Integrating the content security with the QoS in Data networks

Manjunath Ramachandra, Selva kumar, Narendranath Udupa, *Member, IEEE,*

***Abstract*—In a traffic flow, it is important to maintain the end to end data security. An attack on the network results in poor user experience. Security of the data in a flow to a greater extent depends up on the vulnerability and availability of the data for the hackers or attacks. By reducing the data or the stranded time at every hop, it is possible to provide a better security for the data. In this paper, security is treated as a service parameter. The goal of this parameter is to reduce the stranded time in each hop and the number of hops in the path; while the delay parameter aims at the reduction of the overall delay in the path. To enhance the security, the data to be transferred is divided in to multiple independent flows. Such an organization of the data would be extremely useful in peer to peer or mesh networks. The different flows are expected to follow independent paths. In this paper, a method is explored to reduce the vulnerability of a packet for hacking by reducing the available duration of the packet in the network.**

***Index Terms*—Active queue management, Artificial neural networks, Content Security, Intrusion, Network attack**

I. Introduction

DATA security in a network has turned out to be challenging. With the devices increasingly relying on the internet for the content streaming and the poor availability of the infrastructure to detect and respond to the attacks on the network, a built-in mechanism is required to address this issue. Even the usage of long 128 bit keys for encryption has failed to provide fool proof security [1].

In order to prevent the hackers to attack the network, the available time to meddle with the data or the amount of available data to run the decipher algorithms or both are to be reduced [2]. The simple solution towards this end is to divide the data in to multiple streams. Each packet or stream follows its own path due to which the probability of the interception gets reduced. The different streams may be encrypted with different keys to enhance the security. The mutual information between the two streams is to be a maximum. By the time the key is deciphered, the hacker gets a data encrypted with a different key. Thus, the intention of the hacker to sabotage the data fails.

In section II the proposed scheme of providing security for the data is discussed with simulation results. The impact of the proposal to minimize the delay in the path is provided. Section III summarizes the discussion

II. Active Queue Management Method for QoS Provisioning in IP Networks ELEMENTS

In order to provide the required quality of service (QoS) for the data streamed over the network, a controller is introduced in the feedback path to provide the information of the traffic status of the network. It provides a mechanism for the content sources to adjust the streaming rates and thereby prevent the network from getting overloaded. The controller also reduces the delay that in turn enhances the security of the data packets. Typically, in the data network, active queue management algorithm such as random early detection (RED) [3] is used to provide the feedback information. The RED output is related to the probability of the packet drops. However, if the feedback signal from RED is predicted in advance of time and used as the control signal, it provides sufficient time for the sources to adjust the transmission rate. It provides a holistic view of the traffic ahead of time. A shifted version of this prediction, at least by 1 time step, provides better results [4]. The shifts reduce the delay in the buffers. So less time is available for the hackers to meddle with the data.

The predicted feedback signal available at the source provides an indication of the packet drops at a future time instant. If it is too different from the actual output of the RED that reaches the source, it indicates the possibility of an attack. It also indicates the possibility of tampering of the feedback signal to cover up the network attack. Viral attack or spasm may be detected by observing the number of sockets or connections opened by the same machine. An abnormal increase in the number of sockets opened per unit time due to a possible viral attack may be equated to increase in the number of streams N. As a result, the parameters such as delay, packet drop probability etc changes drastically. Rate of change of these parameters with respect to the streams from the same source indicates abnormal activities

The attacker can also resort to QoS attacks wherein the data streamed over the network fails to provide the agreed user experience. The loss rate can be high or simply the delay and (or) the jitter can be unacceptably large resulting in poor quality of the rendered information. The attacker just needs to delay the packets in the network to achieve this. Under this

Manjunath Ramachandra is with Philips Innovation Campus, Bangalore. (Phone: 91-80-41892981; e-mail: manjunath.ramachandra@ Philips.com).

Selvakumar Palaniyappan is with Philips Innovation Campus, Bangalore. (e-mail: selvakkumar.palaniyappan@ Philips.com).

Narendranath Udupa is with Philips Innovation Campus, Bangalore. (e-mail: narendranath.udupa@ Philips.com).

condition, the usage of predicted feedback signal can enhance the QoS as evident from the simulation results.

The simulation has been carried out in MATLAB version 6. A differentially fed artificial neural network (DANN) [5] is used for the prediction of the packet drop probability. The samples of the signal up to simulation time t=10 units is used for training the neural network. There after the prediction starts. Hence, the graphs coincide up to this point of time. The feedback signal and its predicted versions have a strong correlation with the number of data sources N. The variation of the QoS parameters with N are shown the figures 1 to 3. Here the number of sources is varied from 40 to 120. The figures explain how the packet delay decreases with time when a shifted feedback on the congestion status of the channel is provided. A shift of 4 is considered. As the number of streams increases, the advantage of splitting the data in to multiple streams gets reduced. However, still it would be better than not using the shifted prediction for the feedback signal. It calls for an optimal choice of splitting the data in to streams. If the split is fine, it provides less chance for the hacker to intercept them. However, the packets stay for long in the network providing sufficient time to decrypt them. Usage of shifted and predicted feedback signal can however reduce this delay and provide a workaround.

III. Conclusion

Meeting security constraints for the data that gets transferred over the networking has been challenging ever since the data transfer over the network started. Though tools and techniques were developed to counter attacks on the network, new methodologies were developed by the attackers exploiting the loopholes in the technology. Day by day, the intrusion and attacks are coming with more harm and impact. The divide and conquer approach for the data in to multiple independent streams each encrypted differently would help in overcoming the network attacks.

The simulation shows encouraging results in reducing the duration of the overall presence of a packet in the network that helps in enhancing data security. As an extension for the simulation, the data packets are to be deliberately hacked & it is required to see how fast the data sources can analyze the predicted data loss and realize the hacking. The performance with more secure keys during such eventuality is to be tested.

References

[1] Roshan Duraisamy, Zoran Salcic, Maurizio Adriano Strangio, Miguel Morales Sandoval**,** Supporting symmetric 128-bit AES in networked embedded systems: an elliptic curve key establishment protocol-on-chip, *EURASIP Journal on Embedded Systems*, pp4, No 1, 2007

[2] Manjunath.R, Dynamic management of security constraints in advanced enterprises, in *Advances in Enterprise IT Security*, IDEA group publishers, 2007

[3] Floyd, S., and Jacobson, V., Random Early Detection gateways for Congestion Avoidance, *IEEE/ACM Transactions on Networking*, V.1 N.4, August 1993, p. 397-413

[4] Manjunath.R, K.S.Gurumurthy, (2004) Maintaining Long-range dependency of traffic in a network, CODEC'04

[5] Manjunath.R, Gurumurthy.K.S., Information geometry of differentially fed artificial neural networks, TENCON 2002, Vol 3, PP 1521 – 1525

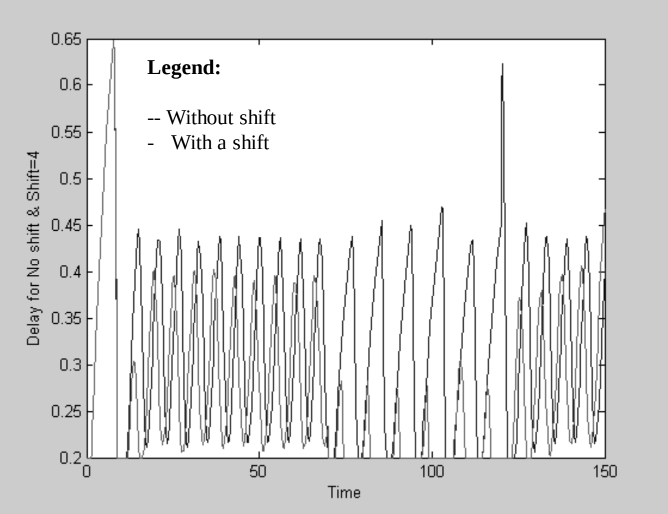

Fig 1. Packet delay for 40 sources with a shift of 4

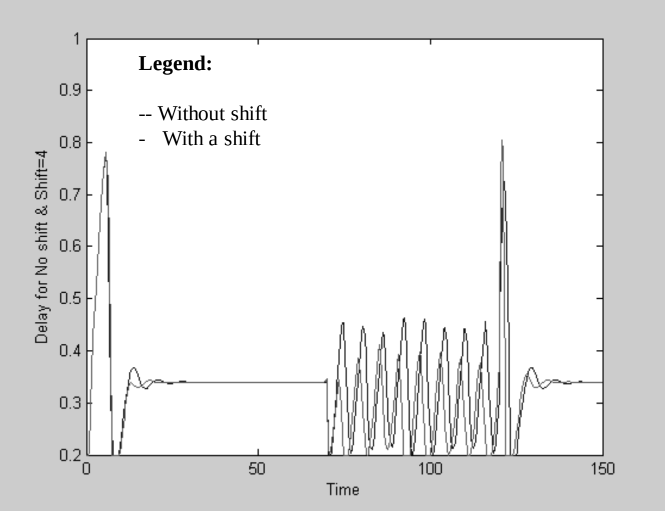

Fig. 2. Packet delay for 80 sources with a shift of 4

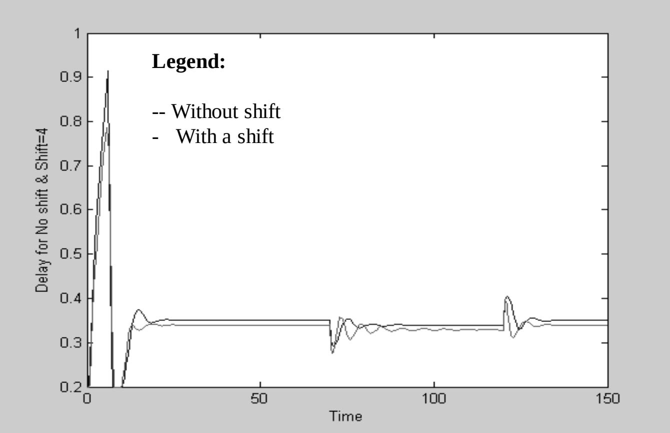

Fig. 3. Packet delay for 120 sources with a shift of 4