وارسی ویژگی های زمانی پروتکل های امنیتی با رویکرد منطق زمانی PS-LTL

سعید جلیلی سید مهدی سجادی

گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه تربیت مدرس

m_sajjadi@modares.ac.ir sjalili@modares.ac.ir

چکیده: در این مقاله، مدل تحلیل صحت و آسیب پذیری *Analyze* به گونه ای گسترش داده شده است که بتوان ویژگی های وابسته به زمان را نیز توصیف و وارسی کرد. در مدل گسترش یافته، فرایند تحلیل صحت و آسیب پذیری در دو فاز و شش مرحله انجام می شود. در فاز اول قدم های یک پروتکل به صورت یک مجموعه قواعد، توصیف شده و آنگاه ویژگی های صحت این پروتکل وارسی می شود. در فاز دوم برای توصیف ویژگی های زمانی، از منطق زمانی *PS-LTL* استفاده می شود و برای وارسی این ویژگی ها قدم های پروتکل به دستگاه حل محدودیت بهبود یافته نگاشت می شود و سپس ویژگی های امنیتی وابسته به زمان با روش حل محدودیت، وارسی می گردد. به عنوان نمونه، پروتکل توافق کلید *EKE* در مدل گسترش یافته وارسی شده و یک حمله نشست موازی برای آن اثبات شده است.

واژه های کلیدی: پروتکل های امنیتی، تحلیل صحت، تحلیل آسیب پذیری، منطق زمانی $PS-LTL$، روش حل محدودیت

۱- مقدمه

روش های توصیف و وارسی رسمی عموما برای تحلیل و ارزیابی صحت عملکرد سیستم هایی استفاده می شود که میزان اطمینان بالایی از نحوه عملکرد آنها مورد انتظار است. روش های وارسی رسمی به دو رویکرد متفاوت اثبات قضیه و بررسی مدل قابل تقسیم است.

پروتکل ها قوانینی هستند که محاوره بین عوامل مرتبط را امکان پذیر می کنند. برای ایجاد امنیت در سیستم های توزیع شده نسبت به نوع خطرات و حملاتی که سیستم را تهدید می کند از سرویس های امنیتی مختلفی استفاده می شود. عمده این سرویس ها در قالب پروتکل های امنیتی تحقق یافته اند.

در طراحی پروتکل های امنیتی همواره دو نگرانی وجود دارد. اول اینکه بدون در نظر گرفتن نفوذی آیا پروتکل طراحی شده در نهایت سرویس های امنیتی مورد نظر را به صورت صحیح ارائه می کند؟ نگرانی دوم از این بابت است که با فرض وجود عوامل نفوذی به همراه قابلیت های ارتباطی و محاسباتی در بستر اجرای پروتکل آیا تمهیدات در نظر گرفته شده، امنیت پروتکل را تامین می کند؟ بر این اساس روش های تحلیل رسمی پروتکل ها را از لحاظ هدف تحلیل به دو رویکرد تحلیل صحت و تحلیل آسیب پذیری دسته بندی می کنیم.

کاربرد ابزار های منطقی در تحلیل پروتکل های امنیتی توسط *Burrow* و همکارانش با مطرح کردن منطق *BAN* شروع شده است [۱]. این منطق برای استنتاج راجع به پروتکل های احراز اصالت طراحی شده است و دارای مشکلات متعددی است از جمله این که به طور مستقیم دارای مولفه زمانی نیست و لذا با آن نمی توان عبارت « اگر یک پیام دریافت شده باشد، آنگاه این پیام در لحظه ای در گذشته فرستاده شده است» را توصیف نمود [۲].

اولین تلاش برای ورود مولفه زمان در *BAN* توسط *Syverson* صورت گرفت [۲]. از سوی دیگر در [۳] با نوعی منطق انشعابی ساده، در [۴] با استفاده از منطق زمانی TLA[1]، به توصیف ویژگی ها و وارسی پروتکل های امنیتی

[1] Temporal Logic of Action