

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

محمدحسن انصاری^{*}، وحید طباطبائی کیلی^۲، محمد گوهری^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 توزیع شده 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 شناخته شده احراز اصالت هم‌زمان برابر و مشارکت امن حلقه کارآمد استفاده می‌کند. از آنجایی که 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 درعین حال با توجه به محاسبه پیچیدگی مخابراتی و حافظه از نظر سربار تحمیل شده 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، دسته‌ی، توابع یک‌سویه.

۱- مقدمه

تعدادی واحد اندازه‌گیری فاز (PMU^۵) است که برای هم‌زمانی دقت بالا با کنترل‌کننده داده‌ها 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.

از آنجایی که در غیاب هر سیستم سیمی یا زیرساخت بی‌سیم فناوری 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

در حوزه‌های مختلف شبکه هوشمند یک زیرساخت مشخص و یکپارچه وجود ندارد، بنابراین شبکه‌های WLAN^۱ 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^۲)، شبکه ناحیه همسایه (NAN^۳) و شبکه ناحیه پست (SAN^۴) 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

* 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 Measurement Unit

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 به صورت 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 دوره‌های 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.

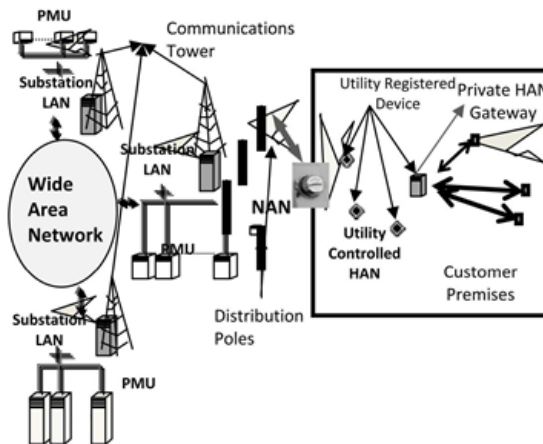
۲- امنیت سیستم‌های مش

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 با قابلیت اطمینان بالا و فرآیند احراز اصالت از دسترسی مهاجم به شبکه برای اختلال در شبکه به وسیله تولید پیام‌های جعلی جلوگیری می‌کند. به عنوان 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 به طرف خودش منحرف و شبکه را مختل کند. در این مقاله به منظور ایجاد عملکرد امن در یک مسیر طولانی، رهیافتی که قادر به تغییر دینامیکی اطلاعات کلید به صورت دوره‌ای و/یا در شرایط وجود حمله فعال آشکار شده، 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 می‌باشد 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 به صورت دوره‌ای آگهی ریشه را برای ایجاد درخت خود پخش

چندپرشه مستعد و آسیب‌پذیر بودن در مقابل حملات مختلف به دلیل ارسال بسته‌های داده به صورت 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 توزیع شده برای احراز اصالت نقاط مش (MP) می‌باشند.



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

[۱۲]

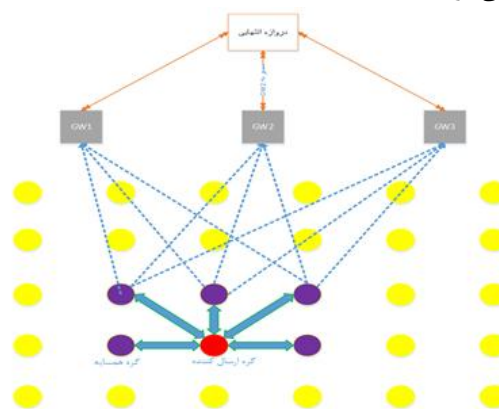
تاکنون، کارهای زیادی بر روی پروتکل امنیت شبکه‌های مش انجام شده و آسیب‌پذیری‌های مختلف شبکه در برابر حملات بررسی شده است [۳-۶]. همچنین برای انطباق و بهره‌برداری از شبکه‌های محلی IEEE802.11 به صورت مش، اخیراً استاندارد IEEE802.11s برای شبکه‌های مش ارائه شده است. این استاندارد احراز اصالت هم‌زمان یکسان (SAE) را به صورت پیش‌فرض به عنوان پروتکل امنیتی پشتیبانی می‌کند. پروتکل SAE بر پایه گذرواژه به اشتراک گذاشته شده بین همه گره‌های شبکه می‌باشد [۳]. در این روش با وجود این که 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 سلسله 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 بر این، از طریق شنود، مهاجم می‌تواند تبادل ۴- سویه را به وسیله 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 حمله DoS پیشنهاد شده است؛ بنابراین در اینجا هدف توسعه یک

شبکه‌های LAN تعریف می‌کند، پیام‌های EAP بین درخواست‌کننده و احراز اصالت‌کننده (دروازه اصلی) تبادل می‌شود، سپس پیام‌های EAP از درخواست‌دهنده به سرور احراز اصالت رله می‌شود. به محض احراز اصالت موفق، دروازه اصلی و دروازه درخواست‌دهنده یک تبادل ۴-سویه را شروع می‌کنند که حاصل آن استخراج PTK (زوج کلید گذرا) برای ارتباطات تک پخش و GTK (کلید گذرای گروهی) برای ارتباطات چندپخش 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 این که 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، به عنوان 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 کلید ارتباطات بین احراز اصالت‌کننده مش و توزیع‌کننده کلید مش (دروازه اصلی) هنگامیکه درخواست‌کننده به احراز اصالت‌کننده مش تبدیل می‌شود، استفاده شده است. در ادامه دروازه درخواست‌کننده احراز اصالت جدید فرآیند احراز اصالت را برای یکی از گره‌های انتخاب شده در مسیر درخت شروع می‌کند. اگر گره MP قبلاً توسط MP همسایه دیگری احراز اصالت شده باشد، فرآیند احراز اصالت تنها شامل ایجاد لینک همتا با تبادل ۴-سویه بدون نیاز به احراز اصالت EAPOL می‌باشد که این فرآیند به عنوان احراز اصالت ثانویه شناخته می‌شود [۸]. فرآیند ایجاد لینک و احراز اصالت تا زمانی که هر گره فرآیندهای PTK، GTK و PTK-KD را در تمام مسیر درخت برآورده نکند، ادامه می‌یابد.

۲-۲- پروتکل SAE برای شبکه‌های چند دروازه‌ای

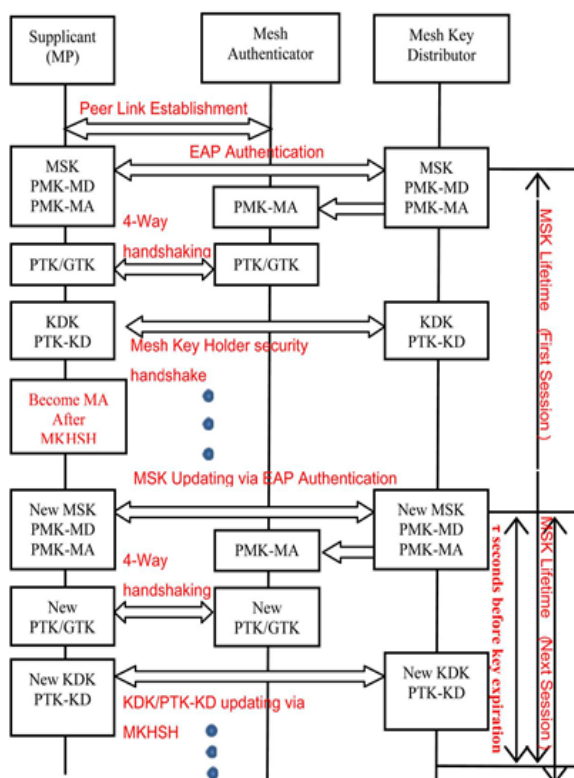
در SAE کلمه عبور به اشتراک گذاشته شده به وسیله همه MPها برای احراز اصالت یکدیگر استفاده می‌شود. در اینجا، بخش‌های درگیر به صورت MP-A و MP-B تعریف و توسط آدرس MAC شناسایی می‌شوند. پس از تشخیص درخواست ارتباط از طریق پایش غیرفعال بیکن‌ها یا جستجوی فعال، MPها پروتکل SAE را اجرا می‌کنند. قبل از تبادل پیام‌ها، 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. به محض 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

می‌کند. همه دروازه‌ها نیز از طریق دروازه اصلی به صورت بی‌سیم به پشت شبکه متصل می‌باشند. در اینجا فرض شده است که دروازه اصلی به عنوان یک احراز اصالت‌کننده مش (MA) به علاوه توزیع‌کننده کلید مش (MKD) عمل می‌کند. در حالت کلی MKD کلیدها را برای ایجاد سلسله مراتب کلید مش استنتاج می‌کند. در شبکه، دروازه‌های اصلی مسئول ایجاد و توزیع کلیدهای سلسله مراتبی مش به دروازه‌های محلی و در نتیجه به همه نقاط مش بعد از هر مرحله فرآیند احراز اصالت می‌باشند. به عبارت دیگر دروازه‌های اصلی همه اطلاعات احراز اصالت MPها را ذخیره می‌کنند. علاوه بر این، پروتکل EMSA شامل ایجاد لینک همتا طبق زیرساخت EAP و تبادل ۴-سویه، برای استنتاج کلید بین هر زوج گره مش در شبکه است. در پروتکل EMSA بعد از تبادل کلید مش، درخواست‌دهنده احراز اصالت یک احراز اصالت‌کننده مش می‌باشد. در واقع 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 MA 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 تأیید 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 احراز اصالت EMSA هر دروازه (به عنوان درخواست‌دهنده) از طریق فریم‌های درخواست و پاسخ با دروازه اصلی اجتماع را شروع می‌کند که شامل تبادل بازبودن لینک همتا و اطلاعات تأیید لینک همتا می‌باشد. به محض این که ایجاد لینک با موفقیت انجام شد، دروازه اصلی فرآیند احراز را شروع می‌کند. تحت IEEE 802.1X که EAP را برروری



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

۱-۳- 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-R1 (در SAE) 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 احراز اصالت‌کننده یا درخواست‌کننده شناخته می‌شود.

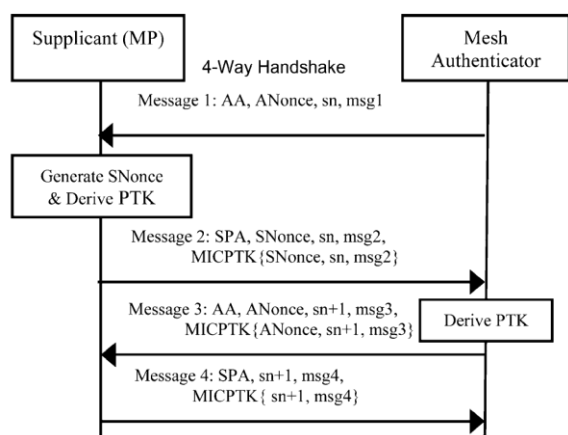
بنابراین انتظار می‌رود که حملات به‌دلیل رمزنگاری لایه لینک داده تنها قبل از تولید اولین PTK امکان‌پذیر باشند. پس حفاظت PTK در همه زمان‌ها اهمیت حیاتی دارد به‌گونه‌ای که تقریباً شکستن توابع رمزنگاری به‌جز در حالتی که یکپارچگی PTK نقض شود، غیرممکن است.

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

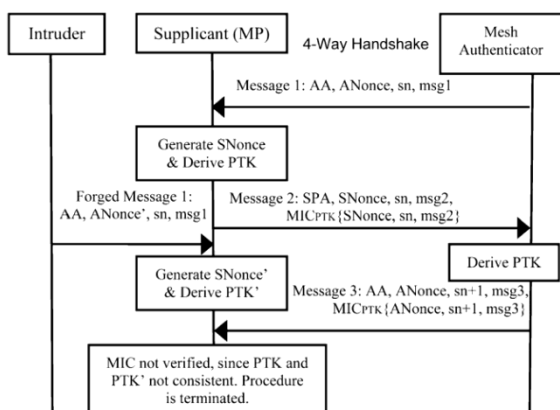
در این طرح مواد کلید در بازه‌های منظم به‌روزرسانی می‌شوند. در ابتدای احراز اصالت EAP یا SAE و تبادل ۴- سویه به‌روزرسانی برای استخراج یک مجموعه کلیدهای جدید قبل از ابطال مواد کلید موجود، انجام می‌شود. برای مثال در EMSA طول عمر کلید توزیع‌کننده و KDK نباید از طول عمر MSK بیشتر باشد. علاوه بر این طول عمر PTK و PMK-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-R0، PMK-R1 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 آشکار شده 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 در نتیجه 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 MSK، 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 به‌نشست 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.



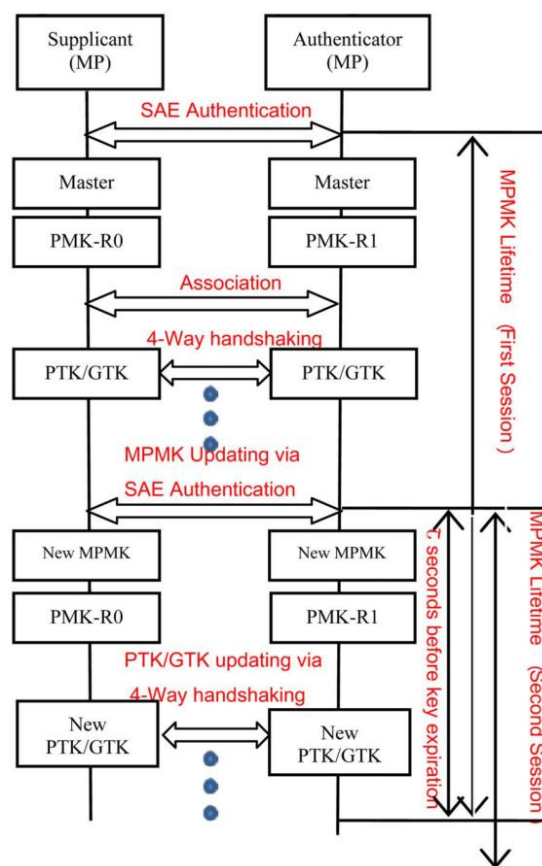
شکل (۵). رویه دست دهی ۴- سویه در استاندارد IEEE802.11s [۴]

بنابراین درخواست کننده، پیام ۲ را به وسیله محاسبه MIC بر روی کل پیام ۲ محافظت می کند. این فرآیند به MA اجازه آشکارسازی دست کاری پیام ۲ را می دهد؛ بنابراین از آنجایی که پیام ۱ به وسیله MIC محافظت نشده است، مهاجم قادر به تخریب تبادل ۴- سویه به وسیله جعل آن است. برای روشن شدن موضوع، نحوه پیاده سازی حمله DoS با استفاده از این ضعف در شکل (۶) نشان داده شده است.



شکل (۶). پیاده سازی حمله DoS با استفاده از آسیب پذیری پیام ۱ در فرآیند دست دهی 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 درخواست کننده ارسال می کند. نتیجتاً درخواست کننده بعد از دریافت پیام جعلی ۱ یک PTK جدید را تولید می کند که با PTK احراز اصالت کننده در تناقض است. بنابراین این رخداد سبب خاتمه یافتن فرآیند احراز اصالت و ابطال می شود. یک راه حل مقابله با این حمله ذخیره دو PTK لحظه ای (TPTK) و یک PTK در درخواست کننده است. در این حالت زمانی که پیام ۱ دریافت شود به روزرسانی می شود، در حالی که PTK تنها به محض دریافت پیام ۳ با MIC معتبر به روزرسانی می شود. این



شکل (۴). طرح به روزرسانی دوره ای 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 به منظور جلوگیری از دسترسی احراز اصالت کننده و درخواست کننده به کلید انجام دهد. فرض شده است که مهاجم قادر به جعل آدرس MAC سایر MP ها، شنود و نیز جعل پیام های دریافت شده است. شکل (۵) پیام های چکیده ای را که در تبادل ۴- سویه تبادل می شوند را نشان می دهد. در این شکل SPA، ANonce، SNonce، AA و ANonce بیانگر آدرس MAC و Nonce درخواست دهنده و احراز اصالت کننده است، sn دنباله اعداد و MICptk{ } بیانگر کد یکپارچگی پیام محاسبه شده برای محتوای درون براکت با PTK تازه می باشد. به نظر می رسد در حالت شبکه با زیرساخت امنیتی IEEE802.11i که در تبادل ۴- سویه مشارکت دارند، قابلیت های امنیتی، احراز اصالت و کلید رمزنگاری انتخابی از طریق عناصر اطلاعات RSNE پخش می شود. در این حالت همواره برای مهاجمان دست کاری پیام رمز نشده به راحتی امکان پذیر است. مطابق شکل (۶) در فرآیند تبادل ۴- سویه به محض این که درخواست کننده پیام ۱ را دریافت کند، برای تولید پیام نیازمند اطلاعات تولید پیام پاسخ است.

در محیط بی‌سیم سربار مخابراتی را به شدت افزایش می‌دهد. در این مقاله، به‌عنوان قابل اعتمادترین راه‌حل، یک روش درهم‌ساز سلسله مراتبی برای حفاظت پیام ۱ و پیام ۳ پیشنهاد شده است. برای این منظور، MA از تابع درهم‌ساز یک‌راهه SHA-1 برای احراز اصالت امن استفاده می‌کند.

۴- طرح پیشنهادی

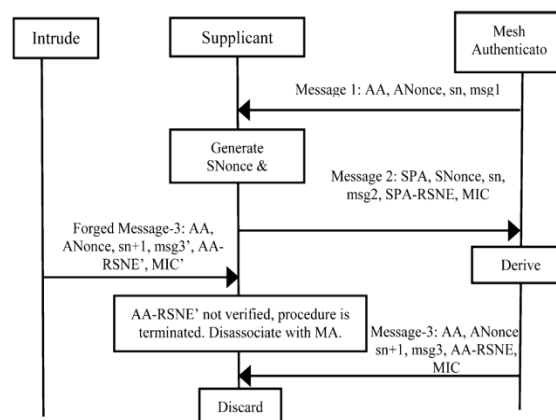
در روش‌های دست‌دهی یکی از مهم‌ترین ضعف‌های امکان حمله DoS است. این حمله به دلیل امکان تغییر در پیام‌های تبدالی در مراحل ۱ و ۳ قابل پیاده‌سازی است، به‌گونه‌ای که با تغییر در هر یک از مراحل کاربر در مقایسه‌ای که در مرحله ۳ انجام می‌دهد به تناقض می‌رسد و با تکرار آن امکان حمله DoS فراهم می‌شود. به دلیل ارسال پیام‌ها به صورت واضح در روش دست‌دهی، مهاجم با استراق سمع می‌تواند به آن‌ها دست‌یافته و با تغییر آن‌ها حمله را پیاده‌سازی کند. در واقع 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 تبدالی و تولید مقدار چکیده متناظر امکان پیاده‌سازی حمله DoS وجود دارد.

$$X = \text{hash}(A, B, C) \quad (1)$$

بنابراین برای جلوگیری از حمله DoS باید پیام X به مقداری که در تبدال 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 هر یک 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 استفاده شده است، علاوه بر این برای کاهش پیچیدگی و سربار به جای توابع رمزنگاری در رویه دست‌دهی 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.

روش برای دفاع در برابر حمله DoS زمانی که MIC در پیام ۳ به‌وسیله دو TPTK یا PTK تأیید اعتبار شود، کارآمد است. با این وجود، 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 دریافتی TPTK ها را ذخیره کند، بطوریکه تبدال ۴-سویه با احراز اصالت‌کننده 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 دست‌دهی، بعد از دریافت پیام ۳، درخواست‌کننده عنصر شبکه امن قوی (RNSE) را به‌وسیله مقایسه با RSNE قبلی دریافت شده (هر یک از بیکن یا فریم پاسخ جستجو) تصدیق می‌کند [۷]. اگر دو RSNE یکسان نباشد، درخواست‌کننده تبدال ۴-سویه را متوقف می‌کند. همان‌طور که در شکل (۷) نشان داده شده است، مهاجم می‌تواند به‌وسیله جعل پیام ۳ با AARSNE، MSG3 و MIC جعلی حمله را بر روی پیام ۳ انجام دهد.

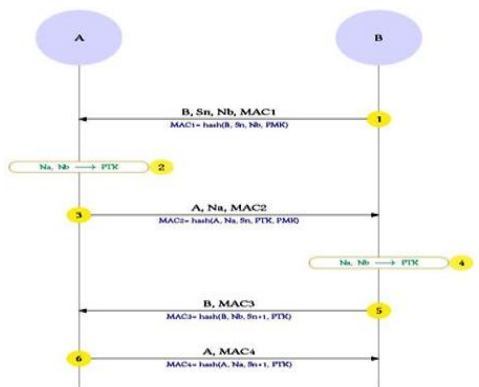


شکل (۷). پیاده‌سازی حمله DoS با استفاده از آسیب‌پذیری پیام ۳ در فرآیند دست‌دهی ۴- سویه استاندارد [۹]

مشاهده می‌شود که این فرآیند برای مهاجمی که AA، Anonce و sn+1 صحیح را استخراج و آنگاه AARSNE را تصدیق می‌کند، از آنجایی که RSNE جعلی نمی‌تواند با مقدار دریافت شده قبلی منطبق باشد، درخواست‌کننده از تبدال ۴- سویه صرف‌نظر و ارتباط خود را با MA قطع می‌کند؛ اما در این روش نیز پیام ۱ احراز اصالت شده هنوز در برابر حمله پاسخ آسیب‌پذیر است. روش مقابله دیگری که پیشنهاد شده است، استفاده از یک زوج شمارنده هم‌زمان شده برای اجتناب از حمله پاسخ می‌باشد [۹]. گرچه جزییات روش پیشنهادی در [۱۰] ارائه نشده است، متأسفانه طراحی و پیاده‌سازی شمارنده‌های هم‌زمان شده، به‌ویژه

متناظر باید مستقل از مراحل دیگر محاسبه شوند، بنابراین مقادیر در مرحله بعد مورد استفاده قرار نمی گیرند (N_A, N_B, S_n, S_{n+1})

علاوه بر این به منظور دست یابی A به کلید PTK در مرحله دوم این کلید تبادل شده است. همچنین به منظور وابستگی نشست به PMK و ایجاد گسترش تغییرات پیام ۲ نسبت به پیام ۴ از PMK استفاده شده است.



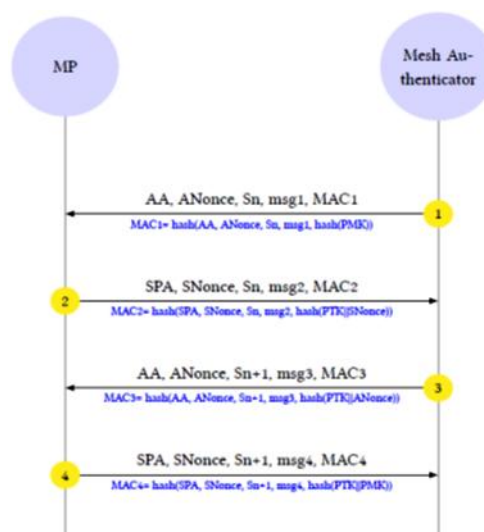
شکل (۹). پروتکل دست دهی پیشنهادی با استفاده از وابسته سازی مراحل و توابع درهم ساز

۵- نتایج شبیه سازی

به منظور بررسی اعتبار و ارزیابی امنیتی پروتکل های پیشنهادی از بسته نرم افزاری AVISPA استفاده شده است [۱۱]. AVISPA شامل چهار آنالیز امنیتی خودکار و تصدیق شامل 1 OFMC، 2 CL-AtSe، 3 STMAC و 4 TA4SP است. در این مقاله ما از سه آنالیز اول برای اثبات امنیت پروتکل پیشنهادی استفاده شده است. پیاده سازی پروتکل دست دهی بر پایه توابع درهم ساز وابسته نیز با استفاده از HLPSSL ارائه شده است. پس از شبیه سازی توسط AVISPA نتایج رویه های تصدیق خروجی های OFMC (شکل ۱۰)، CL-AtSe (شکل ۱۱) و SATMC (شکل ۱۲) نشان داده شده است. مطابق با نتایج به دست آمده، مشاهده می شود که پروتکل پیشنهادی دارای منطق امنیتی صحیح و بدون اشکال منطقی است.

علاوه بر این نتایج نشان می دهد که پروتکل پیشنهادی امن و قادر به جلوگیری از پیاده سازی حمله DoS توسط مهاجم است.

با توجه به استراتژی تازه کردن کلید پیشنهاد شده در بخش



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

پروتکل پیشنهادی دارای ویژگی یکپارچگی وابسته می باشد و با این ویژگی قادر به مقابله با حمله DoS مبتنی بر تغییر پیام است. علاوه بر این در فرآیند دست دهی از رمزنگاری استفاده نشده و به جای آن از توابع درهم ساز وابسته به کلید استفاده شده است، بنابراین سربرار مخابراتی و محاسباتی کاهش می یابد. در حالت کلی، در بررسی عملکرد پروتکل پیشنهادی در مقایسه با طرح بر پایه درخت مرکل مشاهده می شود که طرح پیشنهادی با پیچیدگی و سربرار کمتر به امنیت ساختارهای مبتنی بر درخت مرکل دست می یابد؛ اما به منظور بهبود عملکرد در اینجا پروتکل دست دهی کارآمدتری با ایجاد وابستگی بین پیام های هر مرحله در فرآیند دست دهی 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 به مرحله قبلی است، به گونه ای که اگر در مرحله قبل پیامی مانند S_n آورده شده است، در مرحله بعد، از این پیام استفاده نمی شود. در واقع، در این پروتکل به دلایل زیر از ایجاد وابستگی استفاده شده است:

- پیام های ارسالی در مراحل دو، سه و چهار کوتاه می شود و سربرار مخابراتی کاهش می یابد.
- با استفاده از وابسته سازی مراحل به یکدیگر یکپارچگی تأمین و از حمله DoS جلوگیری می شود.
- در مقایسه با پروتکل های دارای وابستگی مراحل به یکدیگر با توجه به نگهداری مقادیر قبلی سربرار حافظه کاهش می یابد
- با وجود مقدار S_n در پیام ۲ و S_{n+1} در پیام ۳ و ۴ مقادیر

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

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 از نظر 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/workfileb1HFuy.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/workfileb1HFuy.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
workfileb1HFuy.if
GOAL
%% see the HLPSSL 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

۳، PMK، PTK و GTK به صورت دوره‌ای به روزرسانی می‌شوند؛ بنابراین از به روزرسانی 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 HLPSSL 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 HLPSSL 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

به صورت ذهنی به روزرسانی 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

۶- نتیجه گیری

حمله DoS در خلال فرایند دست به دست شدن و تبادل پیام است یک آسیب پذیری امنیتی شدید در شبکه های مخابراتی و به ویژه شبکه های مش می باشد. با توجه به اهمیت این چالش در شبکه های هوشمند و به کارگیری معماری مش در این شبکه ها، در این مقاله یک طرح بر پایه به روزرسانی دوره ای 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 درهم ساز یک راهه وابسته و ایجاد عدم وابستگی بین مراحل دست دهی پیشنهاد شده است. قابلیت اطمینان طرح احراز اصالت بر پایه توابع درهم ساز وابسته با استفاده از شبیه سازی ارزیابی و تصدیق شده است.

۷- مراجع

- [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/>.

- [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.

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 optimum cost between different domains of smart grids 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