۱۲:۵۹ ب.ظ پنجشنبه, ۳ آذر ۱۴۰۱

رویکرد تطبیق پذیر با تنوع ترافیکی شبکه‌های پهن باند برای شناسایی حملات منع خدمت توزیع شده

روش‌های شناسایی و مقابله با حملات DDOS، ترافیک را از سه منظر بررسی می‌کنند(ترافیک را از سه منظر مشاهده می‌کردند) و سعی در مقابله دارند:

- بسته : یعنی جلوی یک بسته مثلاً HTTP را می‌گیرند.
- جریان: یهنی جلوی یک جریان که مثلاً سایزش بیش از ۱۰۰ کیلوبایت بود را می‌گیرند.
- رفتار کاربر: اگر رفتار ترافیک کاربری نامتعارف بود، جلوی آن را می‌گیرد. مثلاً در یک دقیقه، بیش از ۱۰ درخواست به منابع مختلف یک سایت ارسال کند

و در هر یک ازمنظرها طبق اطلاعاتی که به دست می‌اوردند، بر اساس روش‌هایی زیر، ترافیک نامتعارف را تشخیص می‌دهند :

- روشهای آماری
- استفاده از یادگیری ماشین
- مبتنی بر مدل و تشخیص آنومالی (بی‌نظمی)

اما این روش‌ها(۳ روش اولی) مشکلشان این بود که با تنوع پروتکلی اپلیکیشن‌های مختلف، سازگار نبودند و باعث بروز خطا می‌شدند. در واقع ترافیک برای هر اپلیکیشن می‌تواند الگوی مختلفی داشته باشد و برای هر کاربردی نمی‌توان یک الگو، مرز و شناسه برای حالت متعارف آن تعریف نمود. برای حل این مشکل به شناسایی اپلیکیشن‌های مختلف می پردازند ،که از روش‌های مثل dpi یا یادگیری ماشین استفاده می‌شود و سپس با استفاده از اطلاعات آنها ترافیک را دسته بندی کرده و در هر کدام برای تشخیص الگوهای نامتعارف، تنظیمات متفاوتی(مثل مقادیر آستانه متفاوت برای حجم بسته‌ها) به کار می‌برند.
اما در شبکه‌های پهن باند با مشکلی به نام تنوع ترافیکی بالا مواجه هستیم واز طرفی با توجه به استریمینگ ترافیک بایستی در کمترین زمان ممکن، کم هزینه‌ترین راهکار را ارایه دهیم. راهکارهای مبتنی بر یادگیری ماشین و استفاده از DPI، سربار محاسباتی زیاد دارند.