IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON FUTURE NETWORKS: ARCHITECTURES, PROTOCOLS, AND APPLICATIONS

Received February 4, 2017, accepted March 9, 2017, date of publication March 13, 2017, date of current version January 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2681684

Research and Simulation of Queue Management Algorithms in Ad Hoc Networks Under DDoS Attack

WEI WEI[1,2], (Senior Member, IEEE), HOUBING SONG[3], (Senior Member, IEEE), HUIHUI WANG[4], (Member, IEEE), AND XIUMEI FAN[5]

[1]School of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710048, China
[2]Key Laboratory for Computer Vision and Pattern Recognition, Xiamen 361021, China
[3]Department of Electrical and Computer Engineering, Institute of Technology, West Virginia University, Morgantown, WV 25136, USA
[4]Department of Engineering, Jacksonville University, Jacksonville, FL 32211, USA
[5]School of automation and information engineering, Xi'an University of Technology, Xi'an 710048, China

Corresponding author: W. Wei (weiwei@xaut.edu.cn)

This work was supported in part by the Scientific Research Program through the Shaanxi Provincial Education Department under Program 2013JK1139, in part by the China Postdoctoral Science Foundation under Grant 2013M542370, in part by the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 20136118120010, in part by NSFC Grant under Program 11226173, Program 11301414, and Program 61272283, and in part by the Open Program of Xiamen Key Laboratory of Computer Vision and Pattern Recognition, Huaqiao University, under Grant 600005-Z17X0001.

ABSTRACT Concentrating on the influence of DDoS applied to ad hoc networks, we introduced three classic queue management algorithms: Drop-Tail, random early detection (RED), and random exponential marking (REM). We analyzed and compared the defensive abilities of these algorithms applied to ad hoc networks with NS2 under DDoS attack. The results showed that active queue management algorithms, such as REM and RED, exhibited stronger defensive abilities than the passive queue management algorithm Drop-Tail under medium- and small-scale DDoS attacks; however, under large-scale DDoS attack, all three algorithms exhibited insufficient defensive capabilities. This means that other defense schemes, such as network detection, must be integrated into security schemes to defeat DDoS attacks.

INDEX TERMS DDoS, ad-hoc network, queue management algorithms, network simulation software, defense scheme.

I. INTRODUCTION

In recent years, DDoS (distributed denial of service) attacks have become prevalent, and they are difficult to detect in networks. Because of their intimate, simple and effective characteristics, DDoS attacks are recognized as one of the main threats faced by network services [1], [2]. A queue management algorithm is important to guarantee the fair distribution of resources and quality of service (QoS) in the event of network congestion, and such an algorithm is also the first line of defense for a network when facing a DDoS attack. Consequently, the design of such algorithms is directly related to the network's ability to provide normal bandwidth allocation, latency, packet rate and other basic services [3]. This paper analyzes three common queue management algorithms, Drop-Tail, RED, and REM, and then, in an ad hoc network environment, we conduct simulations using the network simulation software NS2 to compare the defense capabilities of these algorithms under DDoS attacks.

A. Ad-hoc NETWORKS AND DDoS ATTACKS

According to the hierarchical structure of ad hoc networks(see also Figure 1), DDoS attacks can be divided into four types: 1) attacks aimed at the physical layer, 2) MAC-layer attacks, 3) network-layer or transport-layer attacks (i.e., attacks on the upper layer of the network structure), and 4) application-layer DDoS attacks.

DDoS attacks on the physical layer can be divided into attacks on the wireless electromagnetic spectrum and wireless mobile devices with wireless signals as the transmission media. This class of DDoS attacks uses the same spectral information to disturb normal transmissions in the network. Ad hoc networks can use different transmission technologies, and there are different corresponding types of DDoS attacks. Generally, according to the different transmission technologies, all ad hoc networks currently belong to the following categories:

1) Infrared (IR) ad hoc networks: because the infrared rays cannot penetrate opaque walls, an IR MANET will be

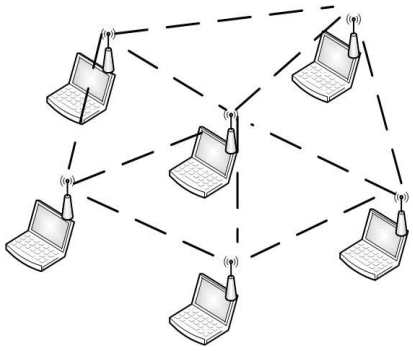

FIGURE 1. Ad hoc network configuration diagram.

confined to a single room. This has two advantages: first, relative to other transmission technologies, infrared communication is easier to defend from outside intrusion of illegal users, thus helping to ensure safety. In addition, independent IR ad hoc networks can be established in each room of a building without mutual interference, even when they use the same spectrum. However, infrared media in indoor environments also have shortcomings, such as background infrared radiation from the sun and indoor lighting appearing in infrared receivers as noise. Such noise can produce a DDoS attack.

2) Spread spectrum ad hoc networks: this type of ad hoc network uses spread spectrum transmission technology, which uses a wider bandwidth signal to increase the difficulty of interference and eavesdropping. Due to the spread spectrum technology transmissions, this type of ad hoc network can resist outside radio electromagnetic spectrum attacks [5].

3) Narrowband microwave ad hoc networks: these ad hoc networks operate at microwave frequencies but do not use spread spectrum technology. Thus far, however, there are no details about the transmission technology used by these products.

In addition to attacking the physical layer of the wireless electromagnetic spectrum, some mobile equipment defects can also be attacked. Compared with wired network equipment, the power supply of wireless mobile devices is limited. The attacker, by consuming the electric energy of a particular device by some means, can achieve a denial of service. In addition, the bandwidth of wireless networks is limited; consequently, consuming the limited bandwidth makes such attacks simpler.

B. MAC-LAYER DDoS ATTACKS

A DDoS attack aimed at the MAC layer is mainly reflected by the media access control technology of the attack. These types of attacks mainly cause network congestion by creating useless data packets, thus achieving their purpose of media access rejection. This technique is fundamentally intended to prevent one or more nodes from obtaining or providing services. The most critical parameter in all media access control technology is the manner of control. Different MAC layer protocols with different control techniques lead to different attack methods. The following is a summary of possible MAC-layer attacks: (1) by keeping all node channels within a region busy, the node suffers from a DDoS attack. (2) If a node continues to respond to false information, node energy will soon be depleted, at which point the node cannot access or provide other services. In certain circumstances, end-to-end authentication can prevent attacks on the MAC layer. When a node does not hold the certificate, it cannot obtain channel access. However, even when the sending and receiving sides are authenticated, the possibility of such an attack still exists. The FAIRMAC protocol, introduced in [6], improves the fairness of access to media. Experiments have shown that MAC-layer DDoS attacks are effective mainly because of the unfairness of the capture effect and the resulting media access. The FAIRMAC protocol can reduce DDoS attack effectiveness to a certain extent but cannot fundamentally prevent DDoS attacks.

C. DDoS ATTACKS AT THE NETWORK LAYER

Because of the existence of certain limits, any wireless electromagnetic wave transmitter exhibits distance attenuation. To conserve energy, the power requirements of each node/transmitter in an ad hoc network are very low; thus, the effective distance of signals is very limited. Ad hoc communication between two nodes can utilize an efficient routing path through a multi-hop routing protocol, and then, cooperation and information through other nodes can occur along the routing path to the destination node. However, compared to the traditional routing protocol in wired networks, ad hoc routing protocols must be able to adapt faster. This is because the changes due to mobile nodes or wireless environment conditions lead to rapid changes in network topology. Thus, the routing protocol is particularly important for long-distance information transmission in ad hoc networks. The premise for the design of routing protocols for ad hoc networks is that all the nodes in the network are assumed to be honest and reliable and to be capable of mutual cooperation to jointly complete transmission through the network's nodes. This design premise is often used by attackers, leading to different forms of DDoS attack. The following summarizes network-layer DDoS attacks. (1) Illegal nodes become routing nodes. They lose a number of packets; consequently, the connection quality decreases. If the transport layer uses the TCP protocol, this will have a greater impact. Examples include black hole attacks (all information will secretly be discarded) and gray hole attacks (information such as forwarding routing protocol packets and packets will be selectively discarded). (2) The illegal nodes will transmit false routing information or replay outdated routing information. This will cause routing failures, negatively impacting the transmission performance. Wormhole attacks and loop attacks are typical representatives of this type of attack. The principle of the wormhole attack is to establish a normal link via wired or wireless means over a long distance in the MANET. By establishing the link, the routing protocol is deceived, resulting in false

routing information. Wei and Yong [14], uses geometric random graph theory and lists the necessary and sufficient conditions for wormhole attack detection and defense. In this theory, the author developed a defense mechanism based on a local broadcast key. As demonstrated by experiments, this defense mechanism can resist wormhole attacks well. (3) By hiding the attacker using IP spoofing of a real position and node mobility, an attack source can quickly change, which makes tracing the attack source extremely difficult. To study DDoS attacks in ad hoc networks, an attack source traceback in a wired network can learn from DDoS attack source tracking technology to a certain extent. However, there are still differences between the two. In [7], the wired network attack source traceback technologies PPM (sample labeling method) and ITrace (ICMP packet positioning method) are transplanted into an ad hoc network. At the same time, as shown through experiments, the use of the techniques of attack source traceback and attack source tracing through the Ad protocol and the Hoc network scale has a certain contact. Guo *et al.* [8] and Athuraliya *et al.* [9], introduced a new concept: small regions (Small World). In this concept, the entire ad hoc network is divided into many small regions according to physical or logical relationships, and then, attack source traceback through the TPM (matching flow patterns) and TVM (matching the size of the flow) is performed. This type of attack source traceback technology does not perform tracking based on IP information; instead, it uses traffic characteristics to analyze selective traces. Thus, the attack source tracing technology can not only solve IP spoofing, attacks on the source node's mobility and other issues but also reduce the flow of tracking information.

D. DDOS ATTACKS ON THE NETWORK TRANSPORT LAYER AND APPLICATION LAYER

The application layer and transport layer—the upper structure and the equivalent wired network at the ad hoc level—have the same characteristics; therefore, for the upper network, DDoS attacks in ad hoc networks and DDoS attacks in wired networks are basically the same. The TCPSYN flooding and TCP RST flooding attacks are typical of upper network attacks. In addition, defense methods against DDoS attacks in wired networks can be applied to ad hoc networks. DDoS attack, especially the address spoofing attack tends to produce massive attacking data stream which will consume a huge amount of network space and thus make the network performance appear sharp decrease [2]. Take Ad Hoc network as an example, since each node is connected through a distributed wireless network, the rival is likely to replace or take control of a number of nodes in the network (like nodes 1 and 2 in Figure 2) and endowed them with a lot of resources.

E. THE CONTRIBUTION AND APPLICATION OF QUEUE MANAGEMENT

Different from the passive queue management algorithm, the contribution of active queue management algorithm is to discard the packet before the queue is full, therefore we can

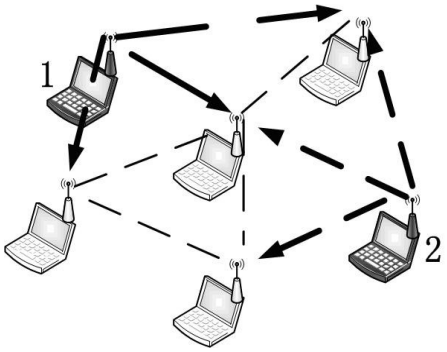

FIGURE 2. Ad hoc network under DDoS attack.

regulate the discharge velocity of the original transmission end which could control congestion in order to avoid the negative effects like the long time end-to-end delay caused by the state of full queues or the reduction of utilization ratio and so on. Common active queue management algorithms include random early detection algorithm (RED) [6], [7] and random exponential marking algorithm (REM) [9].

II. QUEUE MANAGEMENT ALGORITHMS

The composition of a network is mainly based on the technology of store-and-forward and statistical multiplexing because data are inherently unexpected; thus, it is necessary to allow the transmission of unexpected data packets. The important role of the queue in a router is to absorb unexpected packets; a larger cohort can absorb more unexpected data and thus improve the throughput, but it also increases the data packet delay. Thus, we must manage the queue through the router to maintain a smaller queue length; therefore, a number of queue management algorithms have been generated [6].

The current queue management algorithms can be divided into two categories: passive queue management (PQM) algorithms and active queue management (AQM) algorithms.

A. SIGNIFICANCE OF QUEUE MANAGEMENT ALGORITHMS

In contrast to passive queue management algorithms, active queue management algorithms discard packets before the queue is full to regulate the discharge velocity of the original transmission source. This approach helps control congestion to avoid other negative effects such as long end-to-end delays caused by full queues and a reduction of the utilization ratio. Common active queue management algorithms include the random early detection algorithm (RED) and the random exponential marking algorithm (REM).

B. PASSIVE QUEUE MANAGEMENT ALGORITHMS

Passive queue management algorithms, the traditional way to manage queue length, set a maximum length for each queue (in packets) and then accept packets into the queue until the queue length limit is reached. Thus, any subsequent packet that arrives will be rejected by the queue until the queue

length has decrease. This technique includes the traditional ''Drop-Tail'' algorithm. Because packets must be dropped when the queue is full, this algorithm is called passive queue management [6]–[16]. Drop-Tail queue management mechanisms are still the most widely used method for queuing and discarding network packets.

1) RED QUEUE MANAGEMENT ALGORITHM

The RED [6], [7] queue management algorithm uses the average queue length to predict impending network congestion and drops packets using random selection so that the transmission side, which has the function of congestion control, can be influenced to regulate the discharge velocity before congestion occurs, thus avoiding congestion.

RED uses the weighted average method to calculate the average queue length; the calculation formula is as follows:

$$avg = (1 - w_q) \cdot avg + w_q \cdot q, \tag{1}$$

where avg refers to the average queue length, q refers to the current actual queue length, and w_q refers to the current actual weighted coefficient of the queue, whose value must meet the condition $0 < w_q < 1$. Generally, the value of w_q is set to be very small so that the calculation of the average queue length changes very slowly, thus avoiding the problem of dropping of a large number of data packets just because of the arrival of unexpected discharges, which might lead to a rapid increase in the average queue length. When the average queue length is between the shortest queue length $\min_{th}$ and the longest queue length $\max_{th}$, packets are dropped in accordance with the probability formula below:

$$P_b = \max_p \cdot \frac{avg - \min_{th}}{\max_{th} - \min_{th}}. \tag{2}$$

C. REM QUEUE MANAGEMENT ALGORITHM

The random exponential marking (REM) algorithm management mechanism stems from ''optimal flow control'' theory [8]–[19]. The REM algorithm uses the concept of ''price'' from the network traffic optimization theory proposed by F. Kelly to detect and control the network's congestion state. The change of ''price'' is determined by two factors: one is the difference between the actual queue length and the expected queue length, and the other is the difference between the input rate of aggregated flow and the output rate of the port. For the deepening algorithm of ''price,'' REM uses a simple proportional relationship. The sum of the probability of a single node and the ''price'' on the link shows an approximate proportional relationship. REM stabilizes the input rate to remain close to the link capacity and maintains the queue length within a small target range, regardless of the number of connections sharing the link, because the REM algorithm is based on the solution of gradient optimization. There are two core features for the load-based REM algorithm [9]–[28]:

1) Compare the rate and empty the buffer. Calculate the packet arrival rate and approximate the rate difference with the queue difference. The price of the link is calculated as follows:

$$p_l(t+1) = [p_l(t) + \gamma(q_l(t+1) - (1-\alpha_l)q_l(t) - (1-\acute{a}1)ql(t)\acute{a}1 \cdot q] \tag{3}$$

where $\gamma > 0$, $\alpha_l > 0$, $[z]^+ = \max\{0, z\}$, $q_l(t)$ refers to the instantaneous queue length of link l at time t, and q^* refers to the target queue length.

2) Calculate the ''sum.'' The marking rate of link l at time t is:

$$m_l(t) = 1 - \phi_{-p_l(t)}, \tag{4}$$

where ϕ is a constant and $\phi > 1$. The end packet marking probability is:

$$1 - \phi_{-\sum \phi_l(t)}. \tag{5}$$

As seen from the above analysis, compared to the queue-based algorithm, the REM algorithm mainly measures the link load conditions and, thus, calculates the packet loss rate [10].

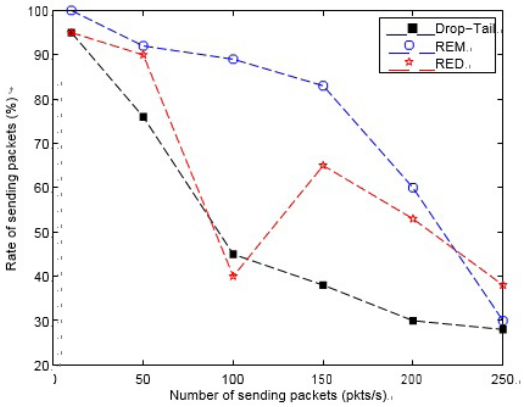

FIGURE 3. The packet rate of ad hoc networks under a DDoS attack.

III. SIMULATION AND ANALYSIS OF ATTACK EFFECTS

In this paper, we assume to consider the large-scale DDOS attacks since in daily practical scenarios there are always happened in real situations. According to the parameters given in **Table 1** [11] and using the network simulation software NS2 (version 2.35) in the Ubuntu environment, we compared the two indicators of packet rate and average end-to-end latency (with all nodes in a stationary state) imposed on ad hoc networks under DDoS attacks with the three queue management algorithms of Drop-Tail, RED, and REM. The simulation results were shown in Figure 3 and Figure 4. As can be seen from Figure 3 and Figure 4, under the condition of the same contract rate, Drop-Tail performed the worst, RED followed, and REM performed the best. But when the contract rate is constantly increased, the performances of the three algorithms all have decreased significantly. The simulation results show that as the first line of defense against unexpected network flow, traditional active and passive queue management algorithm possess very limited defense capacity against DDoS attack.

TABLE 1. NS2 simulation parameters.

Simulation Parameters	Value
Scene	300*300 m^2
Number of Nodes	100
Time	100 s
Mac	802.11
Routing Protocol	AODV
Traffic Flow	CBR
Packet Size	512 bits
Sessions	10

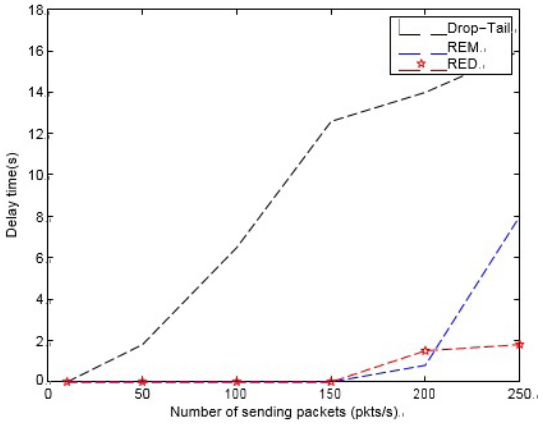

FIGURE 4. The average end-to-end latency of ad hoc networks under a DDoS attack.

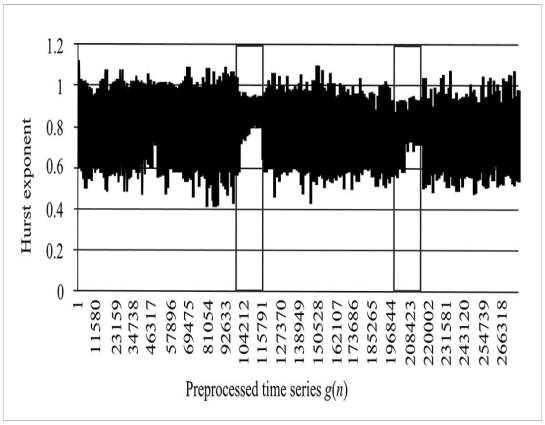

FIGURE 5. Hurst exponent for SYN-flood samples Hurst exponent.

A. SIMULATION SETTING AND METRICS

The simulation results in Figure 3 and Figure 4 show that under the same contract rate conditions, Drop-Tail performed the worst, followed by RED, and REM performed the best. However, as the contract rate steadily increases the performances of the three algorithms all decrease significantly. The simulation results show that, as the first line of defense against unexpected network flow, traditional active and passive queue management algorithms possess limited defense capacity against DDoS attacks [29]–[38].

B. DETECTION EXPERIMENTS

The queue management algorithms described in Section 3 were applied to the experimental data, and the results of the Hurst values [32] are shown in Figure 5. The DDoS attacks occurred in the frame part (the attacks occurred between 100,000 ms and 117,998 ms and between 200,000 ms and 217,998 ms), and the Hurst value during an attack period tends to be stable. Through the variance after treatment, in the low flow background, the Hurst index variance value obviously tends to 0, and it is relatively easy to detect the attack. However, in the context of high flow (after a box), the attack Hurst variance value and Hurst variance with normal flow values have no obvious difference, and the two states can only be distinguished from the correlation trend before and after of certain characteristics and node data. The variance and mean

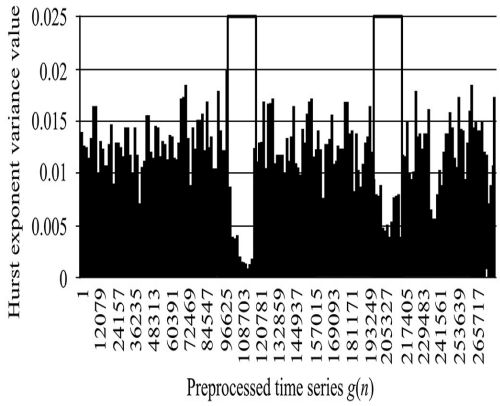

FIGURE 6. Hurst exponent variance value for SYN-flood samples.

processing of the Hurst index method in this paper are shown in Figure 6 and Figure 7, respectively. As seen from the graph, when a DDoS attack occurs, the Hurst index variance from the mean in the set threshold value falls.

From the experimental results (Figures 6 and 7), anomaly detection with the use of queue management algorithms was possible when the attack traffic reached 36.90. When the attack is enhanced while the background flow remains constant, the attack detection rate increases, and the attack detection integrity also increases; the attack traffic accounted

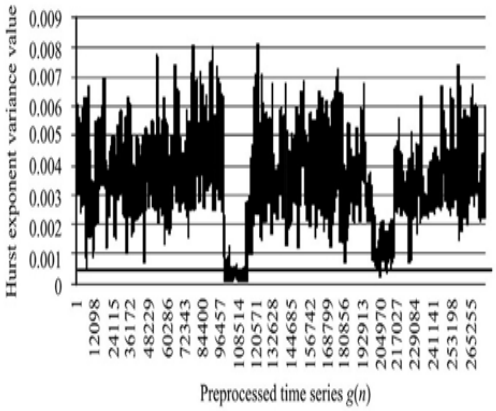

FIGURE 7. Hurst exponent average value.

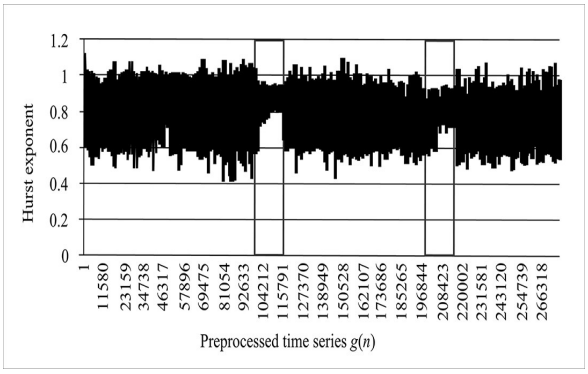

FIGURE 8. Algorithm detection delay comparison.

for a total flow of 91.36. When the attack is intensity invariant, the background flow changes are large; consequently, the integrity of the smaller flow background attack detection and the detection rate of integrity of the larger gap are significantly reduced.

C. COMPARISON WITH A TYPICAL METHOD

The DDoS simulation contains a 30-s period in which the attack intensity rises; therefore, by detecting the delayed reaction, early attack detection (0 s, 30 s) is possible to a certain extent. As seen in Figure 8, the performance of this method for delay detection using the same Holder index detection method used in [14] and [15] is quite good. Compared to the algorithm of low false alarm rate, the method of false alarm rate using the Holder index detection method is an obvious improvement. Therefore, this method has a better detection rate and greater integrity than the other two types of detection algorithms, as shown in Figure 9.

IV. MAIN STRATEGIES AGAINST DDOS ATTACK

Under conditions of low contract rates, active queue management algorithms possess strong defense capability against DDoS attack, but in the case of higher contract rates, both

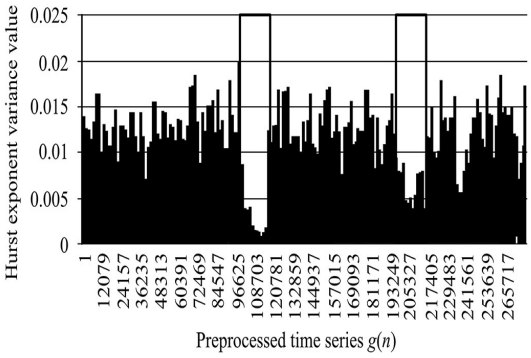

FIGURE 9. Algorithm detection false positive rate.

active and passive queue management algorithms are unable to effectively prevent DDoS attack. This means that other defense schemes must be integrated; a combination of various defense strategies can be used to comprehensively and effectively prevent DDoS attack. Because conventional DDoS attacks take advantage of the safety hazards of the underlying protocol or the design problem of the system to attack, most of the studies targeting this type of attack mainly rely on analysis of the grouping features, flow features and request rate of the network packets to detect attacks. These schemes can be divided into source-based attack detection and detection based on attacked nodes [13]–[25].

A typical source-based attack detection scheme is described in [12]. This scheme establishes a simple data-filtering model based on a feedback mechanism. The filtering model utilizes statistical techniques to determine the probability that a packet will be discarded based on the current network traffic and latency and the processing ability of the filtering nodes.

A. LIMITATIONS OF CURRENT TECHNIQUES

In [13], a decision tree-based DDoS detection system using an attacked node-based detection scheme was proposed. After detecting an attack, the system can track the location and path of the attacker's attack using a data flow model matching mechanism. In a simulation, the false negative rate of the system in detecting DDoS attacks was 1.2–2.4% and the false positive rate was 10%; the false negative rate and false positive rate for detecting the attack path were 8–12% and 12–14%, respectively. Some new recent techniques of DDoS should be considered in the following research [30]–[38].

V. CONCLUSION

This paper introduced three types of traditional network queue management algorithms, Drop-Tail, RED and REM. Using the network simulation software NS2 in an ad hoc network environment; we performed a simulation to compare the packet rate and average end-to-end latency of the three algorithms under DDoS attack. The results showed

that the active queue management algorithms, such as REM and RED, exhibited stronger defense capabilities than the passive queue management algorithm Drop-Tail under medium- and small-scale DDoS attacks; however, under large-scale DDoS attacks, all three algorithms exhibited insufficient defense capabilities. Because of the inherent shortcomings of queue management algorithms, in practical applications, queue management algorithms are usually integrated with other strategies that can prevent DDoS attacks (such as DDoS attack detection) to improve the network's defensive capabilities. Consequently, under the premise of ensuring a network's QoS, determining how to modify the original active queue management algorithm so that it can effectively address DDoS attacks will be our next research priority.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] J. Shuyuan, Y. Xiaochun, and B.-X. Fang, "Challenge of DDoS attacks detection," *IT Lett.*, vol. 6, no. 5, pp. 25–35, Sep. 2008.
[2] Z. Changwang, Y. Jian-ping, and C. Zhiping, "AQM Algorithms of Anti-DDoS Attacks," *J. Softw.*, vol. 22, no. 9, pp. 2182–2192, 2011.
[3] W. Jianxin, R. Liang, and X. Xuefeng, "Simulation and performance assessments on several active queue management algorithms," *Comput. Eng.*, vol. 33, no. 3, pp. 128–130, Feb. 2007.
[4] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2706–2716, 2016, doi: 10.1109/TIFS.2016.2596138.
[5] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network based defense mechanisms countering the DoS and DDoS problems," *ACM Comput. Surv.*, vol. 39, no. 1, pp. 1–42, Apr. 2007.
[6] F. LuPing, L. Shihua, and C. Pan, *NS-2 Network Simulation Basis and Application*. Beijing, China: National Defense Industry Press, May 2008, pp. 156–166.
[7] Z. Wei, T. Liang-Sheng, and P. Gang, "Dynamic queue level control of TCP/RED systems in AQM routers," *Comput. Elect. Eng.* vol. 35, no. 1, pp. 59–70, 2009.
[8] P. Guo, J. Wang, X. H. Geng, C. S. Kim, and J.-U. Kim, "A variable threshold-value authentication architecture for wireless mesh networks," *J. Internet Technol.*, vol. 15, no. 6, pp. 929–936, 2014.
[9] S. Athuraliya, S. H. Low, and V. H. Li, "REM: Active queue management," *IEEE Netw.*, vol. 15, no. 3, pp. 48–53, Mar. 2001.
[10] W. Chunming, J. Ming, and Z. Miao-Liang, "A comparative study of several active queue management algorithms," *J. Electron.*, vol. 32, no. 3, pp. 429–434, Mar. 2004.
[11] K. Zhiheng, C. Rongxiang, and D. Dejuan, *NS2 imulation Experiment—Multimedia and Wireless Network Communication*. Beijing, China: Electronic Industry Press, Mar. 2009, pp. 315–331.
[12] H.-X. Tan and W. K. G. Seah, "Framework for statistical filtering against DDoS attacks in MANETs," in *Proc. 2nd Int. Conf. Embedded Softw. Syst. (ICESS)*, Dec. 2005, p. 8.
[13] Y. C. Wu, H. R. Tseng, and W. Yang, "DDoS detection and traceback with decision tree and grey relational analysis," *Ad Hoc Ubiquitous Comput.*, vol. 7, no. 2, pp. 121–136, 2011.
[14] W. Wei and Q. Yong, "Information potential fields navigation in wireless Ad-Hoc sensor networks," *Sensors*, vol. 11, no. 5, pp. 4794–4807, 2011.
[15] Y. Jiang *et al.*, "Design and optimization of multiclocked embedded systems using formal techniques," *IEEE Trans. Ind. Electron.*, vol. 62, no. 2, pp. 1270–1278, Feb. 2005.
[16] W. Wei *et al.*, "GI/Geom/1 queue based on communication model for mesh networks," *Int. J. Commun. Syst.*, vol. 27, no. 11, pp. 3013–3029, 2014.
[17] Y. Jiang *et al.*, "Design of mixed synchronous/asynchronous systems with multiple clocks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 8, pp. 2220–2232, Aug. 2015.
[18] W. Wei, X. Fan, H. Song, X. Fan, and J. Yang, "Imperfect information dynamic stackelberg game based resource allocation using hidden Markov for cloud computing," *IEEE Trans. Serv. Comput.*, to be published, doi: 10.1109/TSC.2016.2528246.
[19] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, 2016, doi: 10.1109/TIFS.2016.2590944.
[20] W. Wei *et al.*, "Combined energy minimization for image reconstruction from few views," *Math. Problems Eng.*, vol. 16, no. 7, pp. 2213–2223, 2012.
[21] Y. Jiang *et al.*, "Bayesian-network-based reliability analysis of PLC systems," *IEEE Trans. Ind. Electron.*, vol. 60, no. 11, pp. 5325–5336, Nov. 2013.
[22] W. Wei, Y. Qiang, and J. Zhang, "A bijection between lattice-valued filters and lattice-valued congruences in residuated lattices," *Math. Problems Eng.*, vol. 36, no. 8, pp. 4218–4229, 2013.
[23] Y. Jiang *et al.*, "From stateflow simulation to verified implementation: A verification approach and a real-time train controller design," in *Proc. IEEE Real-Time Embedded Technol. Appl. Symp. (RTAS)*, Apr. 2016, pp. 1–11.
[24] W. Wei, H. M. Srivastava, and Y. Zhang, "A local fractional integral inequality on fractal space analogous to anderson's inequality," *Abstract Appl. Anal.*, vol. 46, no. 8, pp. 5218–5229, 2014.
[25] J. Guo, H. Zhang, Y. Sun, and R. Bie, "Square-root unscented Kalman filtering-based localization and tracking in the Internet of Things," *Pers. Ubiquitous Comput.*, vol. 18, no. 4, pp. 987–996, Apr. 2014.
[26] S. Xie and Y. Wang, "Construction of tree network with limited delivery latency in homogeneous wireless sensor networks," *Wireless Pers. Commun.*, vol. 78, no. 1, pp. 231–246, 2014.
[27] V. Singh, I. Gupta, and H. O. Gupta, "ANN-based estimator for distillation using Levenberg–Marquardt approach," *Eng. Appl. Artif. Intell.*, vol. 20, no. 2, pp. 249–259, Mar. 2007.
[28] C. Paar and J. Pelzl, "Understanding cryptography," in *A Textbook for Students Practitioners Introduction to Public-Key Cryptography*. Berlin, Germany: Springer 2009, pp. 149–170, ch. 6.
[29] M. Scott. *MIRACL: Multiprecision Integer and Rational Arithmetic c/c++Library,1988C2007*. [Online]. Available: http://www.shamus.ie/
[30] M. N. Kasirian and R. M. Yusuff, "An integration of a hybrid modified TOPSIS with a PGP model for the supplier selection with inter-dependent criteria," *Int. J. Prod. Res.*, vol. 51, no. 4, pp. 1037–1054, 2013.
[31] D. C. Parkes, M. O. Rabin, S. M. Shieber, and C. A. Thorpe, "Practical secrecy-preserving, verifiably correct and trust-worthy auctions," in *Proc. 8th Int. Conf. Electron. Commerce, New E-Commerce, Innov. Conquering Current Barriers, Obstacles Limitations Conduct. Successful Bus. Internet*, 2006, pp. 70–81.
[32] C. Shi-Wen, W. Jiang-Xing, G. Tong, and L. Ju-Long, "Self-adaptive detection method for DDoS attack based on fractional Fourier transform and self-similarity," in *Proc. Int. Comput. Sci. Inf. Technol.*, vol. 58. Jan. 2012, p. 42.
[33] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Proc. Annu. Int. Cryptol. Conf.*, vol. 576. 1991, pp. 129–140.
[34] R. Crandall and C. Pomerance, "Prime numbers: A computational perspective," *Exponential in Factoring Algorithms*, 1st ed. Springer. 2001, p. 191C226, ch. 5.
[35] M. Bichler and J. Kalagnanam, "Configurable offers and winner determination in multi-attribute auctions," *Eur. J. Oper. Res.*, vol. 160, no. 2, pp. 380–394, 2005.
[36] O. Kaiwartya *et al.*, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.
[37] M. N. Ahmed, A. H. Abdullah, and O. Kaiwartya, "FSM-F: Finite state machine based framework for denial of service and intrusion detection in MANET," *PloS One*, vol. 11, no. 6, p. e0156885, 2016.
[38] M. Bichler and J. Kalagnanam, "Configurable offers and winner determination in multi-attribute auctions," *Eur. J. Oper. Res.*, vol. 160, no. 2, pp. 380–394, Jan. 2005.

WEI WEI received the Ph.D. and M.S. degrees from Xian Jiaotong University in 2011 and 2005, respectively. He is currently an Assistant Professor with the Xi'an University of Technology. His research interests include wireless networks and wireless sensor networks application, image processing, mobile computing, distributed computing, and pervasive computing.

HOUBING SONG (M'12–SM'14) received the M.S. degree in civil engineering from the University of Texas at El Paso, El Paso, TX, USA, in 2006, and the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, USA, in 2012. He was an Engineering Research Associate with the Texas A&M Transportation Institute, Texas A&M University System, in 2007. In 2012, he joined the Department of Electrical and Computer Engineering, West Virginia University, Montgomery, WV, USA, where he is currently an Assistant Professor and the Founding Director of both the West Virginia Center of Excellence for Cyber-Physical Systems, sponsored by the West Virginia Higher Education Policy Commission, and the Security and Optimization for Networked Globe Laboratory. He has authored over 80 peer-reviewed papers. His research interests are in the areas of cyber-physical systems, Internet of Things, intelligent transportation systems, wireless communications and networking, and optical communications and networking. His research has been supported by the West Virginia Higher Education Policy Commission. Dr. Song is a member of ACM. He has served as the General Chair or Technical Program Committee Chair for six IEEE international workshops and a Technical Program Committee Member for numerous international conferences, including ICC, GLOBECOM, INFOCOM, and WCNC, among others. He has been an Associate Editor or a Guest Editor of over ten international journals.

HUIHUI WANG (M'13) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in 2013. In 2011, she was an Engineering Intern with Qualcomm, Inc. In 2013, she joined the Department of Engineering, Jacksonville University, Jacksonville, FL, USA, where she is currently an Assistant Professor and the Founding Chair of the Department of Engineering. She is with the Department of Engineering, Jacksonville University. She has authored over 30 articles and holds one U.S. patent. Her research interests include cyber-physical systems, Internet of Things, healthcare, and medical engineering based on smart materials, robotics, haptics based on smart materials/structures, ionic polymer metallic composites, and MEMS.

XIUMEI FAN received the B.S. degree in electron information engineering from Tianjin University in 1989 and the Ph.D. degree in communication and information system from Northern Jiaotong University in 2001. She is a Professor with the School of Automation and Information Engineering, Xi'an University of Technology. She has finished some projects of NSFC and The National High Technology Research and Development Program of China in delay tolerant networks, vehicular networks, and mobile Internet. She is now leading two advanced wireless network projects under NSFC and SRFDP. Her current research interests focus on wireless broadband network, VANET, DTN, and mobile Internet.