عنوان مقاله:

آگاهی وضعیتی حملات منع سرویس توزیع شده براساس پیش بینی (تجسم آینده نزدیک) صحنه نبرد مبتنی بر نظریه شواهد دمپستر-شافر و بیزین

محل انتشار:

فصلنامه پدافند الکترونیکی و سایبری, دوره 7, شماره 1 (سال: 1398)

تعداد صفحات اصل مقاله: 18

نویسندگان:

حمید اکبری - *دانشجوی دکتری، دانشگاه جامع امام حسین (ع)*

سید مصطفی صفوی همامی - *دانشیار، دانشگاه صنعتی امیرکبیر*

رضوان خاندانی - *دانش آموخته دانشگاه خوارزمی*

خلاصه مقاله:

صحنه نبرد سایبری در حملات منع خدمت‌رسانی توزیع شده دارای دو بازیگر مهاجم و مدافع (قربانی) است که مهاجم با گسیل بسته‌های پی درپی و تغییر روش های خود درصدد قطع یا کاهش خدمت رسانی قربانی است و قربانی با انجام انواع تمهیدات امنیتی درصدد دفاع بوده و اصرار بر خدمت رسانی به ذینفعان خود دارد. ارزیابی این صحنه از منظر یک ناظر می‌تواند دارای ابهام باشد به‌طوریکه قادر باشد ادامه این صحنه را پیش‌بینی نمایید. در این پژوهش انواع وضعیت های مهاجم و مدافع و سپس معیارهای خبرگی در قالب مهارت، قابلیت تداوم حمله یا دفاع، تسریع در عکس‌العمل نشان دادن حمله یا دفاع و درنهایت قابلیت دسترس پذیری خدمات تبیین شده است. در ادامه با استفاده از یک مجموعه داده 3003 تایی که حاوی دنباله وضعیت های یک مهاجم و مدافع است، معیارهای فوق اندازه-گیری شده و نتایج این تحقیق نشان داد که نیمی از داده‌ها دارای طول زمانی کوتاه حمله هستند که این بیانگر بهره‌مندی از اصل غافل-گیری است و یا اینکه قربانی‌ها برای دفاع در برابر حمله، هیچ گونه آمادگی ندارند. همچنین همبستگی معیارها نسبت به یکدیگر نشان داد که هر چه زمان حمله طولانی باشد خسارت مدافع بیشتر می‌گردد و محاسبات به نفع مهاجم رقم می‌خورد. همچنین امکانات و تجهیزات در سرعت عمل مهاجم تاثیر مثبتی ندارد و بلکه قدری هم تاثیر منفی دارد و این بدان معناست که مهارت مهاجم نسبت تجهیزات او اثرگذارتر است. در ادامه به منظور تجسم صحنه نبرد در پیش‌بینی وضعیت طرفین تجسم‌های قابلیت چهارگانه تبیین گردید و سپس با استفاده از نظریه شواهد دمپستر- شافر، تجسم‌های فوق، ادغام شده تا بتوانند پیش بینی وضعیت اثر حمله بر قربانی را تخمین بزنند. همچنین در ادامه، تجسم قابلیت روش و تمهید با استفاده از قوانین بیزین تبیین گردید تا بتواند وضعیت آتی روش مهاجم و تمهید امنیتی مدافع را پیش بینی کند. با اجرای پنج سناریو در چهار گام زمانی، نشان داده شد که تخمین‌های حاصل شده با بیش از 65 درصد قابل باور هستند.

کلمات کلیدی:

حملات منع خدمت توزیع شده, بات نت, آگاهی وضعیت, خبرگی, نظریه دمپستر- شافر, تجسم آینده

لینک ثابت مقاله در پایگاه سیویلیکا: