Advances in Engineering Research, volume 177
International Symposium on Engineering and Earth Sciences (ISEES 2018)

# Study of TCP FREEZE Protocol Behavior in Wireless Data Transmission Networks

Hasambiyev I.V.
Head of the Department of Communication Networks and Switching Systems
Grozny State Oil Technical University named after academician M.D. Millionshchikov
Grozny, Russia
hiv_77@mail.ru

Daudov I.M.
Department of Programming, Information, and Communications Technologies
Chechen State University
Grozny, Russia
Ibr024@mail.ru

Khazhmuradov M.A.
National Science Center Kharkov Institute of Physics and Technology
Kharkiv, Ukraine
khazhm@kiptkharkov.ua

Magomedov I.A.
Department of Programming, Information, and Communications Technologies
Chechen State University
Grozny, Russia
ismwork@mail.ru

Khadzhiyeva L.K.
Department of Communication Networks and Switching Systems
Grozny State Oil Technical University named after academician M.D. Millionshchikov
laura.hadjieva3009@mail.ru

***Abstract*—At present there are several protocols ensuring data transmission within wireless data transmission networks. The majority of them are byte-oriented protocols with reliable data, which is delivered along the route with connection setup.**

***Keywords—TCP Freeze protocol; wireless networks; overloads; data transmission; control mechanism; connection setup; rapid retransmission; fast recovery; bandwidth.***

## I. INTRODUCTION

In recent years, various modifications of the TCP protocol were suggested, however they mainly concern the loss recovery phase (TCP Tahoe, TCP Reno, TCP New Reno, M-TCP and TCPSACK protocols). The mechanism of data transmission control was only changed in the TCP Freeze protocol [2]. It was possible by assessing the available size of the bandwidth of a wireless channel as an overload sign. The beginning of the overload is defined by measuring the difference between the current time value of data transmission package within Tn connection and its minimum value with further correction of intensity of package delivery to the network (according to the value of this difference).

Let us consider the heterogeneous environment where the connection by the TCP Freeze and TCP Reno protocols is done through the general critical channel with bearing capacity C and time of package transmission equal Tn. Both sources function in overload prevention phase. The channel interacts with a router implementing the mechanism thus discarding the back part of a queue and having a service coefficient. Since the general capacity for each connection on a route cannot exceed the channel bandwidth, which is a critical site for a given route, then the existence of such sites for this route will limit the bandwidth capacity of the entire route.

## II. METHODS AND MATERIALS

The TCP Freeze protocol controls the speed of package delivery by assessing the available size of a bandwidth for connection. The biggest difference of such method of control is a new approach to the assessment of the bandwidth size available for connection in comparison with the TCP Reno protocol [2]. The size of the proposed window of data packages changes dynamically on the basis of Tn measurement (time of data package transmission within the established connection) whereas the TCP Reno protocol continues to increase the size of a floating window of connection up to the first loss of a package, which it considers as an overload sign.

The methods of TCP Freeze protocol by speeds of package delivery to a network. It is supposed that when the expected and actual speeds are almost equal, the network is not overloaded, i.e. in case of an overload, the actual speed shall be lower the expected one.

Thus, the overload control mechanism functions against sequential execution of the following stages:

– calculation of the expected speed of package delivery by a source to the network according to the following expression:

$$V = W / T_{min}, \quad (1)$$

where V – expected speed, W – current size of a floating window of the considered connection, a – minimum Tn value for the considered connection throughout the overload-free period (usually during the transmission of the first data package);

– calculation of the actual speed of package delivery by a source to the network according to the following expression:

$$V_p = W / T_p, \qquad (2)$$

– assessment of the number of packages by a source, where such packages are in the queue of a router at every receipt of an acknowledgement package via the following expression:

$$Q = (V - V_p) \cdot T_{min}; \qquad (3)$$

– adjustment of the current size of a floating window W(t) of connection via the following:

$$W(t) = \begin{cases} W(t-1)+1, & if\ Q < \alpha, \\ W(t-1)-1, & if\ Q > \beta, \\ W(t-1), & in\ other\ cases, \end{cases} \qquad (4)$$

where Q – smoothing coefficient in the calculation of cycle duration of the retransmission timer, and Q – value of the upper boundary of the number of nonsusceptible packages within the current route.

The given expressions show that when the values of expected and actual speeds are close, the connection does not use the whole available bandwidth size, hence, it is necessary to increase the speed of data delivery. Similarly, when the actual speed is much lower the expected, thus causing network overload and, hence, it is necessary to reduce the speed of data transmission.

Within the slow start phase, the entry condition of which is successful connection, the TCP Freeze protocol remains valid before reaching some threshold value (usually equal 1). While this condition is satisfied, the size is increased by one package for every second time interval of package transmission. Hence, the exponential increase in the TCP Freeze size with a speed smaller than the speed of the TCP Reno protocol takes place during the slow start. When the size of a floating window W reaches a threshold value of the exit from a slow start phase, or the condition is met, the TCP Freeze protocol will enter the phase of overload prevention.

In this case the TCP Freeze protocol functions on the basis of two parameters (usually equal 1 and 3, respectively), thus changing the size of a floating window according to expression (4). The loss of a package may happen in case of one of two events:

– expiration of the package transmission timer;

– consecutive delivery of three recurrent acknowledgement packages.

In the first case the threshold value for an exit from the slow start phase is set as a half value of the current size of a floating window, and the size of a floating window – as 1 package (or 2 packages in some cases) and then the TCP Freeze protocol again enters the slow start phase.

In the second case the source ensures rapid retransmission and fast recovery similar to the TCP Reno protocol. In fact, the TCP Freeze protocol implements the improved mechanism of rapid retransmission based on more accurate internal timer of a protocol [3]. After an exit from a phase of rapid retransmission, the TCP Freeze protocol sets the size of the floating window as 3/4 of the current values and again enters the overload prevention phase.

The main feature of the TCP Freeze protocol within the wireless networks is the processing of messages of the lower levels of protocol stacks, which allows the recipient finding the forthcoming connection loss due to weak signal in case of the movement of a mobile node and transferring the protocol to a temporary phase of inactivity. Such transition is carried out when a recipient sends a special acknowledgement package to a source.

After a source receives it, the data transmission is stopped and all current connection parameters are fixed (size of a floating window, value of the retransmission timer, etc.), then the sender begins to send trial packages of a special format to the recipient to check the availability of the recipient. Upon return of the recipient to a wireless network zone and receipt of a trial package, he generates a response to the sender in the form of the acknowledgement package of the last correctly accepted package and the connection is restored on the basis of recorded parameters.

Despite some advantages of the TCP Freeze protocol in comparison with modern implementation of the TCP protocol (smaller time of data transmission, smaller fluctuations of the floating window size and much smaller number of retransmissions of packages), below there is a variety of reasons constraining its stage-by-stage introduction into modern networks [4].

## III. RESULTS

Currently, the TCP protocol is the most widespread protocol of the transport level ensuring reliable delivery of data. The logic of delivery of TCP segments is that the data flow is divided into segments. Each segment has a special tag of the sequence number to guarantee the delivery of segments in the necessary order. The reliability of the TCP protocol is reached due to acknowledgement of delivery (ACK), which is sent to the sender in case of successful delivery of segments. If the recipient gets the inconsistent segment, then ACK with the number of the necessary segment is sent. In case the sender does not receive acknowledgement of delivery of the transmitted package during the RTT (round trip time – time for transmission and acknowledgement of reception), then he either transmits a package again, or stops transmitting if the connection is lost. Such method of reliability guarantees data delivery, however, the resources of the communication channel are inefficient.

From the scientific perspective it is interesting to note that in the modern world the main problems include the overload of wireless networks and the long time of loading. The solution of these critical problems is equally important in telecommunication systems. For example, in his book *Ad Hoc Wireless Networks: Architectures and Protocols* Siva Ram Murthy says that TCP-F ensures simple solution with feedback for minimization of problems resulting from frequent ruptures of a route in special wireless networks. It also allows the TCP overload control mechanism to react to an overload in the network. TCP-F depends on ability of intermediate nodes to find route errors and the ability of routing protocols to restore the broken path during a short period. Besides, FP shall have an

opportunity to receive the correct path (package passing) to the TCP-F sender for sending the RFN package. It is simple with the routing protocol, which uses source routing, i.e. dynamic source routing (DSR). If a route to the sender is inaccessible in FP, there might be a need for additional packages to control the RFN package routing [5].

In his book *Ad Hoc Wireless Networks: Architectures and Protocols* Siva Ram Murthy answers the question: why TCP does not work in special wireless networks? He defines the main reasons for deterioration, which TCP faces when ad hoc is used in wireless networks. Let us consider the main reasons.

Incorrect interpretation of package loss: traditional TCP was developed for wired networks where the loss of packages is generally caused by the network overload. The network overload is defined by the RTO period of the sender's package. Once the package loss is detected, the node sender triggers the overload in a network and causes the overload control algorithm. Special wireless networks have much higher loss of packages due to such factors as high bit error ratio (BER) in a wireless channel, increased collisions caused by hidden terminals, noise depending on a competitor's location, unidirectional communication lines, frequent path ruptures caused by mobility of nodes and inherent properties of a fading wireless channel.

Frequent path ruptures: Special wireless networks experience dynamic changes of network topology due to unlimited mobility of nodes in the network. Changes of topology lead to frequent changes in the connectivity of wireless channels, and, hence, it may require the frequent change of a route to a certain destination. The responsibility for a route search and its restoration after breakage is bound to the network level (routing protocols of the network level are considered in detail). As soon as the path is broken, the routing protocol triggers the restoration of a route. This process of route restoration takes a significant amount of time to receive a new route to the destination. The restoration time of a route depends on the number of nodes in the network, ranges of node transmissions, current network topology, bandwidth of the channel, load of traffic in networks and character of the routing protocol. If the restoration time of a route is higher than the RTO period of the TCP sender, then the TCP sender assumes an overload in a network, retransmits the lost packages and initiates the overload control algorithm. These repeated transmissions may reduce the carrying capacity and power of the battery. Eventually, when a new route is detected, the TCP capacity still remains low for some time as it shall create an overload window since traditional TCP undergoes slow start.

Influence of a path length: it is found that the TCP capacity is quickly deteriorated with the increase in the path length within the topology of a linear ad hoc chain of wireless networks [6]. The possibility of path rupture increases with a path length. Considering the fact that the probability of communication rupture equals p l, the probability of a path rupture (p b) for a path length k may be obtained as P b = 1 - (1 - p l) k, and hence, with the increase in a path length the probability of a path rupture increases thus leading to deterioration of network capacity.

The scientific novelty of the study is the fact that it proves the TCP Freeze protocol features in wireless networks, which represents messages of lower levels of a protocol stack, which in turn allows the recipient finding the forthcoming rupture of connection due to signal strength loss during movements of a mobile node and transferring the protocol to a temporary phase of inactivity.

Dynamic change of the connection route.

$T_{min}$ indicates the smallest time of package transmission within the established connection and is used for quantitative measurement of data transmission speed. In case the connection route is changed, the value of this parameter may change, which will not substantially influence the protocol in case of such change to the smaller side since the $T_{min}$ will be updated. If the new route has bigger TR value, the connection will not be able to define the exact reason of such increase – the beginning of an overload or change of a route. It is implied that such TR increase is only caused by the overload and, therefore, the size of a floating window shall be reduced [7].

With the increase in package transmission time, the product of connection bandwidth size increases, (C) for the period of package transmission, TR, which is the assessment of the number of packages within the network. The expression W – C TP allows calculating the number of packages which are in queues on a connection route. The task of the TCP Freeze protocol is to maintain the number of packages in queues within the established route between values $\alpha$ and $\beta$, hence, there is a need to increase the size of a floating window in order to preserve the invariable number of packages in queues with the increase in package transmission time.

When the connection is established on a free site of a network the value $T_{min}$ will be close to the minimum possible. If later the overload begins, the measured TR value increases, hence, the $T_{min}$/TR ratio decreases.

If the connection is established after the beginning of the overload in the network, then its $T_{min\,i+1}$ value will be higher than $T_{min\,i}$, and the $T_{min\,i+1} / T_{i+1}$ ratio will be higher than the $T_{min\,i} / T_i$ ratio.

Thus, the following expression is the condition to start the reduction of the floating window size [5]:

$$W > \beta /(1 - T_{min} / T_p) . \quad (5)$$

Hence, for the above connections, the critical value of parameter W will be smaller than for connections that were established later, and, as a result, the latter ones may reach high efficiency values [8].

The following expression is the condition to start the increase of the floating window size:

$$W < \alpha /(1 - T_{min} / T_p) \quad (6)$$

Since the expression on the right part is bigger for connections, which were established later, then it is more

probable for them to increase the floating window size thus leading to disproportionate distribution of available bandwidth.

Network overload.

When more data enters any network than it is capable to process, the network congestion is formed. In this respect, the Internet is not an exception. Though the network level also tries to fight against overload, the main contribution to the solution of this problem is the reduction in the rate of data transmission by the TCP protocol.

Theoretically, the package conservation law may be used to fight against overload. The idea is not to transfer new packages to a network until the old ones leave it (i.e. are delivered). The TCP protocol tries to achieve this by dynamic control of a window size [9].

The first step in fight against overloads is to detect the overload. It was difficult to find the overload in the network a few decades ago. It was difficult to understand why the package is not delivered in time. Besides the possibility of the network overload, there was also a great probability to lose a package due to high level of noises within the line.

At present, package losses during transmission are quite rare since the majority of long-distance communication lines are fiber-optic (though in wireless networks the ratio of packages lost due to noises is quite high). Respectively, the majority of the lost packages on the Internet is caused by congestions. All TCP algorithms of the Internet imply that the package losses are caused by network overload and thus follow the timeouts as for reasons of problems, similar to miners observing the canaries.

Before discussing the fact how TCP reacts to an overload, let us describe the methods of its prevention applied by the protocol. The corresponding window size shall be chosen when the overload is detected. The recipient can specify the window size based on the amount of free space in a buffer. If the sender considers the size of his window, then the overflow of the recipient's buffer will not cause the problem, however this problem may still arise due to the overload on any site of the network between the sender and the recipient [7].

## IV. RESULTS

Continuous network overload. In this situation the connections may incorrectly assess the time of package transmission and turn the network into constantly overloaded state.

Let the connection open in the overloaded network. Due to increased time of packages in a queue caused by packages of other connections, the time value TP for new connection will be much higher the actual value for this route. As a result of such inaccurate estimation of parameter $T_{mini}$, the size of a floating window will be overestimated. Such scenario will be the same for each established connection thus leading to continuous network overload. One of the solutions of the problem of continuous overload may be the method similar to the case of dynamic change of a connection route when routers with RED discipline are used [10].

Bandwidth. Let the size of the router queue upon entering the channel, which is a critical site of a route, equal $\ell(t)$ packages, and the sizes of floating windows of traffic sources within TCP Freeze and TCP Reno protocols equal W(t) and W1(t) of packages. The router ensures the discipline of FIFO queue service with intensity of package processing equal μ.

The expressions for the smallest time of data package transmission at zero queue size (Tq (t)) may be written as follows:

$$T_0 = T_p + 1/\lambda \tag{7}$$

$$T_{i\div}(t) = T_p + (\ell(t) + 1/\lambda) \tag{8}$$

where Tp – real time of package transmission within the established connection.

During prevention of overloads, in case of a loss of package with constant probability P, the size of the floating window W1 for the connection by the TCP Reno protocol can be calculated using the following expression:

$$W_1 = \sqrt{8/3P}. \tag{9}$$

The expression (9) can be presented in the graphic form (Fig. 1) and describe the following:

$$W_1(t) = K/\sqrt{P(t)}, \tag{10}$$

where K – constant.

The expression to calculate the capacity of the TCP Reno protocol, V1 (t) is as follows:

$$V_1(t) \equiv W_1(t)/T_{i\div}(t) = \frac{K}{\sqrt{p(t)}} \cdot \frac{1}{T_{i\div}(t)}. \tag{11}$$

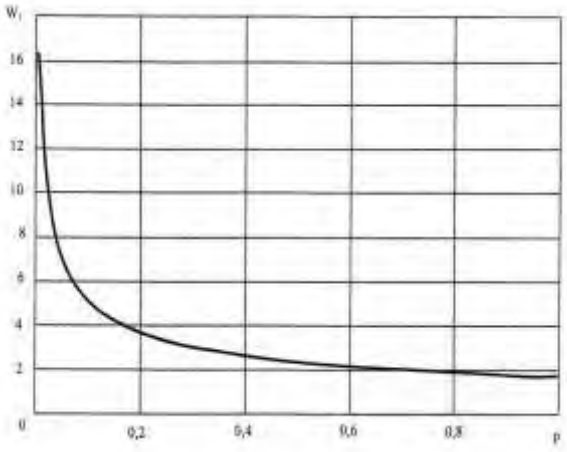


Fig. 1. Dependence of the floating window size of the TCP RENO protocol, W1 on the probability of package losses p

By substituting the expression (8) into (11) we get:

$$V_1(t) = \frac{K}{\sqrt{p(t)}} \cdot \frac{\mu}{\lambda \cdot T_p + \ell(t) + 1}. \tag{12}$$

For further analysis of the carrying capacity it is convenient to write the expression for calculation of Q parameter as follows:

$$Q = \left( W(t) / \mathrm{T}_0 - W(t) / \mathrm{T}_{\text{î÷}}(\text{å}) \right), \quad (13)$$

where Q – assessment of the number of packages in a queue within the established route for connection by the TCP Freeze protocol.

If expressions (7) and (8) are substituted in (13), we will receive the following expression:

$$Q = W(t) \cdot ( \ell(t) / \ell(t) + C\mathrm{T}_{\text{ð}} + 1) \cdot \mathrm{T}_0 \quad (14)$$

Then the method of data transmission control to prevent the overloads of the TCP Freeze protocol may be written as follows:

$$W(t+1) = \begin{cases} W(t)+1, & \alpha \left( \dfrac{\ell(t) + \lambda \mathrm{T}_p + 1}{\ell(t)} \right) > W(t); \\ W(t), & \alpha \le Q \le \beta; \\ W(t)-1, & \beta \left( \dfrac{\ell(t) + \lambda \mathrm{T}_p + 1}{\ell(t)} \right) . < W(t) \end{cases} \quad (15)$$

The expression for the capacity of the TCP Freeze, V(t) may be obtained using expressions (8) and (15) for each of the cases given in (15) as follows:

$$\mathrm{V(t)} = \mathrm{W(t)} / \mathrm{Tоч}\ (\mathrm{t}). \quad (16)$$

Thus, with the increase of α and β parameters of the TCP Freeze protocol, the product

$$\alpha \left( \frac{\ell(t) + CT_p + 1}{\ell(t)} \right) \quad (17)$$

increases thus leading to the increase in W(t) value and, hence, to the protocol efficiency. Consequently, within the heterogeneous wireless network environment the TCP Freeze protocol can also reach higher capacity than the TCP Reno protocol provided the α and β parameters are increased.

Therefore, the paper gives theoretical justification of the TCP Freeze protocol modification based on the improved method of data transmission control.

## V. CONCLUSIONS

The use of the above described mechanisms allows preventing the congestion of wireless networks.

Since with the increase in package transmission time the product of the bandwidth size increases, (C), for the period of package transmission, TP, which represents the assessment of the number of packages in the network. The expression W- C TP allows calculating the number of packages in queues on a connection route.

The main task of the TCP Freeze protocol is to maintain the number of packages in queues on the established route, therefore, with the increase in the size of a floating window, to maintain the invariable number of packages in queues with the increase in package transmission time.

Thus, the given study presents the analysis of the TCP Reno and the TCP Freeze protocols, which made it possible to demonstrate theoretical opportunities of TCP Freeze protocol modification based on the improved method of data transmission control.

## *Acknowledgements*

The authors would like to express deep and profound gratitude to Dr. of Psychology, Candidate of Technical Sciences, professor, director of the Institute of Applied Information Technologies, head of the Department of Informatics and Computer Facilities of Grozny State Oil Technical University named after M.D. Millionshchikov – Alisultanova Esmira Dokuyevna for her contribution and valuable remarks during the study.

## *References*

[1] A.S. Dadashova, N.A. Moiseenko, A.P. Pyatibratov, L.P. Gudyno, A.A. Kirichenko, Computers, networks and telecommunication systems. Educational and methodical complex, M.: EA O.I. publishing house, pp. 292, 2009.

[2] V.G. Olifer, N.A. Olifer, Computer networks. Principles, technologies, protocols. Study manual, St. Petersburg, Piter, 2014.

[3] P. Roshan, D. Liere, Fundamentals of wireless local networks of 802.11 standard, M.: Williams, pp. 296, 2004.

[4] Yu.A. Vintenkova, S.V. Kozlov, E.A. Spirina, "Analysis of efficiency of joint dynamic routing within broadband radio access networks with traffic of TCP, HTTP, FTP protocols," Journal of radio electronics. Moscow, pp. 17, 2017.

[5] Ya.S. Dymarsky, N.P. Krutyakova, G.G. Yanovsky, Communication network control: principles, protocols, applied tasks, M.: Mobile Communications, 2003.

[6] M. Allman, On the Generation and of TCP Acknowledgments [Text] / M.: ACM Computer Communication Review, Vol. 28, No. 5, pp. 4-21, 1998.

[7] J.S. Ahn, P.Danzing, Z. Liu, L. Yan, Evaluation of TCP Vegas: Emulation and Experiment, ACM Computer Communication Review, Vol. 25, No. 4, pp. 185-195, 1995.

[8] S. Brakmo Lawrence, Larry L. Peterson, TCP Vegas: End-to-End. Congestion Avoidance on a Global Internet, IEEE journal on SelectedAreas in Communications, Vol. 13, No. 8, pp. 1465-1480, 1995.

[9] A. Furuskar, Allocation of multiple services in multi – access wireless networks – Mobile and wireless communication networks, September 2002, pp.201-205.

[10] Bo Xing, Nalini Venkalausbramanian, Multi-constraint dynamic access selection in always best connected networks, Donald Bren school of information and computer sciences, University of California.