عنوان مقاله:
ارایه یک روش بهبود یافته جرم یابی دیجیتال مبتنی بر ادغام اطلاعات

محل انتشار:
دومین کنفرانس ملی مهندسی برق و کامپیوتر (سال: 1396)

تعداد صفحات اصل مقاله: 9

نویسندگان:
هانیه تفکری بافقی - *گروه امنیت اطلاعات، مجتمع ICT، دانشگاه صنعتی مالک اشتر، تهران، ایران*

علی جبار رشیدی - *دانشیار گروه مخابرات، دانشگاه صنعتی مالک اشتر، تهران، ایران*

خلاصه مقاله:
جرم یابی دیجیتال شامل نظارت بر ترافیک شبکه و تعیین وجود یا عدم وجود ناهنجاری در ترافیک است و ثابت می کند که آیا نشانی از حمله موجود است یا خیر! اگر حمله تشخیص داده شود سپس ماهیت این حمله نیز مشخص می گردد. تکنیک های جرم یابی شبکه، محققان را قادر به پیگیری مهاجمان می کند. هدف نهایی از جرم یابی قانونی دیجیتال آن است که شواهد کافی ارایه شود برای اینکه مجوز داده شود تا متهم تحت پیگرد قرار گیرد [1] .هدف نهایی این است که شواهد کافی برای صدور مجوز فراهم شود تا از این طریق متهم تحت پیگرد قرار گیرد.این فرآیند در ابتدا مستلزم شناسایی و جمع آوری اطلاعات در مورد حمله و صحت آن است. سپس با ترکیب اطلاعات درست با استفاده از الگوریتم آپریوری می توان به تجزیه وتحلیل حمله پرداخت و خروجی الگوریتم توسط ادغام مبتنی بر تصمیم ارزیابی می گردد. این مسیله به بهبود آگاهی وضعیتی کمک می کند . خروجی این مسیله شامل درک دقیقی از نقاط ضعف و آسیب پذیری هایی است که وقوع حمله را ممکن می سازند . این اطلاعات به مدیران امنیتی جهت پیکربندی سیستم ها کمک می کند تا از وقوع حوادث مشابه در آینده جلوگیری کنند.

کلمات کلیدی:
جرم یابی دیجیتال، ادغام اطلاعات ، الگوریتم آپریوری، حملات سایبری