

عنوان مقاله:

انالیز رسمی پروتکل DLMS با استفاده از AVISPA

محل انتشار:

ششمین کنفرانس بین المللی اقتصاد، مدیریت و علوم مهندسی (سال: 1394)

تعداد صفحات اصل مقاله: 18

نویسنده:

امین ساتیاروند - دانشجوی کارشناسی ارشد، دانشگاه شهید رجایی

خلاصه مقاله:

استفاده از روش های رسمی به عنوان یک تکنیک مفید و کارآمد برای اعتبار سنجی خواص امنیتی پروتکلها در نظر گرفته میشود. در این مقاله، ما امنیت پروتکل DLMS را با استفاده از یک ابزار تجزیه و تحلیل خودکار به نام AVISPA بررسی میکنیم. تجزیه و تحلیل ما از این استاندارد با استفاده از back-end CL-AtSe ، OFMC از AVISPA نشان می دهد که پروتکل های دو حزبی در برابر خواص امنیتی مشخص شده امن هستند. در حالی که back-end ها قادر به پیدا کردن حملات علیه پروتکل های احراز هویت یک طرفه و متقابل دارای party سوم مورد اعتماد هستند.

کلمات کلیدی:

تبادل کلید، سومین party/احراز هویت، ابزار AVISPA/پروتکل

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/480872>

