عنوان مقاله:
آنالیز رسمی پروتکل DLMS با استفاده ازAVISPA

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

تعداد صفحات اصل مقاله: 18

نویسنده:
امین ساتیاروند -

خلاصه مقاله:
استفاده از روش های رسمی به عنوان یک تکنیک مفید و کارآمد برای اعتبارسنجی خواص امنیتی پروتکلها در نظر گرفته میشود. در این مقاله، ما امنیت پروتکلDLMSرا با استفاده از یک ابزار تجزیه و تحلیل خودکار به نامAVISPAبررسی میکنیم. تجزیه و تحلیل ما ازاین استاندارد با استفاده ازOFMC back-end , CL-AtSe ازAVISPA نشان می دهد که پروتکلهای دو حزبی در برابر خواص امنیتی مشخص شده امن هستند. در حالی کهback-end ها قادر به پیدا کردن حملات علیه پروتکل های احراز هویت یک طرفه و متقابل دارایparty سوم مورد اعتماد هستند.

کلمات کلیدی:
تبادل کلید، سومینparty/احراز هویت، ابزارAVISPA/پروتکل

لینک ثابت مقاله در پایگاه سیویلیکا: