QoS safety protocol analysis in FHAMIPv6/MPLS/Diffserv integration and load balancing algorithm

Jesus Hamilton Ortiz
Closemobile Research & Development SL

Bazil Taha Ahmed
Autonomous Madrid University

Juan P. Pantoja
Campinas State University - UNICAMP

Abstract

One of the most important aspects to consider in order to provide quality services in an ad hoc network is the security. In the integration FHAMIPv6 / MPLS / DiffServ and congestion algorithms, we analyses QoS but do not consider the QoS safety. The security issue is essential for not degrade QoS. This paper analyzes the most relevant aspects in security issue in the following protocols (FHAMIPv6, MPLS, Diffserv and Load balancing algorithm). These problems can degrade QoS in the integration.

Detected security problems, we can avoid them. So, we can maintain the quality of service achieved in the integration FHMIPV6 / MPLS / Diffserv in Ad hoc networks. QoS safety protocol analysis will be presented below.

Keywords: *Security, Protocols, QoS, Ad hoc, integration, FHAMIPv6, MPLS, Diffserv, load balancing algorithm.*

1. Introduction

In the FHAMIPv6/MPLS/Diffserv integration[9] case, the FHAMIPv6 protocol [2][3][7][8][9][10] was designed to provide hierarchical addresses in an ad hoc network, but not to provide Quality of Service, as the FHMIPv6 protocol is not designed to be used in ad hoc networks, for this reason this extension version emerged. In order to provide Quality of Service, FHAMIPv6 and MPLS were integrated, (this integration provides End-to-End Quality of Service and allows the adjustment of the IPv6 protocol extension in ad hoc FHAMIPv6 mobile networks), due to the compatibility between IPv6 and MPLS at the headers processing level, decreasing the amount of processing load. In Diffserv´s case, it allows us to segregate End-to-End traffic flows and to provide classification and priority to each traffic, depending on the type of priority assigned in Diffserv. Once these protocols have been integrated and the work is previously done and tested, the Quality of Service degradation in a congested network is evaluated. We have used a load balancing algorithm as a mechanism for limiting the problem of Quality of Service degradation in order to optimize End-to-End traffic or to maintain the minimum Quality of Service requirements for certain traffic by default. The metrics evaluated (Delay, jitter, throughput, loss and send packets) are chosen because they are the most sensitive when a handover or handoff occurs, our tests have been performed in an ad hoc network and in a hybrid network, the Quality of Service metrics have been measured on a handoff in the presence of a congested network so that when the Quality of Service algorithm is used, it allows the problem of network congestion to be neutralized.In another hand, the results obtained in the integration were successfully but the security is not considered. In order to maintain the QoS level, this paper show the biggest problem in the protocols mentioned.

Then, we analyze the QoS safety problems of each protocol detected which can degrade the quality of services.

2. Safety analysis of the FHAMIP / MPLS / Diffserv integration and congestion control algorithm

Security problems of FHAMIPv6 protocol were analyzed in depth by the author of this chapter [5]. In this chapter, the security issue related to FHAMIPv6 protocol will be studied including the way it works and how its message are presented. Subsequently, the safety of ad hoc mobile networks, the security problems they suffer from, and some

Copyright (c) 2014 International Journal of Computer Science Issues. All Rights Reserved.

countermeasures to mitigate the will be studied. Then, some safety issues of the medium access protocol used by FHAMIPv6 will be taken into account, which present some security problems, many of which are also present in FHAMIPv6. We will also consider some ways of compromising security in the FHAMIPv6 by manipulating its diverse messages. Finally the chapter consider some high-risk security issues that are unrelated to the messages used by FHAMIPv6.

A. MPLS Security

Here are some MPLS security-protocol, related works:
Since the protection of the routing information is critical and fundamental to the Ad- hoc mobile networks, in [4] a new approach called MSR (MPLS as secure routing protocol) is proposed, it tries to solve the confidentiality problems of these networks. In similar way in [8] mechanisms to enhance the security of MPLS networks using multipath routing are proposed to eliminate the problems of confidentiality. On the other hand, in [7] secure routing mechanisms in MANET are proposed taking into account QoS considerations, in addition further authentication mechanisms are introduced hop by hop in order to prevent some known attacks on the confidentiality of information .
Then, the MPLS security problems are approached from two perspectives, the problems caused by devices within the MPLS core and the ones caused by internal devices within the core [3]

B. Security issues for devices outside the MPLS core

- Information release: Traffic segregation and the MPLS traffic engineering is based on the label attached to a data packet. If a hacker knows the label used for certain types of traffic he could add it to its packets to receive favorable treatment within the MPLS core.
- Because the MPLS label distribution protocol in general does not use authentication. A hacker could send LDP routing information to MPLS core devices, so he can manipulate the label information base (LIB). This way the hacker could cause a denial of service or a Man-in-the-middle attack. In addition, with the packet injection with labeling information modified, the hacker could make his traffic reach a particular destination through the MPLS network and taking advantage of its QoS characteristics.
- If a MPLS core edge router accepts labeled packets from outside the network, a hacker could label his packets using a combinatorial method so that way he can determine by Brute-force attack which labels are being used by the MPLS core. Such a determination would take place because the edge router will respond differently when receiving a packet with a valid or invalid label.

C. Security issues for devices within the core

The attacks that can be perpetrated from outside the network, can also be performed from inside. In addition to these attacks there are some that can only be performed from within the MPLS core:
- Because the MPLS core has active the routing functions of the non labeled IP traffic, a hacker inside the MPLS core could launch attacks to compromise other devices belonging to the core.
- Although MPLS supports the use of VPNs, it does not provide encryption mechanisms for this type of technology, so a hacker could read details on a VPN tunnel over MPLS if it is placed in the core of the latter, which represents a confidentiality problem.
Because MPLS uses the IP protocol to send control information, all IP vulnerabilities are inherited by it. This may be the biggest MPLS security problem [2].

D. Diffserv

Following, an analysis of the most relevant safety issues concerning Diffserv is presented, some of the vulnerabilities of this protocol will be presented first, followed by an analysis of attacks that may occur in the process of DiffServ configuration and to conclude, an analysis of attacks that may occur in the process of data forwarding.

E. Vulnerabilities

Some of the Diffserv vulnerabilities are presented below [1]:
- Due to the fact that DCSP does not use encryption, a hacker that belongs to the Diffserv core could mark a particular traffic with an invalid or incorrect DSCP to make it receive a Best-effort treatment, in this way the hacker would be causing theft or QoS denial. In a similar way the hacker could highlight its own traffic with a DSCP that allows it to experience a QoS level higher than the contracted. In addition, the hacker could highlight all network traffic to be treated with the highest level of service and to cause a competition between them and the legitimate priority traffic which will deteriorate the QoS of the latter.
- An external hacker can send a large volume of traffic to an edge router to use much of its CPU time and its RAM memory; this would increase the time the router takes to process the legitimate traffic and therefore QoS deterioration.
- If a hacker deliberately removes some packets from a traffic flow, some flow management protocols like TCP, will decrease the transfer rate, since packet loss implies the existence of unavoidable network congestion. In this

Copyright (c) 2014 International Journal of Computer Science Issues. All Rights Reserved.

situation Diffserv cannot maintain a QoS legitimate traffic and it would be greatly affected.
- A hacker in the network Diffserv core could queue some packets randomly chosen and forward the rest by default, it will impress additional jitter to the network traffic which would seriously affect the QoS of applications with strict jitter requirements.
- A hacker might slow packet forwarding evenly using buffers, this way the end-to- end delay of the network increases, affecting the QoS.

F. Attacks on Diffserv configuration process

The attacks that may occur in the process of configuring Diffserv are presented below:
- Packet Injection: a hacker positioned as a configuration authority, can create configuration information packets that cause a too large or too little amount of resources to be reserved. In the first case the hacker achieves a use or consumption of resources, while the second denies resources to the legitimate flow.
- Modification of the packet content: a hacker in the middle of the configuration route may change the amount of resources requested by a user, by modifying a field in the Packet Header configuration. The results of this modification are similar to those of the previous case.
- Packet Delay: a hacker can delay much as he wants the packet forwarding configuration.
- Packet Elimination: a hacker can remove configuration packets so that the network uses an invalid or old configuration, so the new settings will not apply nor the new SLA.

G. Attacks in the Data Forwarding Process

The attacks that may occur in the Data Forwarding process are as follows:
- Injecting packets with an unauthorized DSCP: because the DSCP in Diffserv marks the forwarding differential treatment, theft and denial of service can occur through its handling. For example, the unauthorized use of the DSCP bit can result in deterioration of service across the traffic flow in the same class.
- Modification of service bit: a hacker can modify the header field indicating the service to be received by the packet, so that an EF service packet receives an AF treatment, and an AF packet receives an EF, this way the hacker steals resources for the AF traffic.

H. Congestion Algorithm

A new load balancing routing algorithm for MPLS is presented in [6], however no security considerations are required for the algorithm. Following, the congestion algorithm security used in the proposed integration is analyzed:

Regarding the congestion algorithm the only security issue that was identified, is the following: a hacker located either inside the MPLS core or outside, can send large volumes of traffic to the AMAP using the AN2 as access router at the time that the AMN is in the APAR surrounding area, this will lead the traffic moving in the AMN- > APAR- > AN2 -> AMAP -> AN1 -ACN path (with the segment AN2 > AMAP congested) to be rerouted to the AMN- > APAR- > AN4 -> AMAP -> AN1 -ACN path due to the implementation of the load balancing algorithm. Then the hacker could overload the AN4 -> AMAP segment causing the AMN traffic to be rerouted to the previous route (with no congestion), the systematic implementation of this process will cause the traffic from AMN to be rerouted between one route and another causing impairment to the QoS metrics

References

[1]. 1. Zhi Fu, S. Félix Wu, T.S. Wu, Fengmin Gong y He Huang. Security Issues for Differentiated Service Framework. Internet Draft. Oct. 1999
[2]. 2. Liwen He, Paul Botham, "Pure MPLS Technology," ares, pp.253-259, 2008 Third International Conference on Availability, Reliability and Security, 2008.
[3]. 3. Fischer, T. (2007, Dec). MPLS Security Overview. Retrieved from White Paper for Public Distribution: http://www.ir mplc.com/downloads/whitepapers /MPLS_Security_Overview.pdf
[4]. 4. Qiaolin Hu, Qingyuan Huang, Biao Han, Baokang Zhao, Jinshu Su, "MSR: A Novel MPLS-Like Secure Routing Protocol for Mobile Ad Hoc Networks," nswctc, vol. 1, pp.129-132, 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009
[5]. 5. Ortiz, J., Perea, J., Rodriguez, J. & López, J. (2011). Mobile Ad-hoc: Currents Status and Future Trends. En J. Loo, J. Lloret & J. Ortiz. Security issues in FHAMIPv6. United Kingdom: CRC Chapman, Taylor and Francis.
[6]. 6. Ya-qin Fang, Lin-zhu Wang, "An Algorithm of Static Load Balance Based on Topology for MPLS Traffic Engineering," icie, vol. 2, pp.26-28, 2009 WASE International Conference on Information Engineering, 2009.
[7]. 7. Shahrzad Sedaghat, Fazlollah Adibniya, Vali Derhami, "A Secure Mechanism for QoS Routing in Mobile Ad Hoc Networks with QoS Requirements Consideration," cicn, pp.320-324, 2010 International Conference on Computational Intelligence and Communication Networks, 2010.
[8]. 8. Sahel Alouneh, Abdeslam En-Nouaary, Anjali Agarwal, "Securing MPLS Networks with Multi-path Routing," itng, pp.809-814, International Conference on Information Technology (ITNG'07), 2007
[9]. 9. Jesús Hamilton Ortiz, Bazil Taha Ahmed. Juan p. Pantoja. “FHAMIPv6/MPLS/Diffserv and load balancing

Copyright (c) 2014 International Journal of Computer Science Issues. All Rights Reserved.

algorithm integration". PhD thesis. QoS in MANET networks. 2014, Autonomous Madrid University

[10].Juan P. Pantoja, Jesús Hamilton Ortiz, Bazil Taha, et al., "Performance Analysis of the Proxy Mobile IPv6 (PMIPv6) and Multiprotocol Label Switching (MPLS) Integration", International Journal of Computer Science Issues, Vol. 11, Issue 4, No 2, July 2014.

Copyright (c) 2014 International Journal of Computer Science Issues. All Rights Reserved.