A NOVEL HEADER MATCHING ALGORITHM FOR

INTRUSION DETECTION SYSTEMS

Mohammad A. Alia1,Adnan A. Hnaif1, Hayam K. Al-Anie1, Khulood Abu Maria1,  Ahmed M. Manasrah2, M. Imran Sarwar3

1

Faculty of Science and Information Technology – Al Zaytoonah University of

Jordan, P.O.Box: 130 Amman (11733) Jordan

*dr.m.alia, dr.adnan\_hnaif, drhayam, khulood@alzaytoonah.edu.jo*

2

Al Yarmouk University , Irbed( 21163) – Jordan

*ahmad.a@yu.edu.jo*

3

National Advanced IPv6 - Universiti Sains Malaysia, 11800 Penang, Malaysia

*Imran@nav6.org*

# ABSTRACT

*The evolving necessity of the Internet increases the demand on the bandwidth. Therefore, this demand opens the doors for the hackers’ community to develop new methods and techniques to gain control over networking systems. Hence, the intrusion detection systems (IDS) are insufficient to prevent/detect unauthorized access the network. Network Intrusion Detection System (NIDS) is one example that still suffers from performance degradation due the increase of the link speed in today’s networks. In This paper we proposed a novel algorithm to detect the intruders, who’s trying to gain access to the network using the packets header parameters such as; source/destination address, source/destination port, and protocol without the need to inspect each packet content looking for signatures/patterns. However, the “Packet Header Matching” algorithm enhances the overall speed of the matching process between the incoming packet headers against the rule set. We ran the proposed algorithm to proof the proposed concept in coping with the traffic arrival speeds and the various bandwidth demands. The achieved results were of significant enhancement of the overall performance in terms of detection speed. .*