مکانیزم های تشخیص نفوذ در شبکه (SNIDS)

مریم فرجی بیرگانی، ناصر نعمت بخش

گروه کامپیوتر، دانشگاه غیرانتفاعی شهید اشرفی اصفهانی، اصفهان، ایران، **Tiamo1394@gmail.com**
استادیار، گروه کامپیوتر، دانشگاه غیرانتفاعی شهیداشرفی اصفهانی، اصفهان،ایران، **Nemat@ashrafi.ac.ir**

این مقاله طبق مجوز شماره ۹۳/۱۷/۸۰۵ مرکز منطقه ای اطلاع رسانی علوم و فناوری RICeST زیر نظر وزارت علوم، تحقیقات و فناوری در آن مرکز نمایه و منتشر شده است.

چکیده

امروزه بسیاری از فعالیت هایی که انجام می شود وابسته به سرویس هایی است که توسط شبکه های کامپیوتری ارائه می شود. بنابراین سیستم های تشخیص نفوذ به طور قابل ملاحظه ای برای افزایش امنیت شبکه های کامپیوتری مورد استفاده قرار میگیرند. برای این منظور لازم است که عوامل بروز حمله در شبکه مشخص شوند. یکی از عوامل بروز حمله در شبکه، آسیب پذیریهایی هستند که در سرویسها وجود دارند. یکی از راه های ایمن سازی شبکه تشخیص نفوذ است. اگرچه سیستم های تشخیص نفوذ بی عیب و نقص نمی باشند، اما یک جزء مهم در تشکیل دیوارهای دفاعی سیستم های اطلاعاتی و شناسایی حملات است. در این مقاله با ترکیب سیستم‌های تشخیص نفوذ با شبکه اجتماعی معماری جدیدی ارایه شده، که در آن برای سیستمهای تشخیص نفوذ در بستر شبکه اجتماعی امکان اشتراک دانش فراهم شده است. این سیستم از یک دیدگاه در رسته سیستمهای توزیع شده قرار می‌گیرد. اما به لحاظ عملکردی کاملا با آنها متفاوت می باشد. عمده‌ترین تفاوت آن در نحوه کسب دانشهای جدید است.

واژه های کلیدی

دیواره آتش، تشخیص نفوذ، شبکه اجتماعی، سیستم‌های توزیع شده، امنیت شبکه

1- مقدمه

با ورود همه جانبه اینترنت به زندگی بشریت و در اختیار گذاشتن منابع، اهمیت ایمن سازی شبکه بیشتر از پیش احساس می شود. علاوه بر این موضوع سیستم هایی باید وجود داشته باشند که منابع موجود را بین کاربران براساس نیازشان تقسیم بندی کنند. کلاس بندی یکی از راه حل های این مسِله است. کلاس بندی در اکثر مراجع به سه دسته تقسیم می شوند.

روش های تک ویژگی (SFC)[1]: در این روش در هر بسته فقط یکی از اطلاعات موجود در سرآیند بسته مورد استفاده قرار میگیرد، در کاربرد های مسیریابی مورد استفاده قرار می گیرد.

روش های چند ویژگی (MFC)[2]: در این روش هر بسته به بیشتر از یکی از اطلاعات موجود در سرآیند توجه میشود. این نوع کلاسبندی در کاربردهای امنیتی از قبیل دیوار آتش مورد استفاده قرار می گیرد.

روش های کلاسبندی عمیق (DPC)[3]: در این روش کل سرآیندها بسته مهم است و تعداد ویژگی های استخراج شده از این روش معمولا زیاد است. این روش در امنیت شبکه و مدیریت منابع مورد استفاده قرار میگرد.

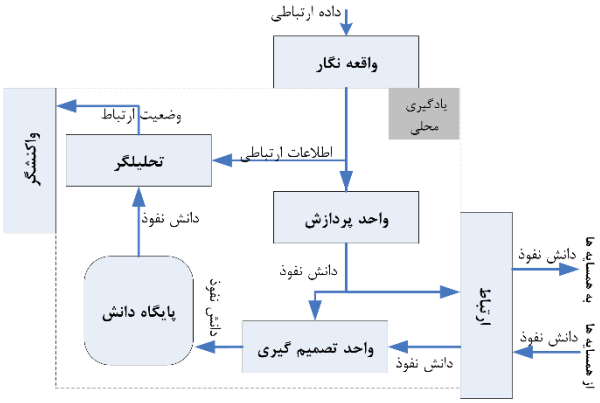
در یک دسته بندی کلی، می توان سیستمهای تشخیص نفوذ را به سیستمهای متمرکز و توزیع شده تقسیم بندی نمود. در سیستمهای متمرکز تمام اجزای سیستم تشخیص نفوذ به صورت یکجا و بر روی یک رسانه در شبکه فعالیت می کنند. اما در سیستمهای توزیع شده با هدف افزایش ضریب ایمنی، تحمل پذیر آسیب و توزیع بار ترافیکی شبکه تمام یا برخی از اجزای سیستم تشخیص نفوذ مانند حسگرها، واقعه نگار و یا حتی جزء تحلیلگر بر روی ناحیه های مختلف یک شبکه یا چندین شبکه متفاوت توزیع می شوند.

۲- سیستم پیشنهادی

یکی از روشهای نوین اشتراک دانش، استفاده از الگوی شبکه‌های اجتماعی است. چنانکه از نام سیستم SNIDS نیز برمی آید، سیستمی است مبتنی بر شبکه اجتماعی و ماهیت عملکردی آن یک روش مبتنی بر همکاری می باشد. در ادامه به تشریح اجزای سیستم و روابط بین آنها می پردازیم.

۲-۱. گره (سیستم تشخیص نفوذ)

در شکل (۱) که یک نمای شماتیک توسعه داده شده از سیستم تشخیص نفوذ است. اجزای لازم برای هر گره نمایش داده شده است. از آنجا که اجزای کلی بین تمام سیستمهای تشخیص نفوذ مشابه می باشند، صرفا به تشریح بخشهای موثر در سیستم پیشنهادی می پردازیم.



شکل ۱: اجزای سیستم تشخیص نفوذ به عنوان یک گره در شبکه اجتماعی

[1] Single field Classification
[2] Multi field classification
[3] Quality of service