چکیده

امروزه امنیت شبکه و مقابله با حملات گوناگون موجود در شبکه مورد بررسی پژوهشگران زیادی قرار گرفته , با این حال هنوز حملات امنیت شبکه را تهدید می‌کنند، یکی از این نوع حملات حمله، انکار سرویس[1] (DOS) و نسخه توزیع شده آن[2](DDoS) است، این نوع حمله‌ها تلاش می‌کنند تا با تخلیهٔ سیستم یا منابع شبکه، مانع از دردسترس قرار گرفتن سرویس‌های شبکه برای کاربران درخواست کننده شوند.

در این تحقیق امنیت شبکه را در برابر حملات DDoS و روش‌های مقابله با این نوع حملات را تا حدودی مورد بررسی قرار داده ایم, با شناخت از چگونگی حملات DDoS و استفاده این حملات از نقاط ضعف شبکه، یک مکانیزم شبکهٔ امنیتی نرم افزار محور[3](SDSNM) را جهت حذف یا محدود کردن شرایط ضروری خلاصه شده از این بررسی، بیان کرده و در ادامه یک نمونهٔ اولیه از SDSNM را از طریق شبیه‌ساز مینی‌نت[4] پیاده‌سازی می‌کنیم. برای حل مسائل مربوط به مدیریت پیچیده، تعمیم پذیری و پایداری، از اِعمال فناوری‌های شبکه نرم افزار محور[5] ، کورد[6] و رایانش ابری می‌توان استفاده کرد.

آزمایش‌های مبتنی بر نمونه‌های اولیه نشان می‌دهد که این مکانیزم جدید، امکان‌پذیر بوده و در صورت استفاده از سیاست‌گذاری‌های کنترل دستیابی سختگیرانه، حملات DDoS نمی‌توانند به اجرا درآیند در عوض، زمانی که از سیاست‌های کنترل دستیابی ضعیف استفاده کنیم، مکان و موقعیت مهاجم و میزبان‌ها در بات‌نت[7]، که مجموعه از کامپیوترهایی است که توسط هکر کنترل می‌شوند، شناسایی و مشخص می‌شود.

1 Denial Of Service (DOS)
2 Distributed Denial Of Service (DDoS)
3 .Software defined security networking mechanism to defend against DDoS Attacks (SDSNM)
4 .Mininet
5 Software Defined Network (SDN)
6 .Chord
7 .Botnet