پایان‌نامه‌ی کارشناسی ارشد: پریسا دایی حسنی، ۱۳۹۶

تشخیص حمله سیبیل در شبکه تجارت الکترونیکی با رویکرد خوشه بندی و مدیریت اعتماد

تجارت الکترونیک یک صنعت رو به رشد است که به دلیل مزیت‌های آن، شرکت‌های زیادی رویکردهای کسب وکاری خود را بر مبنای آن قرار داده‌اند. اما اعتماد متقابل بین فروشنده و خریدار و به ویژه شهرت فروشنده مساله مهمی در حوزه تجارت الکترونیک محسوب می‌شود. برنامه‌های تجارت الکترونیک نظیربه‌نظیر (P2P) در برابر حملات فعال و غیرفعال، بسیار آسیب پذیرند. این حملات، افراد و شرکت‌های تجاری بالقوه را با هدف کسب بهترین منفعت در تجارت الکترونیک با زیان‌های حداقل از میدان خارج کرده‌اند. این حملات زمانی که یک تراکنش اتفاق می‌افتد، در تعاملات میان نظیرهای تجاری رخ می‌دهد. حمله سیبیل یکی از مهم‌ترین حمله‌ها در محیط تجارت الکترونیک است که در آن نظیرها هویت‌های ساختگی و جعلی و چندین هویت می‌توانند داشته باشند. اکثر کارهای تحقیقاتی موجود که بر شبکه‌های اجتماعی و گواهینامه‌های مورد اعتماد تمرکز دارند، قادر به پیشگیری از نظیرهای حملات سیبیل نسبت به انجام تراکنش‌ها نبوده‌اند. در این پایان‌نامه ما راهکاری برای شناسایی و مقابله با حملات سیبیل پیشنهاد می‌کنیم. راهکار پیشنهادی با استفاده ازمکانیزم خوشه‌بندی و اعتماد شباهت، به تشخیص و مقابله با مهاجمان سیبیل می‌پردازد. روش پیشنهادی ما با روش‌های EigenTrust، SybilTrust و EigenGroupTrust مقایسه شده‌است. تجزیه و تحلیل عملکرد و امنیت نشان می‌دهد که حملات سیبیل به‌وسیله اعتماد شباهت پیشنهادی ما می‌تواند به حداقل رسانده شوند.

اولین آزمایش با هدف محاسبه‌ی درصد کشف نودهای مخرب انجام شد که شاهد عملکرد بالای روش پیشنهادی خود نسبت به سایر روش‌ها بودیم. در این آزمایش تعداد نظیرهای مخرب را از 10 تا 40 درصد افزایش دادیم و نرخ تشخیص مهاجمان سیبیل را با استفاده از شبیه سازی بدست آوردیم. مطابق این آزمایش، زمانی که تعداد نظایر مخرب افزایش می یابد نرخ هشدارهای اشتباه، افزایش می‌یابد و نرخ تشخیص مهاجمان سیبیل کاهش می‌یابد.

سپس دومین آزمایش با هدف تایین مقدار بهینه آستانه‌ی thd انجام شده است که مطابق این آزمایش بهترین نرخ تشخیص زمانی است که thd = 0.6می‌باشد که تقریبا 90% مهاجمان تشخیص داده می‌شوند. زیرا زمانی که مقدار thd بیشتر از 0.6 باشد، نرخ هشدارهای اشتباه در حال افزایش می‌باشد. پس بایستی مقدار thd را به نحوی انتخاب کنیم که سخت‌گیری را کاهش دهد و چنانچه مقدار thd کمتر از 0.6 باشد، تعداد زیادی از نودهای مهاجم تشخیص داده نمی‌شوند. پس بایستی مقدار thd را طوری تایین کنیم که محاسبات منطقی‌تری حاصل گردد.

کلمات کلیدی: حمله سیبیل، تجارت الکترونیکی، اعتماد، شبکه‌های نظیر به نظیر

کلیدواژه‌ها: کلمات کلیدی: حمله سیبیل، تجارت الکترونیکی، اعتماد، شبکه های نظیر به نظیر

شماره‌ی پایان‌نامه: ۱۲۷۴۱۰۰۶۹۵۲۰۰۷
تاریخ دفاع: ۱۳۹۶/۰۶/۰۵
رشته‌ی تحصیلی: مهندسی کامپیوتر- نرم افزار
دانشکده: فنی و مهندسی
استاد راهنما: دکتر حسن شاکری
استاد مشاور: مهندس یاسر علمی سولا

M.A. Thesis:

Sybil Attack Detection in E-Commerce Network Based on Clustering and Trust Management

Abstract
E-commerce is a giant industry which numerous corporations have put their business procedures based on it due to its benefits. But mutual trust among seller and buyer and specially seller reputation is considered as a vital issue in the area of e-commerce. P2P E-commerce programs are very vulnerable against active and passive attacks. These attacks have taken the potential individuals and commercial corporations out competition field with the aim to acquire maximum benefit and minimum loss in e-commerce. When a transaction occurs, these attacks takes place at interactions among commercial peers. The Sybil attack is one of most important attacks in e-commerce environment where peers could have false and forged multiple identities. Most available research works which focus on the trusted certificates and social networks, arent able to prevent the Sybil attacks peers from performing transactions. So in the thesis, we suggest a solution for recognizing and overcoming Sybil attacks. The suggested solution detects and overcomes Sybil attacks using clustering mechanism and similarity trust. Our suggested method have been compared to Sybil Trust, Eigen Trust, Eigen Group Trust mechanisms. Finally, the analysis of performance and security indicates that Sybil attacks could be minimized through our suggested similarity trust.
:The first test was performed in order to calculate the recognition percentage of malicious nodes which we saw higher performance of our suggested method than other methods. In this test, we increased the number of Sybil peers from 10 to 40 percent and obtained the recognition rate of Sybil attackers through simulation. Based on this test, as the number of Sybil peers increases, the false alarm rate will increase and the rate of Sybil attacker detection will decrease.
Then second test has been performed to determine the optimal value of thd, So that the best detection rate occurs when thd =0.6 which 90% attackers have been detected. Because as thd value is greater than 0.6, then the false alarm rate is increasing. Therefore, we select thd value such that will reduce the rigidity and if thd value is lower than 0.6 , high numbers of attacker nodes will not be detected therefore we determine thd value such that more logical calculations will be achieved.

:Keywords
Sybil attack, e-commerce, trust, P2P networks.