عنوان مقاله:

Detecting Flooding Attacks on IMS Networks Using Kullback-Leibler Divergence and Triple EWMA

محل انتشار:

فصلنامه پردازش سیگنال و انرژیهای تجدیدپذیر, دوره 1, شماره 4 (سال: 1396)

تعداد صفحات اصل مقاله: 14

نویسندگان:

Noorallah Hemmati Doust - *Department of Electrical Engineering, Shahid Sattary Aeronautical University of Science .and Technology Tehran, Iran*

Mansour Nejati Jahromi - *Department of Electrical Engineering, Shahid Sattary Aeronautical University of Science .and Technology Tehran, Iran*

خلاصه مقاله:

The IP Multimedia Subsystem (IMS) is a platform for the exchange of multimedia communications that was proposed by 3GPP as of the year 2002. The 3GPP proposal called for the integration of mobile cellular networks and internet technology using a completely IP-based structure. The IMS uses the protocols defined by the IETF, such as SIP, RTP and others. SIP is the backbone of the IMS network, where it is used for signaling and multimedia services control. However, security vulnerabilities are inherent in such integration. When the IMS architecture is opened for easy network access and the use of SIP, it is far more vulnerable to SIP flooding attacks. This has presented a significant security problem in new networks. In the presented method for detection, network traffic is captured in two phases, being the training phase and the test phase. The distance between the probable distributions of SIP messages in these two phases is then measured using the Kullback-Leibler divergence. Then, an adaptive threshold is defined for the Kullback-Leibler divergence which, when passed, means that an attack has occurred. The adaptive threshold is accounted for by the use of a Triple Exponential Moving Average (TEMA), and the performance of the presented detection method in various situations of normal traffic and massive attacks is evaluated. The parameters α, β, ε, and γ are used for estimating the threshold and setting a safe margin for authorized traffic. In addition, the effect of .changes of the estimate and setting parameters is evaluated

کلمات کلیدی:

IP Multimedia, flooding attack, adaptive