مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۱، بهار ۱۳۹۵، ص ۱۷- ۹

پروتکل دست‌دهی ۴- مرحله‌ای امن و کارآمد برای مقابله با حمله DoS در شبکه هوشمند انرژی

محمدحسن انصاری [*۱]، وحید طباطباوکیلی [۲]، محمد گوهریی [۳]

۱- دانشجوی دکتری، دانشگاه علم و صنعت ایران
۲- استاد، دانشگاه علم و صنعت ایران
۳- کارشناسی ارشد، دانشگاه صنعتی مالک اشتر

(دریافت: ۹۳/۱۰/۲۷، پذیرش: ۹۵/۰۲/۱۴)

چکیده

شبکه‌های مخابراتی توزیع‌شده ارتباط مخابراتی را در حوزه‌های مختلف شبکه هوشمند انرژی همچون ناحیه خانگی، شبکه ناحیه همسایگان و ناحیه تولید محلی / پست‌ها با هزینه مناسب فراهم می‌کنند. این مقاله با توجه به چالش‌های امنیتی موجود در پروتکل دست-دهی و تبادل کلید این نوع شبکه‌ها، یک طرح توزیع و به‌روزرسانی دینامیک کلید را برای افزایش امنیت شبکه در برابر حملات مهاجمان ارائه می‌کند. طرح پیشنهادی از دو پروتکل امنیتی شناخته‌شده احراز اصالت هم‌زمان برابر و مشارکت امن حلقه کارآمد استفاده می‌کند. ازآنجایی‌که هر دو پروتکل از تبادل ۴-راهه استفاده می‌کنند، در این مقاله دو طرح تبادل بر پایه توابع یک‌سویه و عدم وابستگی بین مراحل پروتکل پیشنهاد شده است که مقاومت شبکه در برابر حمله انکار سرویس به‌صورت کامل بهبود می‌دهد و درعین‌حال با توجه به محاسبه پیچیدگی مخابراتی و حافظه ازنظر سربار تحمیل‌شده به شبکه نیز بهینه است. سرانجام با توسعه مدل حمله DoS، امنیت طرح پیشنهادی با شبیه‌سازی گسترده به‌وسیله Avispa ارزیابی و اثبات شده است.

واژه‌های کلیدی: شبکه هوشمند انرژی، امنیت، تبادل کلید، دست‌دهی، توابع یک‌سویه.

۱- مقدمه

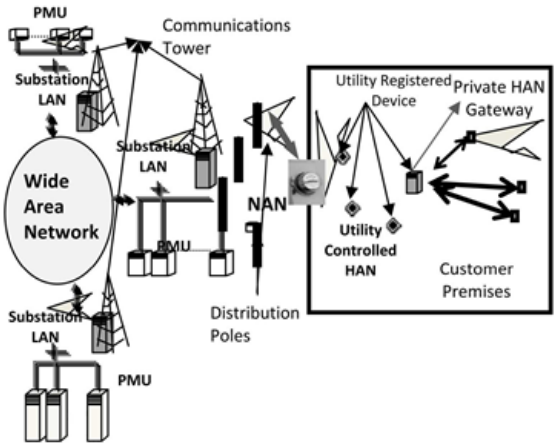
در حوزه‌های مختلف شبکه هوشمند یک زیرساخت مشخص و یکپارچه وجود ندارد، بنابراین شبکه‌های WLAN[1] به‌عنوان یک گزینه مناسب می‌تواند در بسترهای مختلف این شبکه‌ها استفاده شود [۱]. شکل (۱) پیاده‌سازی WLAN در محدوده‌های مختلف شبکه هوشمند شامل شبکه ناحیه خانگی (HAN[2])، شبکه ناحیه همسایه (NAN[3]) و شبکه ناحیه پست (SAN[4]) را نشان می‌دهد. برای بهبود ناحیه پوشش این شبکه‌ها و غلبه بر محدودیت‌های محدوده مخابراتی، از توسعه آن‌ها به شبکه‌های مش استفاده می‌شود [۲]. شبکه ناحیه همسایه، یک شبکه مش چند دروازه‌ای بر پایه استاندارد IEEE802.11s است [۳]. شکل (۱) همچنین یک مثال از شبکه ناحیه پست را نشان می‌دهد. این شبکه شامل تعدادی واحد اندازه‌گیری فاز (PMU[5]) است که برای هم‌زمانی دقت بالا با کنترل‌کننده داده فازور واقع در دروازه‌های متصل به پشت شبکه در حال ارتباط مخابراتی می‌باشند. هر PMU به یک GPS مجهز است و بسته‌ها از طریق PDC محلی با تأخیر پایین به مقصد نهایی برای ذخیره‌سازی، پایش یا کنترل ارسال می‌شوند.

ازآنجایی‌که در غیاب هر سیستم سیمی یا زیرساخت بی‌سیم فنّاوری WLAN یک پرشه ممکن است به‌عنوان یک راه حل مناسب در نظر گرفته شود که توسعه مش آن قابلیت اعتماد شبکه را افزایش و قابلیت عملیاتی آن را ارتقاء می‌دهد. شبکه‌های مش جنبه‌های منحصربه‌فرد مختلفی، همچون خودسازمان‌ده بودن را ارائه و تجهیزات جدید (مانند اندازه‌گیر و PMU) نیز می‌توانند در ساختار موجود مشارکت داشته باشد. علاوه بر این، سهولت نصب، مقیاس‌پذیری و خوددرمانی نیز از جنبه‌های مهم این نوع شبکه‌ها است. با وجود این مزایا، عیب اصلی شبکه مش

* رایانامه نویسنده مسئول: mh_ansari@elec.iust.ac.ir

1- Wireless Local Area Network
2- Home Area Network
3- Neighbor Area Network
4- Substation Area Network
5- Power Measurment Unit

چندپرشه مستعد و آسیب‌پذیر بودن در مقابل حملات مختلف به دلیل ارسال بسته‌های داده به‌صورت پرش به پرش است [۴]؛ بنابراین امنیت شبکه‌های مش یک چالش اساسی در مخابرات بی‌سیم می‌باشد. علاوه بر این، شبکه‌های مش به دلیل فقدان زیرساخت، نیازمند رهیافت توزیع‌شده برای احراز اصالت نقاط مش (MP) می‌باشند.



شکل (۱). کاربرد WLAN در نواحی مختلف شبکه هوشمند انرژی [۱۲]

تاکنون، کارهای زیادی بر روی پروتکل امنیت شبکه‌های مش انجام‌شده و آسیب‌پذیری‌های مختلف شبکه در برابر حملات بررسی شده است [۶-۳]. همچنین برای انطباق و بهره‌برداری از شبکه‌های محلی IEEE802.11 به‌صورت مش، اخیراً استاندارد IEEE802.11s برای شبکه‌های مش ارائه شده است. این استاندارد احراز اصالت هم‌زمان یکسان (SAE) را به‌صورت پیش‌فرض به‌عنوان پروتکل امنیتی پشتیبانی می‌کند. پروتکل SAE بر پایه گذرواژه به اشتراک گذاشته‌شده بین همه گره‌های شبکه می‌باشد [۳]. در این روش با وجود این‌که مهاجم از طریق شنود قادر به تعیین گذرواژه نیست، اما افشای گذرواژه به گره‌های غیرمجاز اجازه الحاق آن‌ها به شبکه را می‌دهد؛ بنابراین محرمانگی و یکپارچگی شبکه نقض می‌شود. رهیافت متناظر SAE پروتکل مشارکت امنیت مش کارآمد (EMSA) است. پروتکل EMSA با استفاده از سلسه مراتب کلید مش قادر به ایجاد لینک امن بین دو MP در شبکه بی‌سیم مش است. در هر دو پروتکل یک دست‌به‌دست شدن ۴- سویه استفاده شده است، بنابراین، شبکه می‌تواند در برابر حمله DoS آسیب‌پذیر باشد. علاوه براین، از طریق شنود، مهاجم می‌تواند تبادل ۴- سویه را به‌وسیله جعل پیام حفاظت نشده-۱ یا پیام ناقص-۳ که یک MP از احراز اصالت کننده (MA) دریافت می‌کند، قطع کند. برای افزایش حفاظت شبکه در برابر چنین حملاتی، در این مقاله یک استراتژی توزیع و تازه شدن دوره‌ای برای افزایش امنیت در برابر حمله‌DoS پیشنهاد شده است؛ بنابراین در اینجا هدف توسعه یک طرح حفاظت تبادل ۴- سویه کارآمد است. طرح پیشنهادی قادر به بهبود امنیت شبکه‌های مش برای پیاده‌سازی در حوزه‌های مختلف شبکه هوشمند انرژی است. مقاله به‌صورت ذیل سازمان‌دهی شده است: در بخش ۲ بعد از مرور پروتکل‌های SAE و EMSA، پیاده‌سازی SAE و EMSA با استفاده از شبکه‌های مش چند دروازه‌ای بیان می‌شود. در بخش سوم روش تازه شدن دوره‌ای کلیدها ارائه می‌شود. در بخش ۴، مدل حمله DoS در خلال فرایند تبادل ۴- سویه ارائه می‌شود و پروتکل پیشنهادی برای حفاظت شبکه در مقابل این حمله تشریح می‌شود. سرانجام در بخش ۵ نتایج شبیه‌سازی ارائه و کارایی و امنیت پروتکل اثبات می‌شود. در انتها نتیجه‌گیری حاصل از کار در بخش ۶ ارائه می‌شود.

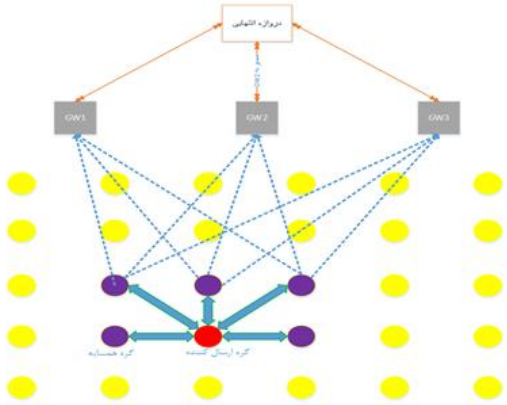
۲- امنیت سیستم‌های مش

امنیت شبکه مش بر پایه قابلیت حفاظت یکپارچگی پیام در برابر حملات بداندیشانه استوار است [۳]. این نیازمندی محرمانگی و احراز اصالت تبادل بسته‌های داده را تضمین و با استفاده از مشارکت باقابلیت اطمینان بالا و فرآیند احراز اصالت از دسترسی مهاجم به شبکه برای اختلال در شبکه به‌وسیله تولید پیام‌های جعلی جلوگیری می‌کند. به‌عنوان مثال در حمله حفره سیاه گره مهاجم با دستکاری کردن مسیریابی و جلوگیری از رسیدن بسته‌ها به مقصد موردنظر می‌تواند با ارسال پیام جعلی مسیریابی همه بسته‌ها را به‌طرف خودش منحرف و شبکه را مختل کند. در این مقاله به‌منظور ایجاد عملکرد امن در یک مسیر طولانی، رهیافتی که قادر به تغییر دینامیکی اطلاعات کلید به‌صورت دوره‌ای و /یا در شرایط وجود حمله فعال آشکارشده، توسعه داده شده است. در این بخش ابتدا توصیف خلاصه‌ای از پروتکل‌های امنیتی مش استاندارد EMSA و SAE ارائه می‌شود.

۲-۱- پروتکل EMSA برای شبکه‌های چند دروازه‌ای

پروتکل EMSA بر پایه ایجاد لینک امن کارآمد از طریق استفاده از سلسله مراتب چکیده ساز کلید بین دو MP در شبکه مش بی‌سیم می‌باشد. در اینجا شبکه مش چند دروازه‌ای که برای NAN توسعه داده شده است، استفاده می‌شود [۷]. شکل (۲) معماری شبکه شامل چندین دروازه را نشان می‌دهد که هر گره مش (مثل ابزارهای اندازه‌گیری) می‌تواند از طریق مسیریاب‌های جداگانه به هر دروازه دسترسی داشته باشد. رهیافت مسیریابی درختی که توسعه‌ای از پروتکل مش بی‌سیم ترکیبی (HWMP) استاندارد IEEE802.11s می باشد برای پیاده‌سازی این شبکه استفاده شده است. همان‌طور که در شکل (۲) نشان داده شده است، هر دروازه (GW-1,GW-2,...) در ریشه یک درخت به‌صورت دوره‌ای آگهی ریشه را برای ایجاد درخت خود پخش

می‌کند. همه دروازه‌ها نیز از طریق دروازه اصلی به‌صورت بی‌سیم به پشت شبکه متصل می‌باشند. در اینجا فرض شده است که دروازه اصلی به‌عنوان یک احراز اصالت کننده مش (MA) به‌علاوه توزیع‌کننده کلید مش (MKD) عمل می‌کند. در حالت کلی MKD کلیدها را برای ایجاد سلسه مراتب کلید مش استنتاج می‌کند. در شبکه، دروازه‌های اصلی مسئول ایجاد و توزیع کلیدهای سلسله مراتبی مش به دروازه‌های محلی و درنتیجه به همه نقاط مش بعد از هر مرحله فرآیند احراز اصالت می‌باشند. به‌عبارت‌دیگر دروازه‌های اصلی همه اطلاعات احراز اصالت MP ها را ذخیره می‌کنند. علاوه براین، پروتکلEMSA شامل ایجاد لینک همتا طبق زیرساختEAP و تبادل ۴-سویه، برای استنتاج کلید بین هر زوج گره مش در شبکه است. در پروتکل EMSA بعد از تبادل کلید مش، درخواست دهنده احراز اصالت یک احراز اصالت کننده مش می‌باشد. درواقع ابتدا قابلیت‌های EMSA از طریق بیکن و فریم‌های پاسخ با استفاده از مقدار نشانگر حوزه MKD اعلان می‌شود. در احراز اصالت اولیه EMSA، یک MP اجتماع امنیتی باMA را انجام و یک سلسله مراتب کلید را برای لینک‌های امن آینده که شامل تبادل ارتباط بین یک MP و MA است، فراهم می‌کند. MP درخواست‌کننده، یک فریم درخواست اجتماع شامل لینک همتا Open IE و درخواست MKDD-IE را برای ایجاد سلسله مراتب کلید صادر می‌کند.MP انتظار دریافت یک فریم پاسخ اجتماع شامل شناسه تائید لینک همتا و اطلاعات استخراج کلید برای ایجاد لینک امن را دارد. در انتها اگر احراز اصالت 802.1X نیاز باشد، توسط تبادل ۴- سویه انجام می‌شود.



شکل (۲). معماری شبکه هوشمند چند دروازه‌ای

در این فرآیند، قبل از احرازاصالت EMSA هر دروازه (به‌عنوان درخواست دهنده) از طریق فریم‌های درخواست و پاسخ با دروازه اصلی اجتماع را شروع می کند که شامل تبادل بازبودن لینک همتا و اطلاعات تایید لینک همتا می‌باشد. به‌محض این‌که ایجاد لینک با موفقیت انجام شد، دروازه اصلی فرآیند احراز را شروع می‌کند. تحت IEEE 802.1X که EAP را برروی شبکه‌های LAN تعریف می‌کند، پیام‌های EAP بین درخواست‌کننده و احراز اصالت‌کننده (دروازه اصلی) تبادل می‌شود، سپس پیام‌هایEAP از درخواست دهنده به سرور احرازاصالت رله می‌شود. به‌محض احرازاصالت موفق، دروازه اصلی و دروازه درخواست‌دهنده یک تبادل ۴- سویه را شروع می‌کنند که حاصل آن استخراج PTK (زوج کلید گذرا) برای ارتباطات تک پخشی و GTK (کلید گذرای گروهی) برای ارتباطات چندپخشی می‌باشد. بعد از تبادل ۴- سویه، MP درخواست‌دهنده قادر به دریافت آگهی مسیر از احراز اصالت‌دهنده مش و در نتیجه مسیر امن به توزیع‌کننده کلید مش (دروازه اصلی) را دارا می‌باشند. قبل از این‌که MP درخواست‌دهنده خودش یک احراز اصالت‌کننده شود، مجموعه دیگری از کلیدهای سلسله مراتبی مورد نیاز از طریق تبادل کلید نگهداری شده امن ایجاد می‌شود. این کلید، به‌عنوان PTK-KD شناخته می‌شود و از KDK (کلید توزیع کلید) برای ارتباط بین گره درخواست‌دهنده (دروازه) و دروازه اصلی استخراج می‌شود. از این کلید برای کلیه ارتباطات بین احرازاصالت‌کننده مش و توزیع‌کننده کلید مش (دروازه اصلی) هنگامیکه درخواست‌کننده به احرازاصالت‌کننده مش تبدیل می شود، استفاده شده است. در ادامه دروازه درخواست‌کننده احرازاصالت جدید فرآیند احرازاصالت را برای یکی از گره های انتخاب شده در مسیر درخت شروع می‌کند. اگر گره MP قبلاً توسط MP همسایه دیگری احرازاصالت شده باشد، فرآیند احرازاصالت تنها شامل ایجاد لینک همتا با تبادل ۴- سویه بدون نیاز به احرازاصالت EAPOL می‌باشد که این فرآیند به‌عنوان احرازاصالت ثانویه شناخته می‌شود [۸]. فرآیند ایجاد لینک و احرازاصالت تا زمانی‌که هر گره فرآیندهای PTK ، GTK و PTK-KD را در تمام مسیر درخت برآورده نکند، ادامه می‌یابد.

۲-۲-پروتکلSAE برای شبکه‌های چند دروازه‌ای

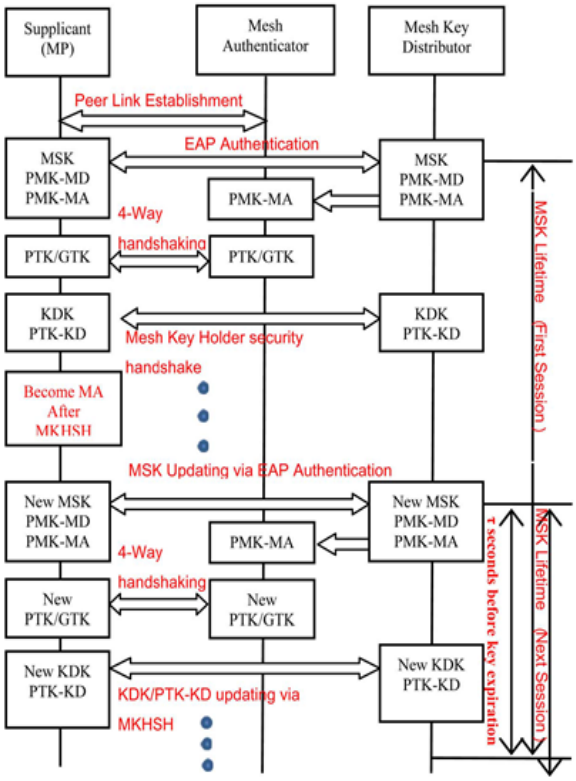
در SAE کلمه عبور به اشتراک گذاشته‌شده به‌وسیله همه MPها برای احراز اصالت یکدیگر استفاده می‌شود. در اینجا، بخش‌های درگیر به‌صورت MP-A و MP-B تعریف و توسط آدرسMAC شناسایی می‌شوند. پس از تشخیص درخواست ارتباط از طریق پایش غیرفعال بیکن‌ها یا جستجوی فعال، MPها پروتکل SAE را اجرا می‌کنند. قبل از تبادل پیام‌ها، PWE بر پایه گذرواژه اشتراک گذاشته شده و آدرس‌های MAC بخش‌های درگیر تولید می‌شود. پس از تولید PWE ، دو عدد تصادفی بنام rand و mask تولید و به همراه PWE برای کامل کردن احراز اصالت SAE استفاده می‌شوند. به‌محض موفق بودن احراز اصالت SAE هر دو MP-A و MP-B یک PMK (زوج کلید اصلی) تولید و در تبادل ۴- سویه برای تولید PTK و GTK از آن استفاده می‌کنند. در شبکه چند دروازه‌ای، هر زوج MP احراز اصالت SAE را بعد از تشخیص

دیگری انجام و کلیدهای PMK را تولید می‌کنند. سیاست امنیتی در رویه اجتماع بر پایه کلیدهای PMK و در یک تبادل ۴- سویه انجام برای تولید PTK و GTK انجام می‌شود.

۳- طرح تازه کردن دوره‌ای کلید

در این طرح مواد کلید در بازه‌های منظم به‌روزرسانی می‌شوند. در ابتدای احراز اصالت EAP یا SAE و تبادل ۴- سویه به‌روزرسانی برای استخراج یک مجموعه کلیدهای جدید قبل از ابطال مواد کلید موجود، انجام می‌شود. برای مثال در EMSA طول عمر کلید توزیع‌کننده و KDK نباید از طول عمر MSK بیشتر باشد. علاوه براین طول عمر PTK وPMK-MA باید با PMK-MKD یکسان باشند. به‌صورت مشابه، طول عمر PTK-KD باید همانند KDK باشد. به‌محض این‌که، طول عمر کلید تمام شود، هر نگه‌دارنده کلید، کلیدهای مشتق شده متناظر را حذف می‌کند. در SEA نیز وضعیت مشابه رخ می‌دهد، در این حالت طول عمر $PMK\text{-}R_0$، $PMK\text{-}R_1$ و PTK بر مبنای طول عمر MPMK اصلی که از آن مشتق شده است محدود است. در هر دو حالت، به‌محض اتمام فرآیند، طول عمر کلیدهای متناظر با عملگر MA به پایان می‌رسد و تنها بعد از فرآیند امنیتی موفقیت‌آمیز ادامه خواهد یافت. این شرایط حتی اگر چرخه عمر ماده کلید کوتاه باشد، منجر به اختلال در عملکرد شبکه می‌شود؛ بنابراین اگر کلیدها برای یک بازه طولانی بدون تغییر باقی بماند، شبکه در برابر حملات مهاجمان آسیب‌پذیرتر می‌شود؛ بنابراین، برای عملکرد امن شبکه در بازه زمان طولانی، در اینجا یک طرح به‌روزرسانی که قادر به تغییر دینامیک اطلاعات کلید به‌صورت دوره‌ای و/یا در وضعیتی که مهاجم فعال آشکارشده است می‌باشد، توسعه داده شده است.

در طرح پیشنهادی، در غیاب هر طرح آشکارسازی قابل‌اعتماد، سیستم می‌تواند به‌صورت پیوسته مواد کلیدها را به‌روزرسانی کند و درنتیجه احتمال قطعی شبکه در اثر حملات را حذف می‌کند. تحت این شرایط، همه مواد کلید همراه با MSK به‌صورت دوره‌ای به‌روزرسانی می‌شود. برای EMSA، همه MS، MSK را به همراه MKD از طریق احراز اصالت EAP تازه می‌کند که در شکل (۳) نشان داده شده است. در حالت کلی به‌روزرسانی ممکن است در بازه‌های زمانی معین انجام شود؛ بنابراین، در خلال هر زمان، طول عمر MSK نیز به نشست MSK ارجاع داده می‌شود، بنابراین به‌روزرسانی PTK/GTK می‌تواند قبل از اتمام طول عمر MSK انجام و منجر به تولید PTK/GTK جدید از طریق تبادل ۴- سویه شود. برای پروتکل SAE نیز رویه مشابهی انجام می‌شود که در شکل (۴) نشان داده شده است.

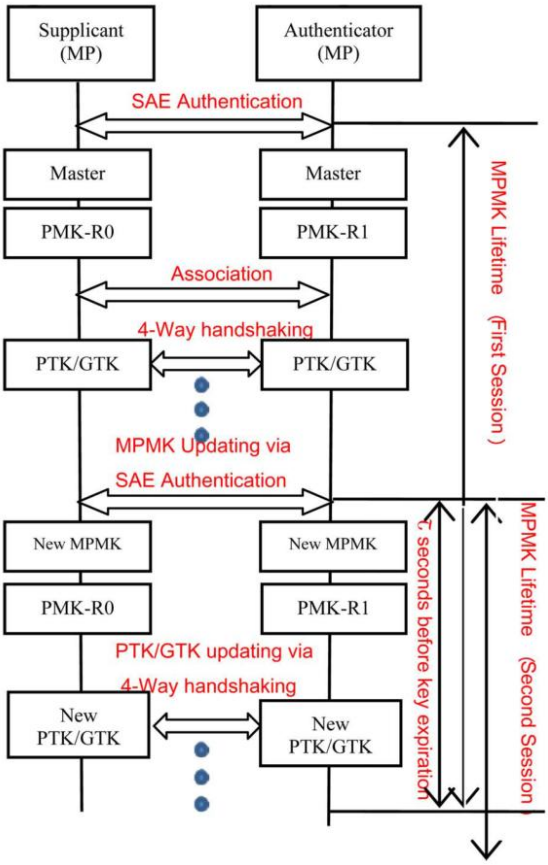


شکل (۳). طرح به‌روزرسانی کلید در پروتکل EMSA [۴]

۳-۱- بهبود امنیتی تبادل ۴- سویه

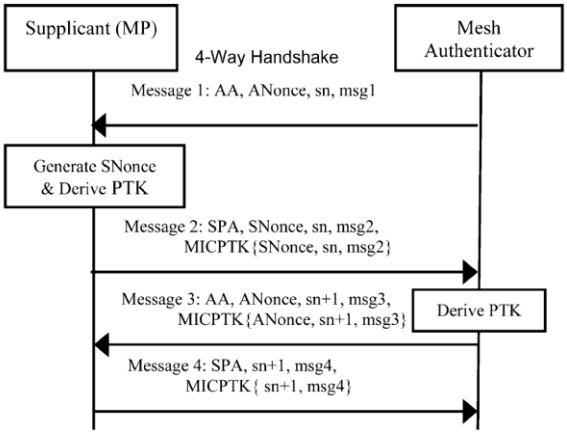
حفاظت محرمانگی و یکپارچگی بسته داده تبادل شده نیازمند طراحی فرآیند احراز اصالت و اجتماع باقابلیت اطمینان بالا برای جلوگیری از تولید پیام‌های جعلی توسط مهاجم ضروری است، بطوریکه در خلال عملکرد شبکه فرآیند ۴- سویه قابل تفسیر می‌باشد. برای مثال همان‌طور که در شکل (۳ و ۴) نشان داده شده است، بعد از به‌دست آوردن PMK-MA (در EMSA) یا PMK-R0 و $PMK\text{-}R_1$ (درSAE) MA و درخواست‌دهنده یک تبادل ۴- سویه را شروع می‌کند که منطقی است. اگر فرض کنیم که کلید PM (استنتاج شده از احراز اصالت SAE یا احراز اصالت EAP) تنها به‌عنوان احرازاصالت‌کننده یا درخواست‌کننده شناخته می‌شود.

بنابراین انتظار می‌رود که حملات به‌دلیل رمزنگاری لایه لینک داده تنها قبل از تولید اولین PTK امکان‌پذیر باشند. پس حفاظت PTK در همه زمان‌ها اهمیت حیاتی دارد به‌گونه‌ای که تقریباً شکستن توابع رمزنگاری به‌جز در حالتی‌که یکپارچگی PTK نقض شود، غیرممکن است.



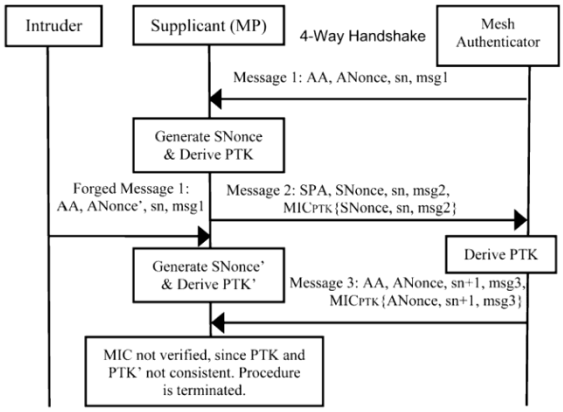
شکل (۴). طرح به‌روزرسانی دوره‌ای کلید در پروتکل SAE [۴]

برای دسترسی به این حالت، در مدل، فرض شده است که مهاجم حمله DoS را در خلال تبادل ۴- سویه به‌منظور جلوگیری از دسترسی احراز اصالت کننده و درخواست‌کننده به کلید انجام دهد. فرض شده است که مهاجم قادر به جعل آدرس MAC سایر MPها، شنود و نیز جعل پیام‌های دریافت شده است. شکل (۵) پیام‌های چکیده‌ای را که در تبادل ۴- سویه تبادل می‌شوند را نشان می‌دهد. در این شکل SPA، AA، Snoce و Anoce بیانگر آدرس MAC و Nonce درخواست‌دهنده و احراز اصالت کننده است، sn دنباله اعداد و MICptk{} بیانگر کد یکپارچگی پیام محاسبه‌شده برای محتوای درون براکت با PTK تازه می‌باشد. به نظر می‌رسد در حالت شبکه با زیرساخت امنیتی IEEE802.11i که در تبادل ۴- سویه مشارکت دارند، قابلیت‌های امنیتی، احراز اصالت و کلید رمزنگاری انتخابی از طریق عناصر اطلاعات RSNE پخش می‌شود. در این حالت همواره برای مهاجمان دست‌کاری پیام رمز نشده به‌راحتی امکان‌پذیر است. مطابق شکل (۶) در فرآیند تبادل ۴- سویه به‌محض این‌که درخواست‌کننده پیام ۱ را دریافت کند، برای تولید پیام نیازمند اطلاعات تولید پیام پاسخ است.



شکل (۵). رویه دست دهی ۴- سویه در استاندارد IEEE802.11s [۴]

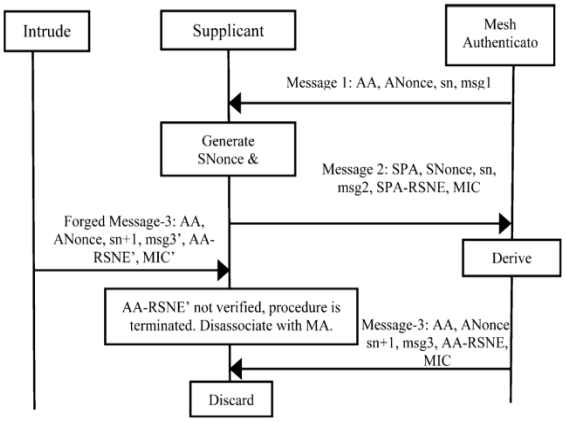
بنابراین درخواست‌کننده، پیام ۲ را به‌وسیله محاسبه MIC بر روی کل پیام ۲ محافظت می‌کند. این فرآیند به MA اجازه آشکارسازی دست‌کاری پیام ۲ را می‌دهد؛ بنابراین ازآنجایی‌که پیام ۱ به‌وسیله MIC محافظت نشده است، مهاجم قادر به تخریب تبادل ۴- سویه به‌وسیله جعل آن است. برای روشن شدن موضوع، نحوه پیاده‌سازی حمله DoS با استفاده از این ضعف در شکل (۶) نشان داده‌شده است.



شکل (۶). پیاده‌سازی حمله DoS با استفاده از آسیب‌پذیری پیام ۱ در فرآیند دست‌دهی ۴- سویه استاندارد [۹]

در این حمله مهاجم پیام ۱ ارسالی از احراز اصالت کننده را شنود و بعد از پیام ۲ یک پیام جعلی ۱ با ANonce جدید برای درخواست‌کننده ارسال می‌کند. نتیجتاً درخواست‌کننده بعد از دریافت پیام جعلی ۱ یک PTK جدید را تولید می‌کند که با PTK احراز اصالت کننده در تناقض است، بنابراین این رخداد سبب خاتمه یافتن فرآیند احراز اصالت و ابطال می‌شود. یک راه‌حل مقابله با این حمله ذخیره دو PTK لحظه‌ای (TPTK) و یک PTK در درخواست‌کننده است. در این حالت زمانی که پیام ۱ دریافت شود به‌روزرسانی می‌شود، درحالی‌که PTK تنها به‌محض دریافت پیام ۳ با MIC معتبر به‌روزرسانی می‌شود. این

روش برای دفاع در برابر حمله DoS زمانی که MIC در پیام ۳ به‌وسیله دو TPTK یا PTK تائید اعتبار شود، کارآمد است. بااین‌وجود، مهاجم هنوز می‌تواند حمله را به‌وسیله یک حمله DoS چند پیامی انجام دهد و پیام‌های جعلی با Nonce های متفاوت را به درخواست‌کننده ارسال کند. در این حالت، درخواست‌کننده می‌تواند همه Nonce های دریافتیTPTK ها را ذخیره کند، بطوریکه تبادل ۴-سویه با احراز اصالت کننده قانونی کامل شود؛ اما این حمله DoS چند پیامی می‌تواند منابع حافظه را تلف کند و اگر مهاجم تعداد زیادی پیام ۱ جعلی را به درخواست‌کننده ارسال کند، سبب تأخیر زیادی در شبکه شود. توجه شود که علاوه بر پیام ۱، مهاجم می‌تواند حمله DoS را با استفاده از پیام ۳ انجام دهد. در حالت کلی در فرآیند دست دهی، بعد از دریافت پیام ۳، درخواست‌کننده عنصر شبکه امن قوی (RNSE) را به‌وسیله مقایسه باRSNE قبلی دریافت شده (هر یک از بیکن یا فریم پاسخ جستجو) تصدیق می‌کند [۷]. اگر دو RSNEیکسان نباشد، درخواست‌کننده تبادل-4 سویه را متوقف می‌کند. همان‌طور که در شکل (۷) نشان داده‌شده است، مهاجم می‌تواند به‌وسیله جعل پیام 3 با AARSNE ، MSG3 وMIC جعلی حمله را بر روی پیام 3 انجام دهد.



شکل (۷). پیاده‌سازی حمله DoS با استفاده از آسیب‌پذیری پیام ۳ در فرآیند دست دهی ۴- سویه استاندارد [۹]

مشاهده می‌شود که این فرآیند برای مهاجمی کهAA، Anonce و sn+1 صحیح را استخراج و آنگاهAARSNE را تصدیق می‌کند. ازآنجایی‌کهRSNE جعلی نمی‌تواند با مقدار دریافت شده قبلی منطبق باشد، درخواست‌کننده از تبادل ۴- سویه صرف‌نظر و ارتباط خود را با MA قطع می‌کند؛ اما در این روش نیز پیام 1 احراز اصالت شده هنوز در برابر حمله پاسخ آسیب‌پذیر است. روش مقابله دیگری که پیشنهادشده است، استفاده از یک زوج شمارنده هم‌زمان‌شده برای اجتناب از حمله پاسخ می‌باشد [۹]. گرچه جزییات روش پیشنهادی در [۱۰] ارائه نشده است، متأسفانه طراحی و پیاده‌سازی شمارنده‌های هم‌زمان شده، به‌ویژه در محیط بی‌سیم سربار مخابراتی را به‌شدت افزایش می‌دهد. در این مقاله، به‌عنوان قابل اعتمادترین راه‌حل، یک روش درهم‌ساز سلسله مراتبی برای حفاظت پیام ۱ و پیام ۳ پیشنهادشده است. برای این منظور، MA از تابع درهم‌ساز یک‌راهه SHA-1 برای احراز اصالت امن استفاده می‌کند.

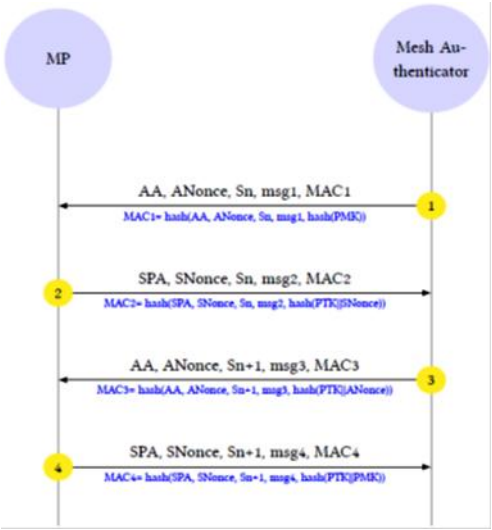
۴- طرح پیشنهادی

در روش‌های دست دهی یکی از مهم‌ترین ضعف‌های امکان حمله DoS است. این حمله به دلیل امکان تغییر در پیام‌های تبادلی در مراحل ۱و ۳ قابل پیاده‌سازی است، به‌گونه‌ای که با تغییر در هر یک از مراحل کاربر در مقایسه‌ای که در مرحله ۳ انجام می‌دهد به تناقض می‌رسد و با تکرار آن امکان حمله DoSفراهم می‌شود. به دلیل ارسال پیام‌ها به‌صورت واضح در روش دست دهی، مهاجم با استراق سمع می‌تواند به آن‌ها دست‌یافته و با تغییر آن‌ها حمله را پیاده‌سازی کند. درواقع به دلیل فقدان یکپارچگی امکان پیاده‌سازی این حملات وجود دارد. حالت ساده برای تأمین یکپارچگی استفاده از MAC مبتنی بر توابع درهم‌ساز است. در این حالت به دلیل دسترسی مهاجم به پیام‌های تبادلی و تولید مقدار چکیده متناظر امکان پیاده‌سازی حمله DoS وجود دارد.

$$X=hash(A,B,C) \qquad (۱)$$

بنابراین برای جلوگیری از حمله DoS باید پیام X به مقداری که در تبادل انتقال نمی‌یابد ولی طرفین به آن دسترسی دارند وابسته کرد. در پروتکل پیشنهادی توابع درهم‌ساز به مقدار کلید توافقی PMK در روند احراز اصالت وابسته می‌شود. در پروتکل ابتدا کاربر و شبکه یک روند احراز اصالت مبتنی بر EAP را پیاده‌سازی و در نهایت طرفین به یک کلید که انتقال نمی‌یابد، دست می‌یابند؛ بنابراین یکپارچگی پیام به یک مقدار ارسال نشده وابسته می‌شود. در این شرایط اگر مهاجم در هریک از مراحل ۱ و ۳ تغییری را ایجاد کند، به دلیل عدم دسترسی به مقدار یکپارچگی پیام قادر به جعل پیام نیست.

در ساختار پیشنهادی از توابع درهم‌ساز وابسته MAC_i استفاده‌شده است، علاوه براین برای کاهش پیچیدگی و سربار به‌جای توابع رمزنگاری در رویه دست دهی ۴- سویه استاندارد از توابع درهم‌ساز استفاده شده است. ساختار و جریان پیام‌های ارسالی در پروتکل دست‌دهی امن پیشنهادی بر پایه توابع درهم‌ساز وابسته در شکل (۸) نشان داده شده است.



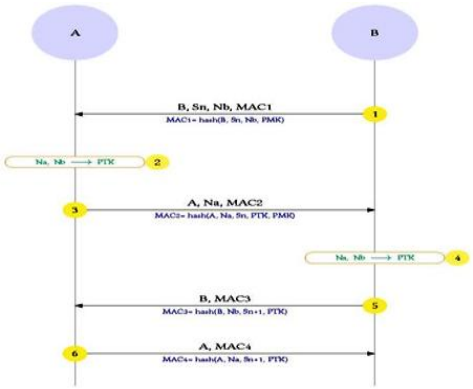
شکل (۸). پروتکل دست دهی امن پیشنهادی با استفاده از توابع درهم‌ساز وابسته

پروتکل پیشنهادی دارای ویژگی یکپارچگی وابسته می‌باشد و با این ویژگی قادر به مقابله با حمله DoS مبتنی بر تغییر پیام است. علاوه‌بر این در فرآیند دست‌دهی از رمزنگاری استفاده نشده و به‌جای آن از توابع درهم‌ساز وابسته به کلید استفاده شده است، بنابراین سربار مخابراتی و محاسباتی کاهش می‌یابد. در حالت کلی، در بررسی عملکرد پروتکل پیشنهادی در مقایسه با طرح بر پایه درخت مرکل مشاهده می‌شود که طرح پیشنهادی با پیچیدگی و سربار کمتر به امنیت ساختارهای مبتنی بر درخت مرکل دست می‌یابد؛ اما به‌منظور بهبود عملکرد در اینجا پروتکل دست‌دهی کارآمدتری با ایجاد وابستگی بین پیام‌های هر مرحله در فرایند دست‌دهی برای مقابله با حمله DoS پیشنهاد شده است که در شکل (۹) نشان داده شده است.

در پروتکل پیشنهادی روش مقابله با حمله DoS بر اساس وابستگی هر مرحله به‌مرحله قبلی است، به‌گونه‌ای که اگر در مرحله قبل پیامی مانند S_n آورده شده است، در مرحله بعد، از این پیام استفاده نمی‌شود. درواقع، در این پروتکل به دلایل زیر از ایجاد وابستگی استفاده شده است:

- پیام‌های ارسالی در مراحل دو، سه و چهار کوتاه می‌شود و سربار مخابراتی کاهش می‌یابد.
- با استفاده از وابسته‌سازی مراحل به یکدیگر یکپارچگی تأمین و از حمله DoS جلوگیری می‌شود.
- در مقایسه با پروتکل‌های دارای وابستگی مراحل به یکدیگر با توجه به نگهداری مقادیر قبلی سربار حافظه کاهش می‌یابد
- باوجود مقدار S_n در پیام ۲ و S_{n+1} در پیام ۳ و ۴ مقادیر متناظر باید مستقل از مراحل دیگر محاسبه شوند، بنابراین مقادیر در مرحله بعد مورد استفاده قرار نمی‌گیرند (N_A,N_B,S_n,S_{n+1}).

علاوه براین به‌منظور دست‌یابی A به کلید PTK در مرحله دوم این کلید تبادل شده است. همچنین به‌منظور وابستگی نشست به PMK و ایجاد گسترش تغییرات پیام ۲ نسبت به پیام ۴ از PMK استفاده شده است.



شکل (۹). پروتکل دست‌دهی پیشنهادی با استفاده از وابسته‌سازی مراحل و توابع درهم‌ساز

۵- نتایج شبیه‌سازی

به‌منظور بررسی اعتبار و ارزیابی امنیتی پروتکل‌های پیشنهادی از بسته نرم‌افزاری AVISPA استفاده شده است[۱۱]. AVISPA شامل چهار آنالیز امنیتی خودکار و تصدیق شامل OFMC[1]، CL-AtSe[2]، STMAC[3] و TA4SP است. در این مقاله ما از سه آنالیز اول برای اثبات امنیت پروتکل پیشنهادی استفاده شده است. پیاده‌سازی پروتکل دست دهی بر پایه توابع درهم‌ساز وابسته نیز با استفاده از HLPSL ارائه‌شده است. پس از شبیه‌سازی توسط AVISPA نتایج رویه‌های تصدیق خروجی‌های OFMC (شکل ۱۰)، CL-AtSe (شکل ۱۱) و SATMC (شکل ۱۲) نشان داده شده است. مطابق با نتایج به‌دست‌آمده، مشاهده می‌شود که پروتکل پیشنهادی دارای منطق امنیتی صحیح و بدون اشکال منطقی است.

علاوه براین نتایج نشان می‌دهد که پروتکل پیشنهادی امن و قادر به جلوگیری از پیاده‌سازی حمله DoS توسط مهاجم است.

با توجه به استراتژی تازه کردن کلید پیشنهاد شده در بخش

1- On the fly Model Checker
2- Constraint Logical base Attack Searcher
3- SAT based Model Checker

PTK ، PMK،۳ و GTK به‌صورت دوره‌ای به‌روزرسانی می‌شوند؛ بنابراین از به‌روزرسانی مواد کلید در طرح‌های توابع یک‌سویه پیشنهادی برای حفاظت بهتر پیام ۱ و ۳ استفاده شده است.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/web-interface-computation/./tempdir/workfileR6TN8P.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.04s
  visitedNodes: 16 nodes
  depth: 4 plies
```

شکل (۱۰). خروجی OFMC

```
SUMMARY
  SAFE

DETAILS
  STRONGLY_TYPED_MODEL
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH

PROTOCOL
  workfileR6TN8P.if

GOAL
  %% see the HLPSL specification..

BACKEND
  SATMC

COMMENTS

STATISTICS
  attackFound                false      boolean
  upperBoundReached          true       boolean
  graphLeveledOff            2          steps
  satSolver                  zchaff     solver
  maxStepsNumber             11         steps
  stepsNumber                2          steps
  atomsNumber                0          atoms
  clausesNumber              0          clauses
  encodingTime               0.03       seconds
  solvingTime                0          seconds
  if2sateCompilationTime     0.27       seconds

ATTACK TRACE
  %% no attacks have been found..
```

شکل (۱۱). خروجی CL-AtSe

```
SUMMARY
  SAFE

DETAILS
  STRONGLY_TYPED_MODEL
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH

PROTOCOL
  workfileR6TN8P.if

GOAL
  %% see the HLPSL specification..

BACKEND
  SATMC

COMMENTS

STATISTICS
  attackFound                false      boolean
  upperBoundReached          true       boolean
  graphLeveledOff            2          steps
  satSolver                  zchaff     solver
  maxStepsNumber             11         steps
  stepsNumber                2          steps
  atomsNumber                0          atoms
  clausesNumber              0          clauses
  encodingTime               0.03       seconds
  solvingTime                0          seconds
  if2sateCompilationTime     0.27       seconds

ATTACK TRACE
  %% no attacks have been found..
```

شکل (۱۲). خروجی SATMC

به‌صورت ذهنی به‌روزرسانی مداوم مواد کلید به معنی پیچیدگی کمتر با توکن های احراز اصالت کمتر است، اما این در قبال سربار و تأخیر بالاتر است. همچنین پیاده‌سازی پروتکل دست دهی بر پایه عدم وابستگی مراحل فرآیند با استفاده از AVISPA ارزیابی شده است. پس از شبیه‌سازی توسط AVISPA خروجی‌های OFMC (شکل ۱۳)، CL-AtSe (شکل ۱۴) و SATMC (شکل ۱۵) تولید شده است. مطابق با نتایج به دست آمده مشاهده می‌شود که پروتکل پیشنهادی ازنظر منطقی امن است و در مقابل حمله DoS نیز مقاوم است. بنابراین مشاهده می‌شود که طرح پیشنهادی اهداف یک طرح امن و مقاوم در برابر حمله DoS را برآورده می‌کند.

OFMC Output.txt

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/avispa/web-interface-computation/./tempdir/workfileblHFuy.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.04s
  visitedNodes: 16 nodes
  depth: 4 plies
```

شکل (۱۳). خروجی OFMC پروتکل دست‌دهی بر پایه عدم وابستگی

CL-AtSe Output.txt

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/avispa/web-interface-computation/./tempdir/workfileblHFuy.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 1 states
  Reachable  : 0 states
  Translation: 0.01 seconds
  Computation: 0.00 seconds
```

شکل (۱۴). خروجی CL-AtSe پروتکل دست‌دهی بر پایه عدم وابستگی

SATMC Output.txt

```
SUMMARY
  SAFE

DETAILS
  STRONGLY_TYPED_MODEL
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH

PROTOCOL
  workfileblHFuy.if

GOAL
  %% see the HLPSL specification..

BACKEND
  SATMC

COMMENTS

STATISTICS
  attackFound                false      boolean
  upperBoundReached          true       boolean
  graphLeveledOff            2          steps
  satSolver                  zchaff     solver
  maxStepsNumber             11         steps
  stepsNumber                2          steps
  atomsNumber                0          atoms
  clausesNumber              0          clauses
  encodingTime               0.03       seconds
  solvingTime                0          seconds
  if2sateCompilationTime     0.26       seconds

ATTACK TRACE
  %% no attacks have been found..
```

شکل (۱۵). خروجی SATMC پروتکل دست‌دهی بر پایه عدم وابستگی

۶- نتیجه‌گیری

حمله DoS در خلال فرایند دست‌به‌دست شدن و تبادل پیام است یک آسیب‌پذیری امنیتی شدید در شبکه‌های مخابراتی و به‌ویژه شبکه‌های مش می‌باشد. با توجه به اهمیت این چالش در شبکه های هوشمند و به‌کارگیری معماری مش در این شبکه‌ها، در این مقاله یک طرح بر پایه به‌روزرسانی دوره‌ای مواد کلید پذیرفته و اثرات آن بر روی بهبود حفظت شبکه در مقابل حملات مهاجمان بررسی شده است. برای حفاظت بیشتر تبادل پیام، دو طرح احراز اصالت بر پایه تابع درهم‌ساز یک‌راهه وابسته و ایجاد عدم وابستگی بین مراحل دست‌دهی پیشنهاد شده است. قابلیت اطمینان طرح احراز اصالت بر پایه توابع درهم‌ساز وابسته با استفاده از شبیه‌سازی ارزیابی و تصدیق شده است.

۷- مراجع

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid – The New and Improved Power Grid: A Survey," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, 2012.

[2] T. W. Chim, S. M. Yiu, V. O. K. Li, and J. Zhong, "PRGA: Privacy-preserving Recording and Gateway assisted Authentication of Power Usage Information for Smart Grid," IEEE Transactions on Dependable and Secure Computing, vol. 5971, no. 1, pp. 85-97, 2014.

[3] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Computer Networks, vol. 57, pp. 1344–1371, 2013.

[4] IEEE Standard for Information Technology–Telecommunications and information exchange between systems–Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking. IEEE, IEEE 802.11s, 2011.

[5] IEEE Standard for Local and metropolitan area networks - Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 4: Alternative Physical Layer Extension to Support Medical Body Area Network (MBAN) Services Operating in the 2360 MHz 2400 MHz Band. IEEE 802.15.4, 2013.

[6] H. Gharavi and B. Hu, "Multigate Communication Network for Smart Grid," Proceedings of the IEEE, vol.99, pp.1028–1045, June 2011.

[7] 802.11i-2007 - IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE, 2007.

[8] S. Zonouz and P. Haghani, "Cyber-physical security metric inference in smart grid critical infrastructures based on system administrators' responsive behavior," Computers & Security, pp.1–11, July 2013.

[9] D. Mohan, "Denial of Service attack in Wireless Mesh Network," International Journal of Computer Science and Information Technologies, vol. 3, 2012.

[10] Z. Bai and Y. Bai, "4-Way Handshake Solutions to Avoid Denial of Service Attack in Ultra Wideband Networks," Third International Symposium on Intelligent Information Technology Application, pp. 232–235, 2009.

[11] "The AVISPA Project", Avispa-project.org, 2016. [Online]. Available: http://www.avispa-project.org/.

Journal Of Electronical & Cyber Defence
Vol. 4, No. 1, 2016, Serial No.13

Secure and Efficient 4-way Handshake in Smart Grid to DoS Attacks Mitigation

M. H. Ansari*, V. Tabatab Vakily, M. Gohareie

*Iran University Science and Technology

(Received: 17/01/2015, Accepted: 03/05/2016)

ABSTRACT

Abstract: Distributed communication networks provide proper connection with ooptimum cost between different domains of smart gride such as: home area network, neighbor area network and substation area network. With respect to handshake and key distribution are security challenges in smart grid, this paper proposed novel distribution and dynamic key procedures to enhance network resilience against malicious DoS attack. Proposed procedures using two famous security protocols: SAE and EMSA. These procedures are based on hash function and protocol stage dependency to improve network resilience against DoS attacks, because SAE and EMSA use 4-way handshake. Proposed procedures have optimum overhead. Finally, AVISPA is applied to prove the security of the enhanced protocol in smart grid. With extremely simulations and extended DoS attack model securities of proposed procedures are proved.

Keywords: Smart grid, Security, Key exchange, Handshake, Hash function.

* Corresponding Author Email: mh_ansari@elec.iust.ac.ir