استراتژی چند سطحی به عنوان راهکاری مؤثر جهت کاهش پیچیدگی تحلیل رمزنگارهای قالبی

محسن شکیبا[1]، محمد دخیل‌علیان[2]

[1] دانشجوی دوره تحصیلات تکمیلی ، دانشگاه صنعتی اصفهان
اصفهان، ایران
mshakiba_1360@yahoo.com
[2] استادیار گروه مخابرات ، دانشگاه صنعتی اصفهان
اصفهان، ایران
mdalian@yahoo.com

چکیده

در رمزنگارهای قالبی و بر اساس آنالیز خطی و تفاضلی رمزنگار، طرح حمله به طور معمول به این ترتیب است که مسیری با بیشترین ضعف (متناسب با نوع حمله) یافت می شود و سپس حمله از طریق آن صورت می گیرد. به این ترتیب پیچیدگی حمله به صورت تابعی از تعداد متنهای اصلی و رمز شده معلوم – که خود وابسته به قدرت مشخصه یافت شده است – و نیز هزینه هر بار آنالیز روی هر یک از آنها قابل بیان است. همچنین آنچه در نهایت حاصل خواهد شد بسته به نوع حمله، بازیابی بخشی از کلید دور نهایی و یا دورهای پیش از آن خواهد بود. هر چند پذیرش حمله ای که با بیشترین توان (کمترین پیچیدگی) قادر به بازیابی بخش‌هایی از کلید باشد به عنوان نمایش دهنده توان مشخصه یافت شده قابل قبول است اما طبیعی است که در یک حمله عمیق، حمله ای موفقتر ارزیابی خواهد شد که با پیچیدگی کمتر در بازیابی کامل کلید دور این امر را محقق سازد. این موضوع یعنی بررسی پیچیدگی به صورت کلی و نه با بررسی تنها یک مشخصه قوی، نقطه مورد نظر در این مقاله است و فرآیند آن در مقابل حمله صرفا متکی به یک مشخصه قوی (یک سطحی)، حمله با استراتژی چند سطحی نامیده شده است.

با بررسی صورت گرفته این نکته استنباط شد که حملات بهتر از منظر پیچیدگی محاسباتی، حملاتی نیستند که حتی الزاما شامل بهترین مشخصه باشند و در بسیاری موارد می توان با انتخاب مشخصه‌های ضعیفتر اما با استراتژی مناسبتر و چند سطحی به پیچیدگی کلی کمتری دست یافت. جهت اثبات این موضوع آنچه مورد بررسی قرار گرفت آنالیز خطی روی یک شبکه SPN نوعی، ۱۶ بیتی با ۴ دور بود که ضمن برخورداری از ساختاری ساده، دارای تمامی اجزای اساسی یک رمزنگار مرسوم نیز هست. در نهایت در چند سطح موفق به یافتن استراتژی‌هایی جهت اعمال حمله کامل به ساختار فوق شدیم که به مراتب دارای پیچیدگی کمتر نسبت به حملات صرفا متکی به مشخصه‌های قوی هستند و این دلیلی بر صحت موضوع مطرح شده در بالا خواهد بود.

کلمات کلیدی

آنالیز خطی، شبکه SPN، مشخصه خطی، بهینه سازی، پیچیدگی محاسباتی .

۱- مقدمه

واضح است که نخستین مرحله از طرح یک حمله دلخواه روی یک رمزنگار قالبی شامل یافتن مشخصه و یا به عبارتی دیگر نقطه ضعفی متناسب با نوع حمله است که این مرحله در بسیاری موارد قابل تبدیل به یک مسأله بهینه سازی

استراتژی چند سطحی به عنوان راهکاری مؤثر جهت کاهش پیچیدگی تحلیل رمزنگارهای قالبی

محسن شکیبا[1]، محمد دخیل‌علیان[2]

[1] دانشجوی دوره تحصیلات تکمیلی ، دانشگاه صنعتی اصفهان
اصفهان، ایران
mshakiba_1360@yahoo.com
[2] استادیار گروه مخابرات ، دانشگاه صنعتی اصفهان
اصفهان، ایران
mdalian@yahoo.com

چکیده

در رمزنگارهای قالبی و بر اساس آنالیز خطی و تفاضلی رمزنگار، طرح حمله به طور معمول به این ترتیب است که مسیری با بیشترین ضعف (متناسب با نوع حمله) یافت می شود و سپس حمله از طریق آن صورت می گیرد. به این ترتیب پیچیدگی حمله به صورت تابعی از تعداد متنهای اصلی و رمز شده معلوم – که خود وابسته به قدرت مشخصه یافت شده است – و نیز هزینه هر بار آنالیز روی هر یک از آنها قابل بیان است. همچنین آنچه در نهایت حاصل خواهد شد بسته به نوع حمله، بازیابی بخشی از کلید دور نهایی و یا دورهای پیش از آن خواهد بود. هر چند پذیرش حمله ای که با بیشترین توان (کمترین پیچیدگی) قادر به بازیابی بخش‌هایی از کلید باشد به عنوان نمایش دهنده توان مشخصه یافت شده قابل قبول است اما طبیعی است که در یک حمله عمیق، حمله ای موفقتر ارزیابی خواهد شد که با پیچیدگی کمتر در بازیابی کامل کلید دور این امر را محقق سازد. این موضوع یعنی بررسی پیچیدگی به صورت کلی و نه با بررسی تنها یک مشخصه قوی، نقطه مورد نظر در این مقاله است و فرآیند آن در مقابل حمله صرفا متکی به یک مشخصه قوی (یک سطحی)، حمله با استراتژی چند سطحی نامیده شده است.

با بررسی صورت گرفته این نکته استنباط شد که حملات بهتر از منظر پیچیدگی محاسباتی، حملاتی نیستند که حتی الزاما شامل بهترین مشخصه باشند و در بسیاری موارد می توان با انتخاب مشخصه‌های ضعیفتر اما با استراتژی مناسبتر و چند سطحی به پیچیدگی کلی کمتری دست یافت. جهت اثبات این موضوع آنچه مورد بررسی قرار گرفت آنالیز خطی روی یک شبکه SPN نوعی، ۱۶ بیتی با ۴ دور بود که ضمن برخورداری از ساختاری ساده، دارای تمامی اجزای اساسی یک رمزنگار مرسوم نیز هست. در نهایت در چند سطح موفق به یافتن استراتژی‌هایی جهت اعمال حمله کامل به ساختار فوق شدیم که به مراتب دارای پیچیدگی کمتر نسبت به حملات صرفا متکی به مشخصه‌های قوی هستند و این دلیلی بر صحت موضوع مطرح شده در بالا خواهد بود.

کلمات کلیدی

آنالیز خطی، شبکه SPN، مشخصه خطی، بهینه سازی، پیچیدگی محاسباتی .

۱- مقدمه

واضح است که نخستین مرحله از طرح یک حمله دلخواه روی یک رمزنگار قالبی شامل یافتن مشخصه و یا به عبارتی دیگر نقطه ضعفی متناسب با نوع حمله است که این مرحله در بسیاری موارد قابل تبدیل به یک مسأله بهینه سازی