Scientific Research Publishing

Journal of Information Security, 2018, 9, 25-32
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

The Study of Secure Congestion Control for TCP in Ad Hoc Networks

Weinan Zhang[1], **Li Lin**[2], **Li Du**[1]

[1]Computer Science and Engineering, Northeastern University, Shenyang, China
[2]Division of Engineering and Applied Science, California Institute of Technology, Pasadena, CA, USA
Email: duli@mail.neu.edu.cn

How to cite this paper: Zhang, W.N., Lin, L. and Du, L. (2018) The Study of Secure Congestion Control for TCP in Ad Hoc Networks. *Journal of Information Security*, **9**, 25-32.
https://doi.org/10.4236/jis.2018.91003

Received: October 21, 2017
Accepted: December 2, 2017
Published: December 5, 2017

Abstract

Ad hoc networks are vulnerable to various attacks. In addition, congestion caused by limited resources may occur at any time in the transmission of the packets at intermediate nodes. This paper proposes a dynamic congestion control method of the selection of a secure path. By estimating the average queue length at the nodes, the congestion level at present is detected. If the occurrence of the possible congestion is predicted, the network will select a new path where all nodes have been certified as trusted nodes, generating session keys in the TCP three-way handshake to prevent the denial of service attacks. Simulation results show that the new algorithm is superior to TCP Reno algorithm in terms of security, packets loss rate, throughput, and end-to-end delay.

Keywords

Congestion Control, Average Queue Length, Security, Session Keys

1. Introduction

Ad hoc network possesses the features of distribution, flexible infrastructure, and equal nodes. AA Gutub [1] proposes a new trend of data visualization, trying to link illogical data inputs which are as source of judgments in interactive ways. Hajj services are improved to gain advantage from the development of the exploratory data visualization technology [2]. However, it is vulnerable to all kinds of security attacks due to the poor security management. High security system suitable to hide sensitive text-data on personal computer is proposed and implemented [3]. The system hiding techniques involves AES cryptography followed by image based steganography as two layers to insure high security. The flexible security system provides security information to the user to select the cover-image within the PC based on his/her security priority [4]. Prevention methods such as cryptography [3] [5] only consume limited resources, but also are costly. From the detection [4] perspective, intrusion detection system is necessary to detect attackers.

The main purpose of the congestion control is to improve the network performance by reducing the delay and buffering the overflow caused by network congestion. However, the traditional congestion control cannot be used directly in the Ad hoc network. This is because the delay and packets loss are not necessarily caused by network congestion, but may be mistaken as congestion loss. Here, we focus on the congestion control that can adapt to the security of Ad hoc networks and propose a new algorithm. By estimating the average queue length at the nodes, the congestion control is dynamically adjusted. When the occurrence of the possible congestion is predicted, the network will select a new path where all nodes have been certified as trusted nodes, generating session keys in the TCP three-way handshake to prevent the denial of service attacks. So it has important theoretical significance and the value of practical application in the field of information security and wireless network security.

2. The Design of Secure Congestion Control for TCP

2.1. The Selection of Secure Path

In the past decades, the watchdog system [6] using promiscuous-hearing technology has been implemented to increase the failure counter of sending node if packets loss is observed. In an adaptive confirmation system [7], if the source node receives the acknowledgement packet from the destination node, it represents a successful transmission. Otherwise, the source node switches to double ACK mode to detect malicious nodes. In the proposed enhanced adaptive confirmation [8] system with intrusion detection, secure ACK (SACK) is an improved version of the double ACK system. When a malicious behavior is found in SACK mode, the source node will switch to misbehavior report authentication (MRA) to find an alternative path to reach the destination node, affecting the malicious behavior report.

In solving the problem of black hole attack [9], all legal nodes will send joining request with a trust value of 1 at the initial stage of the network. If the requesting node does not receive acknowledgement from the delegate node, it will stop sending joining request. Each node first verifies the node's address before processing any request and then processes the request if the node is on the trust-list. When the delegate node receives the joining request, it will validate the trust value of the requesting node. If the trust value is matched, the requesting node is added to the trusted list and gets broadcasted in the network. The threshold for the joining request is set to 20 requests per second. **Figure 1** shows the algorithm's flow chart.

The concept of bilinear mapping [10] is introduced to allocate the nodes' key to handle the denial of service attacks [11] and ensure the security of the connection

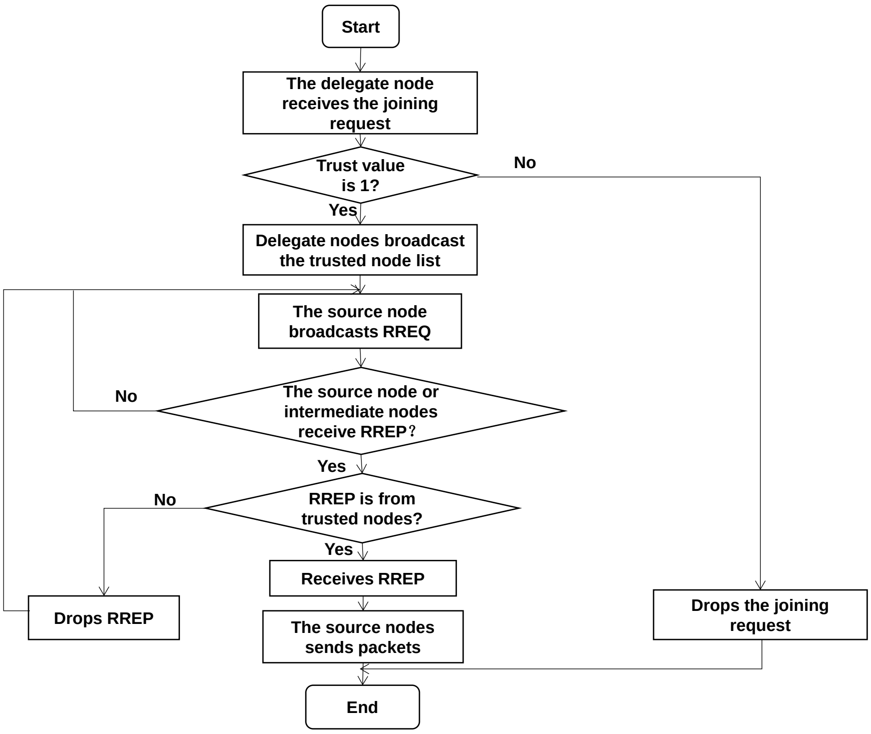
Start
The delegate node receives the joining request
Trust value is 1?
No
Yes
Delegate nodes broadcast the trusted node list
The source node broadcasts RREQ
No
The source node or intermediate nodes receive RREP？
Yes
No
RREP is from trusted nodes?
Yes
Receives RREP
Drops RREP
The source nodes sends packets
Drops the joining request
End

Figure 1. The algorithm of selecting a secure path.

of TCP three-way handshake. After allocating the resource for the source node (S), S starts to send packets with authentication tags. Whenever the intermediate node detects congestion, it will send Explicit Congestion Notification (ECN) to Acknowledgement (ACK) [12].

2.2. The Design of Congestion Control

A simple example is shown in Figure 2. The source node S sends packets to the destination node D, the primary path is S to 1 to 3 and then to D. When intermediate node 1 predicts the occurrence of possible congestion, it will stop sending packets and initialize the safe route discovery mechanism. From the trust-list of node 1, node 2 is selected as the next hop. After receiving the packets from node 1, node 2 will send packets to the destination node D.

The average queue length can provide a direct measurement of the congestion status. The maximum value of the threshold (*Max*) and minimum value of the threshold (*Min*) are set to the queue length respectively, and the queue threshold represents the current state of the queue. Here, w_q stands for the queue weight, and the link utility would be very low if the three thresholds' values are set too small. On the other hand, congestion may occur before the node is notified if the thresholds are too large. Equation (1), (2), and (3) are used to set the thresholds' values.

$$Min = 35\% \times \text{Que\_length} \tag{1}$$

$$Max = 2 \times Min \tag{2}$$

$$w_{\text{qup}} = w_{\text{qpre}} \times H \times S \tag{3}$$

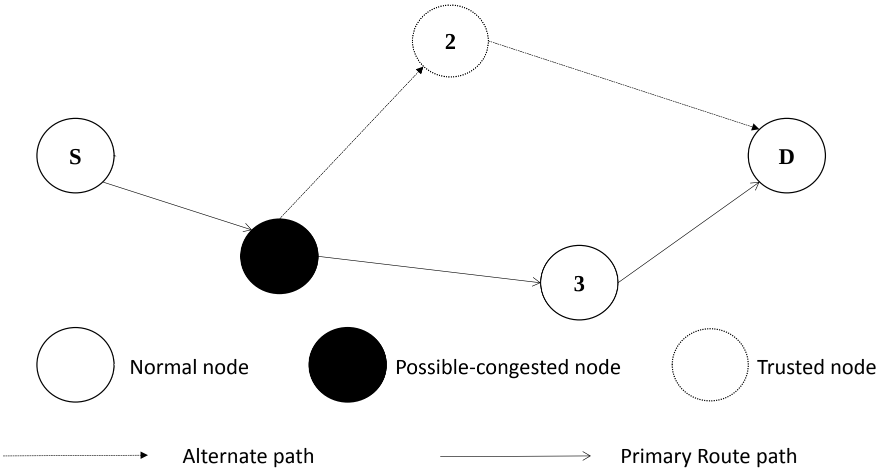

Figure 2. A simple example for secure congestion control.

The average queue length is used to specify all traffic fluctuations, which reflect persistent congestion in the network through a long-term variation of the instant queue. The average queue length is calculated by Equation (4) as followed.

$$\text{Aver\_queue} = \left(1 - w_q\right) \times \text{Aver\_queue} + \text{Ins\_queue} \times w_q \tag{4}$$

Equation (3) is used to dynamically set w_q. *H* represents hop counts, and *S* represents the number of packets sent per second. If the average queue length is smaller than the value of *Min* and the instant queue is smaller than half of the queue length, nodes are in the normal status.

The congestion may occur when the average queue length is between the values of *Min* and *Max*, and the discovery mechanism for a secure path is initiated. When the instant queue is larger than *Max*, the value of *Max* should be reset because of the wrong selected path. If the average queue length is larger than *Max*, the nodes are in the congestion status and the congestion control is carried out. The flow chart of the algorithm is shown in Figure 3.

3. Simulation Results and Analysis

Here, NS-2 [13] is used to compare the performance of the new algorithm with a secure congestion control and the TCP Reno algorithm under malicious attacks. The number of malicious nodes is set to 10 and the maximum running speed of nodes is 20 m/s. The wireless propagation model is two-ray ground.

Figure 4 and Figure 5 show the difference between the two algorithms in packets loss rate and throughput with the increase of simulation time.

As shown in Figure 4, during secure attacks, the new algorithm reduces the possibility of link-disconnection caused routing reestablishment. In comparison, link interruptions frequently occur for the TCP Reno algorithm. As a result, packets loss rate gets more severe with the increasing simulation time.

In Figure 5, with the increase of simulation time, the number of packets received by the receiver per second declines for the TCP Reno algorithm, resulting

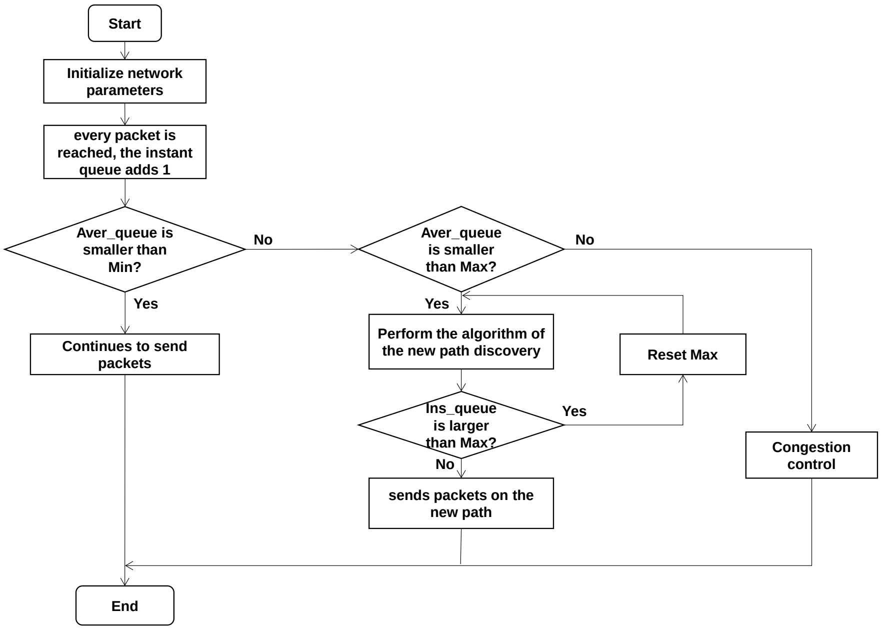
Start
Initialize network parameters
every packet is reached, the instant queue adds 1
Aver_queue is smaller than Min?
No
Yes
Continues to send packets
Aver_queue is smaller than Max?
No
Yes
Perform the algorithm of the new path discovery
Reset Max
Ins_queue is larger than Max?
Yes
No
sends packets on the new path
Congestion control
End

Figure 3. The algorithm of congestion control.

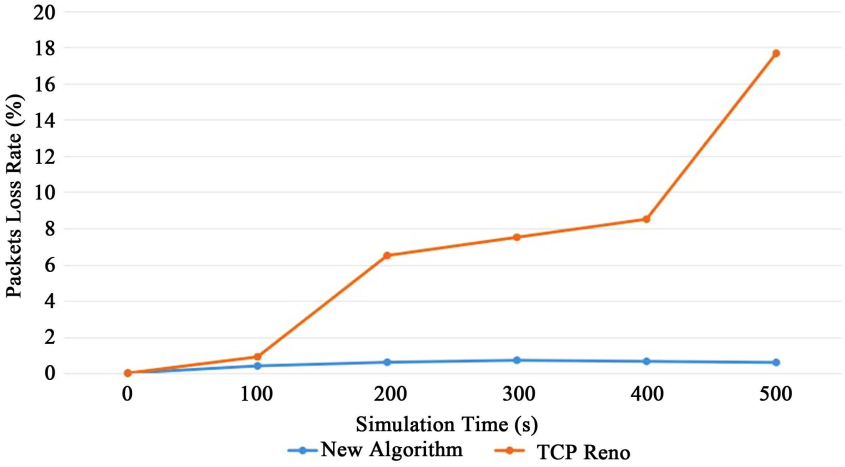

Figure 4. Comparison of packets loss rate with different time.

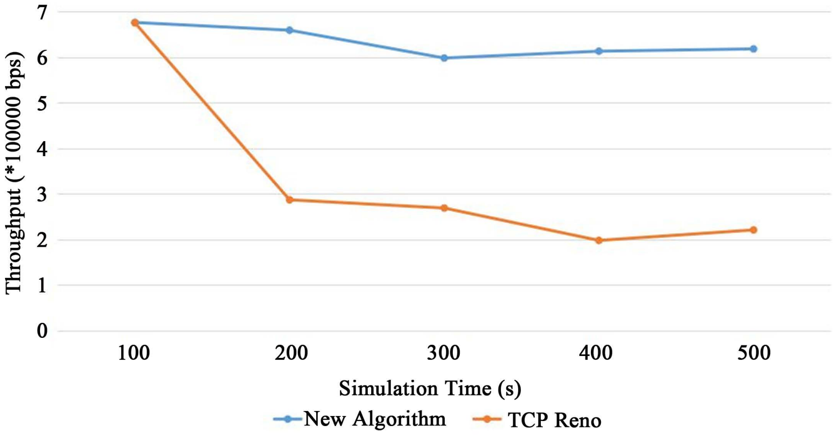

Figure 5. The algorithm of selecting a secure path.

a sharp decrease in the throughput. In comparison, the new algorithm has very low packets loss rate and makes most packets received successfully, providing a relatively constant throughput.

We then fixed simulation time at 300 s and Studied the difference between the packets loss rate and the end-to-end delay under different hop counts.

In Figure 6, when the number of hop counts is less, because the nodes are in the normal status, the end-to-end delay is relatively low for both algorithms. The congestion may occur during the increase of the number of hop counts. The new algorithm selects a new path to prevent the attack of malicious nodes, while the TCP Reno algorithm continues to send packets on the original path, which can only drop packets when congestion occurs. As a result, the end-to-end delay is larger for the TCP Reno algorithm.

In Figure 7, with the increase of hop counts, the probability of packets loss in the network will increase for both algorithms. The TCP Reno algorithm causes serious packets loss due to its incapability to predict the congestion. In comparison, the new algorithm makes a prediction based on the average queue length and changes the path in advance, reducing the number of packets loss.

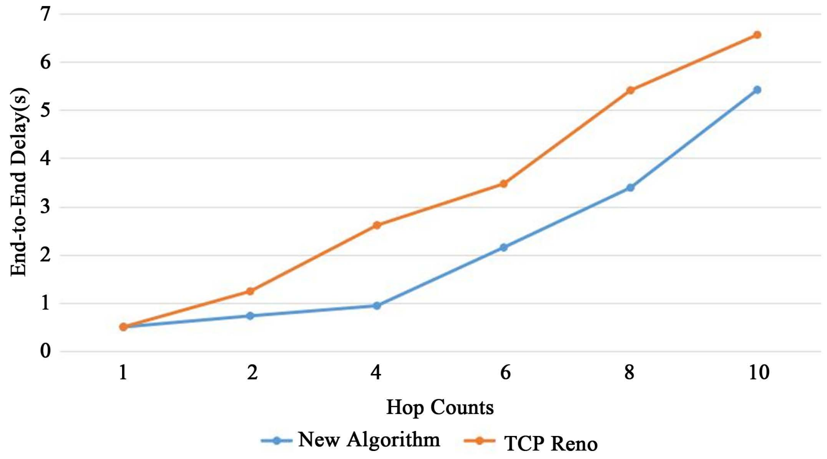

Figure 6. Comparison of end-to-end delay.

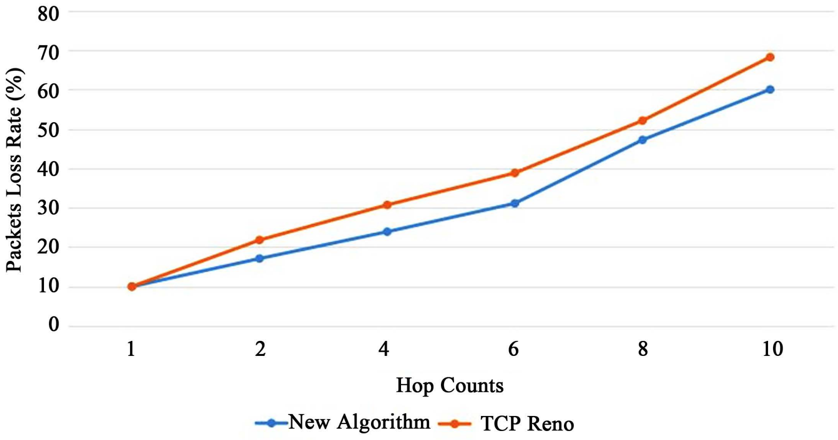

Figure 7. Comparison of packets loss rate with different hops.

The simulation results above indicate that the new algorithm is always superior to the TCP Reno algorithm in terms of security, network throughput, end-to-end delay, and packets loss rate.

4. Conclusion

We propose a new secure congestion control mechanism by using the average queue length to predict the degree of congestion in the network. By comparing the performance of the new algorithm and the TCP Reno algorithm under malicious attacks, the simulation results show that the new algorithm has better performance in security, network throughput, end-to-end delay, and packets loss rate. Thus, the performance can be improved effectively in Ad hoc networks.

References

[1] Gutub, A.A. (2015) Exploratory Data Visualization for Smart Systems. *Smart Cities* 2015 - 3*rd* *Annual Digital Grids and Smart Cities Workshop*, Burj Rafal Hotel Kempinski, Riyadh, Saudi Arabia, May 2015, 1528-1537.

[2] Alharthi, N. and Gutub, A. (2017) Data Visualization to Explore Improving Decision-Making within Hajj Services. *Scientific Modelling and Research*, **2**, 9-18. https://doi.org/10.20448/808.2.1.9.18

[3] Al-Otaibi, N.A. and Gutub, A.A. (2014) 2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers. *Lecture Notes on Information Theory*, **2**, 151-157. https://doi.org/10.12720/lnit.2.2.151-157

[4] Aljuaid, N. and Gutub, A. (2014) Flexible Stego-System for Hiding Text in Images of Personal Computers Based on User Security Priority. *Proceedings of* 2014 *International Conference on Advanced Engineering Technologies* (*AET*-2014), Dubai UAE, 25-26 December 2014, 250-256.

[5] Dife, W. and Hellman, M.E. (2006) New Directons in Cryptography. *In IEEE Transacton on Informaton Theory*, IT-22, Nov. 2006, 644-654.

[6] Marti, S., Giuli, T.J. and Lai, K. (2000) Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *In ACM Proceedings of the* 6*th Annual International Conference on Mobile Computing and Networking*, Boston, Massachusetts, USA, 06-11 August 2000, 255-265. https://doi.org/10.1145/345910.345955

[7] Sheltami, T., Al-Roubaiey, A., Shakshuki, E. and Mahmoud, A. (2009) Video Transmission Enhancement in Presence of Misbehaving Nodes in MANETs. *Multimedia Systems*, **15**, 273-282. https://doi.org/10.1007/s00530-009-0166-0

[8] Shakshuki, E.M., Kang, N. and Sheltami, T.R. (2013) EAACK a Secure Intrusion-Detection System for MANETs. *IEEE Transactions on Industrial Electronics*, **60**, 1089-1098. https://doi.org/10.1109/TIE.2012.2196010

[9] Soleimani, M.T. and Kahvand, M. (2014) Defending Packet Dropping Attacks Based on Dynamic Trust Model in Wireless Ad Hoc Networks. *In IEEE* 17*th Mediterranean Electrotechnical Conference* (*MELECON*), Beirut, Lebanon, 13-16 April 2014, 362-366. https://doi.org/10.1109/MELCON.2014.6820561

[10] Xu, W.Q., Wang, Y.M., Yu, C.H., *et al*. (2000) Cross-Layer Optimal Congestion Control Scheme in Mobile Ad Hoc Networks. *Journal of Software*, **21**, 1667-1678.

[11] Ghosh, U. and Data, R. (2012) A Novel Signature Scheme to Secure Distributed

Dynamic Address Configuration Protocol in Mobile Ad Hoc Networks. *In IEEE WCNC*, 2700-5, Apr. 2012.

[12] Ramakrishnan, K.K., Floyd, S., Black, D. and Ramakrishnan, G.K. (2001) The Addition of Explicit Congeston Notificaton (ECN) to ip. RFC Editor, USA, 3186. 2001.

[13] DARPA (2014) The Network Simulator-NS2. http://www.isi.edu/nsnam/ns/index.html