Feedback Based Congestion Control For TCP/IP Performance Enhancement in Wireless Networks

[1] Leenus.M, [2] Dr.Nancy Jasmine Goldena
[1] Research Scholar, [2] Assistant Professor
[1]Manonamaniam Sundaranar University, [2] Sarah Tucker College, Manonmaniam Sundaranar University
[1, 2] Tirunelveli, Tamilnadu, India

Abstract: The growth of wireless network services and service providers directly proportional to the immense requirement of shared resource accessing feature among the wireless service consumers. wireless network systems are a mixture of autonomous network domains, which are always open and dynamic. Wireless network systems treats large number of users with its services, who are often changeable, and different domains has their individual policies. The existing identity based wireless network models are not scalable, closed, infeasible and inflexible. TCP/IP performance tuning in next generation wireless networks is a heuristic process to handle it with proper care due to the immense effect and exponential quantification. This paper deals with the feedback based congestion control for TCP/IP performance enhancement in wireless networks. The proposed enhancement method is a unification approach with the unique individual implementation towards the fine tuning of TCP/IP performance improvements. The results and discussions of our proposed method lead to the implementation of enhancement of neuro fuzzy based TCP/IP performance improvement in wireless network computing.

Index Terms: **Wireless network, TCP/IP, Feedback, Performance, Enhancement**

I.INTRODUCTION

A *service* is an implementation of well defined functions that are able to interact with other functions. The *service oriented architecture* (SOA) is comprised of a set of services that can be realized by technologies such as the web services [4].

A *domain* can be defined as a protected computer environment, consisted of users and resources under an access control policy. The collaboration which can be established among domains leads to the formation of a virtual organization.

A *user* in a Wireless network environment can be a set of user identifiers or a set of invoked services that can perform on request one or more operations on a set of resources. Furthermore, we identify two types of users. These are the resource requestor and the resource provider [9]. The former type of user acts like a resource access or usage requestor, and the latter type of user acts like a provider of its own sharable resources. All users are restricted by the policies enforced in their participating domains and virtual organization [6].

A *resource* in a Wireless network environment can be any sharable hardware or software asset in a domain and upon which an operation can be performed [5].

Access control's role is to control and limit the actions or operations in the Wireless network system that is performed by a user on a set of resources. In brief, it enforces the access control policy of the system, and at the same time it prevents the access policy from subversion. Access control in the literature is also referred to as access authorization or simply authorization [2].

A Wireless network *access control policy [3]* can be defined as a Wireless network security requirement that specifies how a user may access a specific resource and when. Such a policy can be enforced in a Wireless network system through an *access control mechanism.* The latter is responsible for granting or denying a user access upon a resource. Finally, an *access control model* can be defined as an abstract container of a collection of access control mechanism implementations [8], which is capable of preserving support for the reasoning of the system policies through a conceptual framework [1]. The Wireless network service architecture is represented in Figure 1.1.

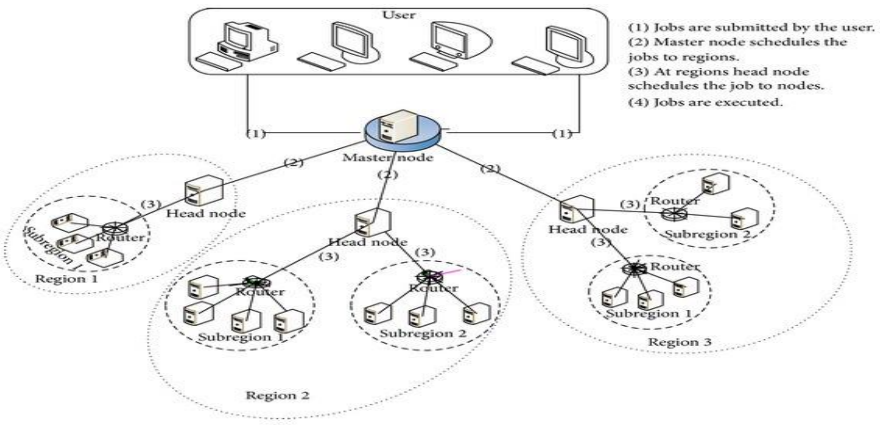

Figure 1.1: Wireless network Service Architecture [10]

II. METHODOLOGY REQUIREMENT

TCP-Casablanca-The receiver has a better "view" of the losses than a sender. Casablanca discriminator must be implemented at the receiver. When detecting wireless losses, TCP receiver must use the duplicate acknowledgements to inform the sender about the nature of the loss. TCP sender, when receiving a notice that the loss is not due to congestion, should react appropriately.

TCP-ECN- Explicit Congestion Notification (ECN) is a perfect example of this end-to-end approach, in which routers report congestion to the TCP sender using an IP header. ECN supposes that dynamic queuing management is arranged at the central group of routers, allowing the discovery of congestion, before loss occurs and before the queue overflows.

The basic terminologies are as follows,

Packet Identifier : RTP sequence number.

Packet Explicit Congestion Notification (ECN) Marking : If ECN [RFC3168] is used, it is necessary to report on the 2-bit ECN mark in received packets,

Packet Arrival Time : Arrival time stamp at the receiver of the media. The sender requires the arrival time stamp of the respective packet to determine delay and jitter the packet had experienced during transmission.

III.PROPOSED IMPLEMENTATION

The proposed methodology not only focuses on scalability at the architectural level where management, maintenance and operational costs do not increase as the number of system components (users, applications, policies and enforcement points) increases along with the dynamic access control through multiple roles for the user access simultaneously towards the Wireless network service environment.

3.1 Proposed Methodology:

The proposed methodology for the enhancement in TCP/IP performance for next generation Wireless network access schema diagram is as follows,

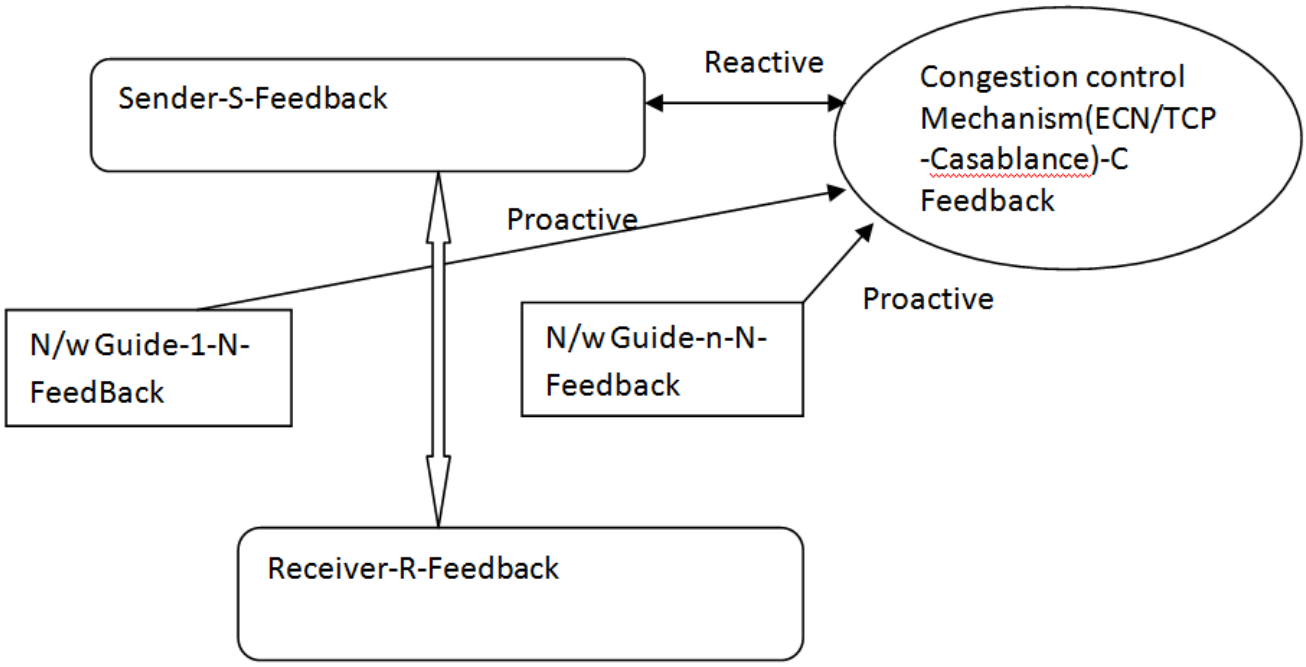

Figure 3.1: Proposed Methodology for Wireless network TCP/IP performance Enhancement

3.2. Phase-1: S-Feedback Enhancement

The sender sense the channel for congestion with a Boolean validation stamp.
Based on the stamp value,
If true then Negative Feedback
else Positive Feedback
end if.

The enhanced Wireless network scalewith sender monitoring affects the ability of wireless network administrators to maintain its complexity. The proposed methodology

Focuses on assigning different administrators for different services. The assignment is based on the capability of handling the request and with minimized cost structure. The following Table 3.1 represents the multiple Feedback assignment with its efficiency based on the wireless network service access.

Table 3.1: Sender Self Feedback Structure Table

Service Request	Sender Feedback-Self
No of users < Resource	"+" ve
No of Protocols > Resource	"-" ve
Topology=low/medium	"+" ve
Topology=Mixed Hybrid	"-" ve
Complex user interface	"-" ve

3.3 Phase-2 C-Feedback Enhancement

3.3.1 TCP-ECN

- L (1 bit): is a boolean to indicate if the packet was received. 0 represents that the packet was not yet received and all the subsequent bits (ECN and ATO) are also set to 0. 1 represent the packet was received and the subsequent bits in the block need to be parsed.
- ECN (2 bits): is the echoed ECN mark of the packet. These are set to 00 if not received, or if ECN is not used.
- Arrival time offset (ATO, 13 bits): is the relative arrival time of the RTP packets at the receiver before this feedback report was generated measured in milliseconds. It is calculated by subtracting the reception timestamp of the RTP packet denoted by this 16bit block and the timestamp (RTS) of this report. If the measured value is greater than 8.189 seconds (the value that would be coded as 0x1FFD), the value 0x1FFE MUST be reported to indicate an over-range positive measurement. If the measurement is unavailable, the value 0x1FFF MUST be reported.

3.3.2 TCP-Casablanca scheme,
(1) packets are marked in or out by the TCP sender (endpoint),
(2) packets of the same TCP connection get different discard priorities, and
(3) packets marked out are dropped first (with probability , before any packet marked.

Table 3.2: Congestion control mechanism based Feedback Evaluation Membership Values

Congestion Control mechanism	C- Feedback based on Fuzzy Membership function
Wired-Wireless	0.1
Loss	0.2
Delay	0.3
Single Bit-Signal	0.4
Multi bit Signal	0.5
Low-Bandwidth	0.6
Lossy links	0.7
Short flows	0.8
Variable infeasible rate links	0.9
Uncontrolled delay	1

3.4 Phase-3 N-Feedback Enhancement

3.4.1 User Arrival Count

When scalable increases by m users and the dynamicity of role also splits into m roles. Such that
Users= $\{u_1, u2, u3....u_m\}$ =Total of m users
Roles= $\{r_1,r_2,r_3....r_m\}$=Total of m corresponding roles

Then the User Arrival Count UAC= $\sum$ui.ri where i= 1 to m

If additional j users appended with corresponding j roles such that m+j=n, i.e. (n-m) new users scaled up. Then

The new User Arrival Count UAC new= $\sum$ui.ri where i=1 to n.The final expansion slowly integrates with the function of Distribution, Which is equilant to the Poisson distribution f $(\mu, \delta) = e^{-\mu} \mu^{\delta} / \delta!$

Table 3.3: Network Guide based Feedback EvaluationValues

User Arrival	Role-60% congestion limit for dual	Total access
5	3	8
10	6	16
15	9	24
20	12	32
25	15	40
30	18	48

3.4.2 User access updates Frequency

The minimum access update frequency =static access for m users=m
The average access of r for m users =mCr =m!/r!(m-r)!
The Maximum access update frequency=m combinations= m!
So the frequency lies between m and m! .

3.5 Phase-4 R-Feedback Receiver Feedback Enhancement

Receiver is the person who receives the message or for whom the message is meant for. It is the receiver who tries to understand the message in the best possible manner in achieving the desired objectives.

3.5.3 Fuzzy based Receiver Feedback Evaluation:

It will be executed on evaluating the Packet reception with network characteristics of trust level based on the collected recent transaction session information. A zero to one point scale of receiver feedback evaluation excluding the extremes are listed in the Table 3.4 as follows,

Table 3.4: Receiver Feedback Evaluation Permission Membership Values

Receiver Feedback Evaluation	Distrust reception	0.9
	Suspect reception	0.7
	Normal Reception	0.5
	Good Time based acknowledgement	0.3
	Trust worthy based Exact interval of time	0.1

IV. RESULTS AND DISCUSSION

The following table 3.5 illustrates the performance tuning of TCP/IP based on Feedback evaluation strategies along with the resultant graph for the fusion of sender,congestion control mechanism,Network guide and receiver side feedback attainments with the proposed methodology by the combined approach of fuzzy based membership functions.

Table 3.5: Performance Tuning for TCP/IP based on Feedback strategies

Feedback Types	Efficiency	Cumulative Success Rate
S-Feedback	5 %	5 %
C-Feedback	5 %	10 %
N-Feedback	40 %	50 %
R-Feedback	50 %	100 %

The proposed schema results with 4 component based feedback system to evaluate all the possibilities with an minimum increase of 10 % (50-40) to a maximum of 30%(40-5-5) attainment rate.

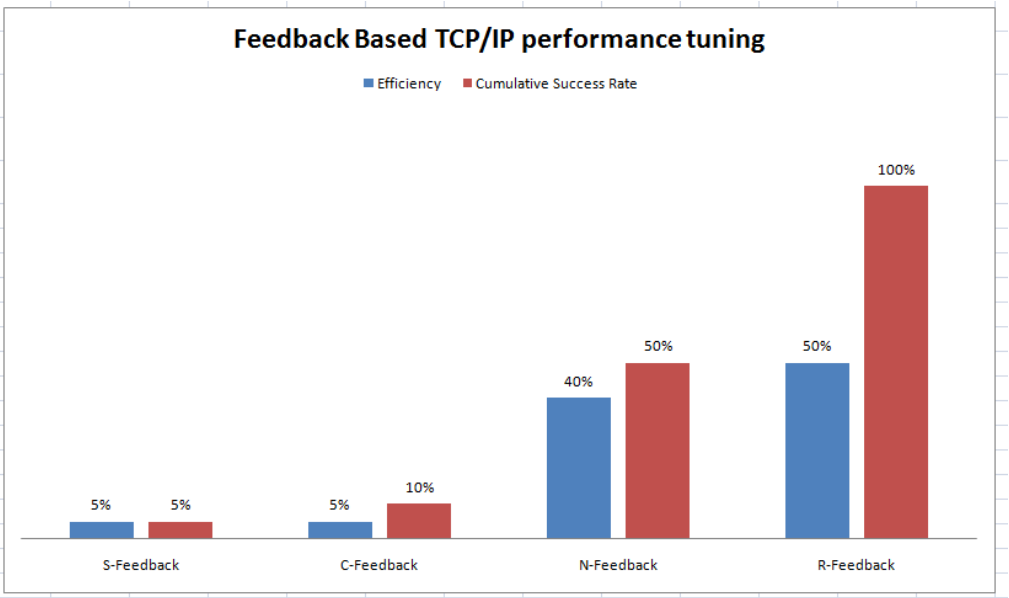

Figure 4.1: Proposed Methodology for Wireless network TCP/IP performance Enhancement Results

V.CONCLUSION

The combined enhancement of TCP/IP performance tuning focuses on sender modification or congestion control mechanism modification or network modifications or receiver modification or the fusion of all.But the merger of these two strategies in wireless network computing with unified enhancement focuses on all the aspects in terms of TCP/IP performance tuning during and after the amalgamation. This paper deals with the enhancement of TCP/IP performance in Wireless network computing systems comprises the Upgradable construct for the architectural design, administrative structure, and Time division credential system along with the safety constraints. The optimization of TCP/IP performance tuning in wireless network computing comprises user association, component interaction, resource collaboration and safety service access and the unification of enhancement in TCP/IP performance tuning includes the individual components of both the strategies along with the ensured enhancement in user arrival rate, user access update frequency for the combined context collection, Our proposed methodology yields the result improvement from 10% to 30% is also an significant improvement over wireless networks.

REFERENCES

[1] N. Aboudagga, M.T. Refaei, M. Eltoweissy, L. DaSilva & J. Quisquater[2005], “Authentication Protocols for Ad Hoc Networks : Taxonomy & Research Issues,” In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless & mobile networks, Quebec, Canada, pp. 96-104.

[2] W. Du, R. Wang & P. Ning[2005], “An Efficient Scheme for Authentication Public Keys in Sensor Networks,” In Proceeding of 6th ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc), IL, USA, pp. 58-67.

[3] H. Cam, S. Ozdemir, D. Muthuavinashiappan & P. Nair, “Energy Efficient Security Protocol for Wireless Sensor Networks,” Vehicular Technology Conference, 2003, vol. 5, pp. 2981-2984.

[4] C. Karlof & D. Wagner [2003], “Secure Routing in Wireless Sensor Networks: Attacks & Countermeasures,” In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols & Applications, Anchorage, AK.

[5] J. P. Walters, Z. Liang, W. Shi & V. Chaudhary, 2005, “Wireless Sensor Network Security: A Survey”.

[6] K.S.J. Pister, J.M. Kahn & B.E. Boser 1999, “Smart Dust: Wireless networks of milli-meter scale sensor nodes”.

[7] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, & D.E. Culler, “SPINS: Security protocols for sensor networks”, Wireless Networks, 2002, vol. 8, pp. 521-534.

[8] H. Luo, P. Zerfos, J. Kong, S. Lu, & L. Zhang 2002, “Self-Securing Ad Hoc Wireless Networks.” In Seventh IEEE Symposium on Computers & Communications (ISCC '02).

[9] D. Park, C. Boyd, E. Dawson. “Classification of Authentication Protocols: A Practical Approach.” Proceedings of the Third International Workshop on Information Security.

[10] S. Zhu, S. Setia & S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks.” In 10th ACM Conference on Computer & Communications Security (CCS '03).