible] $T_I(t)$. I , $J$ [illegible] $T_I(t)$,

$$D_j(t) < T_I(t), \forall j \in \{1, 2, \ldots, J\}. \quad (15)$$

I [illegible] (15) , ( , , ) [illegible] .

### 4.2 Storage Analysis

F DPM , [illegible] . A , DPM . W MOD . T , . S $n$ $(n = 1, 2, \ldots)$ . I - , [illegible] .

$$n\left(\frac{1}{n} + \frac{1}{n-1} + \cdots + \frac{1}{2} + 1\right). \quad (16)$$

I , $n = 2^{s'}$, ( $N_s$) DPM

$$N_s = 2^{s'}\left(\frac{1}{2^{s'}} + \frac{1}{2^{s'} - 1} + \cdots + \frac{1}{2} + 1\right). \quad (17)$$

F MOD , , $N_s = 1$. H , DPM .

TABLE 4
Quantity Comparison Among the Proposed MOD Scheme with the DPM Scheme and the FDPM Scheme

| S | M | M | S |
|---|---|---|---|
| DPM-17 | $2^{11}$ | 32 | 129.87 |
| FDPM-16 | $2^{10}$ | 32 | 129.87 |
| FDPM-24 | $2^{18}$ | 32 | 129.87 |
| MOD-16 | *unlimited* | 1 | 1 |
| MOD-17 | *unlimited* | 1 | 1 |
| MOD-24 | *unlimited* | 1 | 1 |

## 5 Performance Evaluation

I , MOD , DPM FDPM .

F , MOD , DPM FDPM .

B , DPM . A . T 4.

F T 4, - , MOD , DPM FDPM . I DPM FDPM , 32 , MOD , . I , $\frac{1}{129.87}$ DPM FDPM .

W . I , I , F 2. M , DD S .

W DD S 22˙, 23˙, T 5.

F , DD S 5 , , , $T_I$ .

I , ( ) - . F T 2, . M , T 5,

TABLE 5
Key Statistics on DDoS Attack Characteristics

| F | A | 23` | A | 23` | A | 23` | B | 22` |
|---|---|---|---|---|---|---|---|---|
| V | 105/ | | 5 | | 500 | / | 1000 - 2000 | |

. C $\alpha$ C ( T 2), F 5. F F 5, - . I , ( ), 200 . I , 200 ( ) DD S . F , $T_I$ ( (14)) DD S T 5, . I , , 16, 17, 24 , . W F . 6 , 6 , 65, . F , , F 6 ($l = 16$), 1,500 , $T_I \approx 20$ , , 5 . E 3,000 , $T_I > 10$ . W - 5 . S , F 6 ($l = 17$), F 65 ($l = 24$), $T_I \approx 40$ , 5,000 ( ), . C , - , 55 $l = 16$ . B DD S , , .

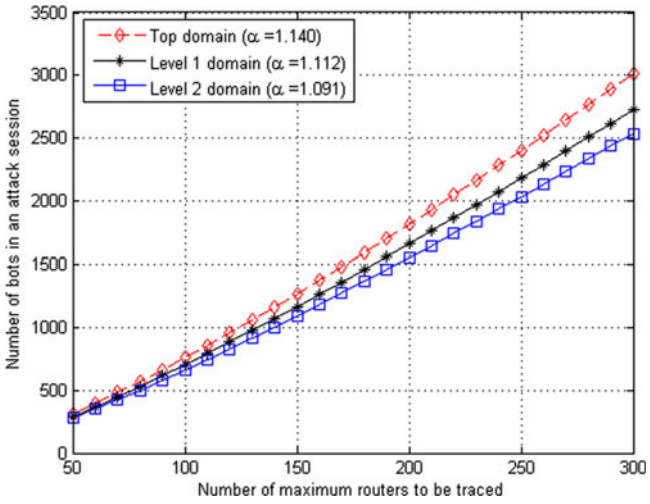
T , 


Fig. 5. The relationship between the number of total bots in an attack session and the number of routers to be traced.

## 6 Further Discussion

I , - DPM , MOD . H , . W .

- I MOD , MOD . H - MOD , , DD S . H . P , MOD , DD S - , DD S MOD , DD S . I 4`.
- D MOD , - MOD .
- A , - . H , . F , 6`, 29`. O ,
- W - - MOD .

## 7 Summary and Future Work

I , DD S , , . I , - DPM . A , , I , . O . I , MOD . S , ( )

R 5 R. T , R R MOD , 5 R MOD 5 . F , - 5 5 - 5 5 5 .

## ACKNOWLEDGMENTS

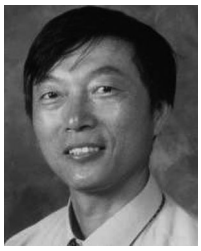
T E C, E , - R 5 . T D . N N S5 5 F C G N 61379041.T D . M G N N S5 5 F C G N 61272099 61261160502. M. G 5 R .

## REFERENCES

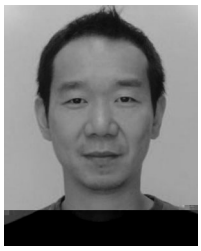
1` T. P R, C. L 5 , K. R , S - 5 5 R D S DD S - , *ACM Comput. Surv.*, . 39, . 1, . 3, 2007.
2` S. , W. , W. J , S. G , . R, F. T R, D 5 R DD S 5 5 R 5 - 5 5 , *IEEE Trans. Parallel Distrib. Syst.*, . 23, . 6, . 794 805, J . 2012.
3` R. C , J.-M. P , R. M 5 , A - -5 R R - - 5 5 , *IEEE Trans. Parallel Distrib. Syst.*, . 18, . 5, . 577 588, M 2007.
4` S. , . T , S. G , D. W , C DD S 5 5 ? *IEEE Trans. Parallel Distrib. Syst.*, . 25, . 9, . 2245 2254, S . 2014.
5` B. A -D G. M , N 5 R 5 R RR R IP 5 5 , *IEEE Trans. Parallel Distrib. Syst.*, . 17, . 5, . 403 418, M 2006.
6` . R, W. , M. G , F 5 5 R: A IP 5 5 5 , *IEEE Trans. Parallel Distrib. Syst.*, . 20, . 4, . 567 580, A . 2009.
7` S. , W. , R. D , W. J , T 5 5 DD S 5 R , *IEEE Trans. Parallel Distrib. Syst.*, . 22, . 3, . 412 425, M . 2011.
8` S. , S. G , I. S 5, F 5 : M 5 R 5 - 5 5 5 , *IEEE Trans. Comput.*, . 64, . 1, . 139 151, J . 2015.
9` S. , R. D , W. , I 5 R 5 R DD S 5 , *IEEE Commun. Lett.*, . 12, . 4, . 319 321, A . 2008.
10` S. , *Distributed Denial of Service Attack and Defence*. N , N , USA: S R , 2014.
11` V. L. L. T R, M. S , N. D , A 5 5 , *Proc. IFIP Int. Inf. Security Privacy Conf.*, 2007, . 229 240.
12` S. , S. G , I. S 5, C R 5 5 R 5 ? *Proc. INFOCOM*, 2012, . 2851 2855.
13` S. S R, D. W , A. R. K , T. E. A , P 5 5 IP 5 5 , *Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun.*, 2000, . 295 306.
14` T. K. T. L , J. C. S. L , D. K. . , 5 , 5 ' : A 5 5 R 5 5 DD S 5 , *IEEE Trans. Parallel Distrib. Syst.*, . 16, . 9, . 799 813, S . 2005.
15` A. , A. P R, D. . S R, F : 5 5 , *Proc. INFOCOM*, 2005, . 1395 1406.
16` M. T. G 5 , P 5 5 R R - 5 IP 5 5 , *IEEE/ACM Trans. Netw.*, . 16, . 1, . 15 24, F . 2008.
17` A. B N. A , IP 5 5 5 5 R, *IEEE Commun. Lett.*, . 7, . 4, . 162 164, A . 2003.
18` A. B N. A , O 5 5 R, *Comput. Netw.*, . 51, . 10, . 2677 2700, 2007.
19` . W R, S. C , S. J , N R 5 - 5 5 5 , *Proc. IEEE Symp. Security Privacy*, O , CA, USA, 2007, . 116 130.
20` W. J , F. P. T , . L R, . F , D. , W. , B 5- 5 , *Proc. INFOCOM*, 2009, . 2195 2203.
21` S. , W. , S. G , M. G , A 5 5 5 R 5 DD S 5 5 , *Proc. IEEE Int.*

25] A. H N. I , B
, *Int. J. Forensic Comput. Sci.*, . 2, . 1, . 19 39, 2007.
26] P. W S. S , C. C. , A - -
, *IEEE Trans. Dependable Secure Comput.*, . 7, . 2, . 113 127, A . J . 2010.
27] M. B , E. C , F. J , . , M. K , A
, *Proc. Cybersecurity Appl. Technol. Conf. Homeland Security*, 2009, . 299 304.
28] B. S -G , M. C , L. C , B. G , M. S ,
R. K , C. K , G. V ,
: A , *Proc. 2009 ACM Conf. Comput. Commun. Security*, 2009, . 635 647.
29] G. J J. , D - IP , *IEEE Commun. Lett.*, . 10, . 3, . 204 206, M . 2006.
30] D. M , C. S , D. J. B , G. M. V , S. S ,
I - - , *ACM Trans. Comput. Syst.*, . 24, . 2, . 115 139, 2006.
31] . C C. J , A - -
, *IEEE Trans. Inf. Forensics Security*, . 4, . 3, . 530 541, S . 2009.
32] S. , G. G , A. B , S. G , I. S , M
- , *IEEE Trans. Knowl. Data Eng.*, . 27, . 1, . 170 179, J . 2015.
33] S. S , G. G , A. L. N. R , C. P. L , A - ,
, *IEEE Trans. Inf. Forensics Security*, . 7, . 2, . 676 690, A . 2012.
34] M. M , A
, *Internet Math.*, . 1, . 226 251, 2004.
35] M. E. J. N , P , P ,
, *Contemporary Phys.*, . 46, . 323 351, 2005.

**Shui Yu** (M'05-SM'12) is currently a senior lecturer in the School of Information Technology, Deakin University. His research interest includes networking theory, cyber security, mathematical modelling, and big data. He has published two monographs and edited one book, more than 150 technical papers, including top journals and top conferences, such as *IEEE TPDS*, *IEEE TC*, *IEEE TIFS*, *IEEE TMC*, *IEEE TKDE*, *IEEE TETC*, and IEEE INFOCOM. He initiated the research field of networking for big data in 2014. His h-index is 18. He actively serves his research communities in various roles. He is currently serving the editorial boards of *IEEE Transactions on Parallel and Distributed Systems*, *IEEE Communications Surveys and Tutorials*, *IEEE Access*, and a number of other international journals. He has served more than 50 international conferences as a member of organizing committee, such as publication chair for IEEE Globecom 2015 and IEEE INFOCOM 2016, TPC co-chair for IEEE BigDataService 2015, IEEE ATNAC 2014 and 2015. He is a member of Deakin University Academic Board (2015-2016), a senior member of the IEEE, and a member of AAAS, the vice chair of Technical Subcommittee on Big Data Processing, Analytics, and Networking of IEEE Communication Society.



**Wanlei Zhou** (SM'09) received the PhD degree from The Australian National University, Canberra, Australia, in October 1991. He also received the DSc degree from Deakin University, Victoria, Australia in 2002. He is currently the chair professor and head of the School of Information Technology, Deakin University, Melbourne, Australia. His research interests include distributed and parallel systems, network security, mobile computing, bioinformatics and e-learning. He is a senior member of the IEEE.



**Song Guo** (M'02-SM'11) received the PhD degree in computer science from the University of Ottawa, Canada in 2005. He is currently a senior associate professor at the School of Computer Science and Engineering, University of Aizu, Japan. His research interests are mainly in the areas of protocol design and performance analysis for reliable, energy-efficient, and cost effective communications in wireless networks. He is an associate editor of the *IEEE Transactions on Parallel and Distributed Systems* and an editor of *Wireless Communications and Mobile Computing*. He is a senior member of the IEEE and the ACM.

**Minyi Guo** received the PhD degree in computer science from the University of Tsukuba, Japan. He is currently a chair professor and a head of the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. He received the national science fund for distinguished young scholars from NSFC in 2007. His research interests include parallel and distributed computing, compiler optimizations, embedded systems, pervasive computing, and bioinformatics. He has more than 300 publications in major journals and international conferences in these areas. He is on the editorial board of the journals *IEEE Transactions on Parallel and Distributed Systems* and *IEEE Transactions on Computers*. He is a senior member of the IEEE, a member of the ACM, IEICE IPSJ, and CCF.