



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 و کاری خود را بر مبنای آن قرار داده اند. اما اعتماد متقابل بین فروشنده و خریدار و به ویژه شهرت فروشنده مساله مهمی در حوزه تجارت الکترونیک محسوب می‌شود. برنامه‌های تجارت الکترونیک نظیر به نظیر (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 کرده اند. 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 نبوده اند. در این پایان‌نامه ما راهکاری برای شناسایی و مقابله با حملات سیبیل پیشنهاد می‌کنیم. راهکار پیشنهادی با استفاده از مکانیزم خوشه‌بندی و اعتماد شباهت، به تشخیص و مقابله با مهاجمان سیبیل می‌پردازد. روش پیشنهادی ما با روش‌های SybilTrust، EigenTrust و EigenGroupTrust مقایسه شده است. تجزیه و تحلیل عملکرد و امنیت نشان می‌دهد که حملات سیبیل به وسیله اعتماد شباهت پیشنهادی ما می‌تواند به حداقل رسانده شوند.

کلیدواژه‌ها: کلمات کلیدی: حمله سیبیل، تجارت الکترونیکی، اعتماد، شبکه‌های 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.

Keywords:

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