پروتکل تعیین اعتبار اعضای گروه در شبکه‌های متحرک اقتضایی

هانیه جلالی[۱]، ناصر موحدی‌نیا[۲]، احمد براآنی[۳]

[۱] دانشجوی کارشناسی ارشد، گروه کامپیوتر، دانشگاه اصفهان
اصفهان، ایران
jalali@eng.ui.ac.ir

[۲] استادیار، گروه کامپیوتر، دانشگاه اصفهان
اصفهان، ایران
naserm@eng.ui.ac.ir

[۳] استادیار، گروه کامپیوتر، دانشگاه اصفهان
اصفهان، ایران
ahmadb@eng.ui.ac.ir

چکیده

در معماری یک شبکه متحرک اقتضایی[۱] (MANET)، هیچ ساختار شبکه ثابت و از قبل مشخصی وجود ندارد و یک نود متحرک در این شبکه بسته‌های داده را به صورت مستقیم یا از طریق نودهای همسایه به نود مقصد می‌فرستد. از آن‌جایی که نودهای همسایه همیشه برای انتقال اطلاعات قابل اعتماد نیستند، این موقعیت به توجهات امنیتی زیادی نیاز دارد و استفاده از روش‌های تعیین اعتبار توصیه می‌شود. در این مقاله یک پروتکل تعیین اعتبار اعضای گروه برای MANET ارائه می‌شود. هدف این پروتکل آنست که اجازه دهد مجموعه‌ای از نودها به صورت قانونی وارد یک گروه شوند و در ادامه به نودهای پذیرفته‌شده کلید رمز گروه را توزیع کند تا ارتباط امنی را بین اعضای گروه ایجاد کند. این پروتکل، تعیین اعتبار اعضای گروه را براساس دانش فراهم می‌کند که در آن از اثبات با دانش صفر(ZKP[۲]) و رمزنگاری سطح آستانه[۳] استفاده می‌شود.

کلمات کلیدی

شبکه متحرک اقتضایی، امنیت، تعیین اعتبار، جامعیت داده‌ای، تعیین اعتبار اعضای گروه.

۱- مقدمه

در شبکه‌های بی‌سیم[۴] اولیه برای ایجاد شبکه همیشه به یک سیستم حمایت مرکزی مثل نقطه دسترسی[۵] احتیاج بود تا ارتباط کاربران بی‌سیم را برقرار کند. اما این خصوصیت باعث می‌شد که نتوان این شبکه‌ها را در همه جا، سریع و به آسانی ایجاد کرد و به اصطلاح قابلیت تطابق[۶] وجود نداشت. در نتیجه به شبکه‌های احتیاج بود که سریع و آسان و در هر مکانی قابل توسعه باشند. این

امکان‌پذیر نبود مگر اینکه شبکه به هیچ ساختار ثابت و از پیش تعریف شده‌ای احتیاج نداشته باشد و با توجه به این نیازمندی‌ها شبکه‌های متحرک اقتضایی به وجود آمدند.

مهمترین خصوصیت شبکه‌های MANET این است که به هیچ ساختار ثابتی مانند نقطه دسترسی احتیاج ندارند و امکان توسعه سریع و آسان شبکه را فراهم می‌کنند. این شبکه‌ها می‌توانند ارتباط فوری بین دو یا چند نود را بدون نیاز به هیچ ساختار یا مدیریت مرکزی برقرار کنند.

نودها در این شبکه آزاد هستند که حرکت کنند و خودشان را در هر مدل تصادفی شکل دهند و هر کاربر آزاد است تا در حین ارتباط با دیگر نودها مکان خود را تغییر دهد. هر نود می تواند به عنوان یک میزبان و مسیریاب برای همه دیگر نودها باشد. به طور کلی چون در این شبکه هیچ سیستم حمایت مرکزی وجود ندارد، همه وظایف از جمله مسیریابی توسط خود نودها انجام می‌شود.

نودها در این شبکه از طریق لینک‌های بی‌سیم به هم متصل هستند و یک مسیر بین دو نود می‌تواند شامل یک یا چند پرش[۷] باشد. این شبکه به صورت اقتضایی شکل می‌گیرد، به این معنی که برای یک منظور خاص ایجاد شده و پس از رسیدن به هدف پایان می‌یابد.

از آن‌جایی که در این شبکه نودها آزاد هستند که حرکت کنند، توپولوژی شبکه مرتباً در حال تغییر است و نحوه اتصال نودها و کیفیت انتقال ممکن است در طول زمان براساس ورود، خروج و حرکت نودها تغییر کند [۷، ۸].

در یک شبکه متحرک اقتضایی، هر نود متحرک نودهای همسایه خود را پیدا کرده و با آن‌ها یک مسیر ارتباطی برقرار می‌کند. در چنین محیطی نود متحرک نودهای همسایه خود را نمی‌شناسد و در نتیجه بسته‌های داده او برای رسیدن به مقصدی که در برد او نیست، ممکن است از نودهای تصادفی عبور کنند. این موقعیت به توجهات امنیتی نیاز دارد، زیرا نودهای همسایه ممکن است کاربران مغرضی باشند که بسته‌های داده را استراق سمع کرده و یا ترافیک زیادی را فرستاده و منجر به حمله توقف خدمات[۸] شوند.

از آن‌جایی که استفاده از این شبکه‌ها روز به روز افزایش می‌یابد مسئله برقراری امنیت در آن‌ها بسیار مهم است. براساس خصوصیات ذکر شده تشخیص نودهای قانونی که یک گروه را در شبکه تشکیل می‌دهند در فاز اول برای تعیین اعتبار[۹] نودها و در فاز دوم برقراری ارتباطی امن بین خود نودها بسیار مهم است. با توجه به این نیازمندی‌ها، در این مقاله پروتکل تعیین اعتباری براساس دانش ارائه می‌شود که در دو مرحله دسترسی به داده‌ها و منابع را کنترل می نماید و برای این کار از اثبات با دانش صفر و رمزنگاری با سطح آستانه با کمی تغییر استفاده می‌کند.

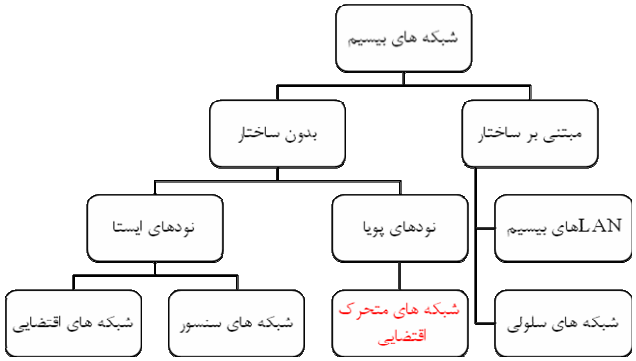
برای مکانیسم‌های اشتراک کلید گروه، پروتکل‌های توافق کلید گروه (GKA[10]) کاندیدهای مناسبی برای کاربردهای گروهی هستند[۲، ۵]. هدف اصلی در GKA استفاده از یک کانال امن برای توزیع کلید جدید به همه اعضای گروه می باشد، اما این کار با هر بار وارد و خارج شدن نودها باید انجام شود.

در مقابل GKA مکانیسم اشتراک کلید دیگری براساس رمزنگاری سطح آستانه وجود دارد [۳و۴]، که روش بسیار مفیدی است اما اشکالاتی بر آن وارد می باشد. در روش‌های ارائه شده به بعضی مسائل امنیتی توجه نمی‌شود. برای مثال در بعضی موارد به یک مرکز رسمی برای توزیع کلید احتیاج است که چنین چیزی در طبیعت شبکه‌های متحرک اقتضایی امکان‌پذیر نیست. همچنین در بسیاری از روش‌ها راهبردی برای تعیین اعتبار اعضای گروه وجود ندارد. که پروتکل ارائه شده در این مقاله سعی در رفع این اشکالات دارد.

در ادامه مقاله ابتدا به معرفی شبکه‌های متحرک اقتضایی پرداخته شده و نیازمندی‌های امنیتی این شبکه ذکر و تعیین اعتبار به عنوان یکی از مهم‌ترین نیازها شرح داده خواهد شد. پس از آن پروتکل تعیین اعتبار پیشنهاد شده معرفی و دو مکانیسم استفاده شده در پروتکل به عنوان پیش نیاز شرح داده می‌شوند. در بخش بعد قسمت‌های مختلف پروتکل مانند نهادهای موجود، مدل ارتباطی و تنظیمات اولیه آن بیان می‌شوند. در بخش آخر نتیجه‌گیری شده و کارهای آینده ذکر می‌شوند.

۲- شبکه متحرک اقتضایی

شبکه متحرک اقتضایی سیستمی خودمختار است از نودهای متحرک که به صورت بی‌سیم به یکدیگر متصل هستند و هر نود برای دیگر نودها به عنوان یک نود انتهایی و یا یک مسیریاب عمل می‌کند [۷]. با توجه به خصوصیات گفته شده جایگاه این شبکه در بین شبکه‌های بی‌سیم در شکل (۱) نشان داده شده است.



شکل (۱): جایگاه شبکه متحرک اقتضایی در بین شبکه‌های بی‌سیم [۸]

یک MANET می تواند به تنهایی کار کند یا به یک شبکه بزرگتر متصل شود. این شبکه کاربردهای بسیار زیادی در زمینه‌های مختلفی دارد، از جمله در کنترل بلایای طبیعی، عملیات‌های نظامی و جنگ‌ها، ارتباط قایق‌ها بر روی آب، شبکه کردن وسایل نقلیه. علاوه بر شرایط خاص، این شبکه می تواند باعث ایجاد کیفیت بهتر

در جاهای دیگر نیز بشود. برای مثال می‌توان گروهی از افراد را همراه با لپ‌تاپ در یک ملاقات تجاری در نظر گرفت که هیچ گونه سرویس شبکه‌ای وجود ندارد. آن‌ها می‌توانند به آسانی سیستم‌های خود را با ایجاد یک شبکه متحرک اقتضایی، شبکه کنند [۸، ۷].

شبکه‌های متحرک اقتضایی نسبت به شبکه‌های بی سیم سنتی مزایایی دارند که شامل سادگی توسعه این شبکه‌ها، سرعت توسعه آن‌ها و وابسته نبودن به هیچ ساختار ثابتی می باشد.

اما ویژگی‌های خاص این شبکه چالش‌های متفاوتی را نیز فراهم می‌کنند که از آن جمله پویایی توپولوژی شبکه، مسیریابی، دشواری ارائه کیفیت سرویس[۱۱]، مصرف توان زیاد و امنیت هستند.

براساس ذات پویای شبکه متحرک اقتضایی این شبکه از تغییرات مداوم ساختار رنج می‌برد. ساختار این شبکه می‌تواند به صورت سریع و غیرقابل‌پیش‌بینی تغییر کند و نحوه اتصالات در طول زمان متفاوت شود. بنابراین شبکه متحرک اقتضایی باید بتواند خود را با شرایط ترافیک و انتشار و الگوهای تحرک نودهای متحرک وفق دهد. اضافه بر این در این شبکه‌ها به یک مکانیسم مسیریابی کارا احتیاج است تا انتقال مناسبی را در طول شبکه ایجاد کند. از آن‌جایی که ساختار این شبکه مرتباً در حال تغییر است، موضوع مسیریابی بسته ها بین هر جفت نود در MANET یک چالش است.

کیفیت‌سرویس به توانایی شبکه در فراهم کردن سرویس قابل-اعتمادتری به ترافیک انتخاب شده‌ای از شبکه برمی‌گردد. فراهم کردن لایه‌هایی از کیفیت‌سرویس در یک محیط پویا یک چالش دیگر این شبکه ها است.

در بیشتر ترمینال‌های متحرک سبک وزن، توابع مربوط به ارتباط باید طوری بهینه شوند که در مصرف برق صرفه جویی شود. شبکه‌های بی‌سیم اقتضایی چالش دیگری را نیز در طراحی سیستم کارای مصرف برق دارند. به دلیل نبود یک ساختار ثابت، هر نود در این شبکه می تواند به عنوان یک مسیریاب نیز عمل کند. برای اینکه یک MANET بتواند به خوبی کار کند باید بتوان بار ترافیکی را طوری در بین نودها متعادل نمود که نودهای با محدودیت مصرف برق بتوانند در زمانی که ترافیک از طریق نودهای دیگر در حال مسیریابی است در حالت خواب و مصرف کمتر قرار گیرند.

و اما یکی از مهم‌ترین نکات در این شبکه فراهم کردن ارتباطی امن بین نودهای میزبان است. خصوصیات خاص شبکه‌های متحرک اقتضایی مانند معماری باز شبکه، رسانه بی‌سیم مشترک، سیستم توزیع‌شده و ساختار پویا چالش‌های مختلفی را برای ایجاد امنیت بوجود آورده‌اند، به طوریکه نیاز به توسعه راه حل‌های امنیتی که منجر به حفاظت بیشتر و کارایی دلخواه شبکه می‌شود را بیشتر کرده است. کانال بی‌سیم در MANET هم توسط کاربران قانونی قابل دسترس است و هم مهاجمان مغرض. در نتیجه مسئله امنیت برای این شبکه‌ها، خصوصاً برای کاربردهایی که حساس به امنیت[۱۲] هستند، بسیار مهم است [۹]. در ادامه نیازمندی‌های امنیتی یک شبکه متحرک اقتضایی بیان می‌شوند.

۲-۱- نیازمندی‌های امنیتی MANET

برای ایمن کردن یک MANET برآورده شدن نیازهایی مانند محرمانگی، جامعیت[۱۳] داده، دسترس‌پذیری و حفظ اعتبار ضروری است.

محرمانگی تضمین می‌کند که اطلاعات خاصی هرگز برای نهادهای غیرمجاز آشکار نشود. انتقال اطلاعات حساس در شبکه مانند اطلاعات استراتژیکی یا تاکتیکی نظامی، به محرمانگی نیاز دارند. اطلاعات مسیریابی نیز باید در موارد خاصی محرمانه بمانند، زیرا ممکن است این اطلاعات برای دشمنان ارزشمند باشد تا از طریق آن اهداف خود را در جنگ تشخیص و مکان‌یابی کنند.

جامعیت داده ضمانت می‌کند که پیام‌های انتقال داده شده هرگز خراب نمی‌شوند یا به زبان دیگر داده‌ها هیچ وقت به صورت غیرمجاز تغییر نمی‌یابند.

دسترس‌پذیری باعث می‌شود که داده‌ها در هنگام درخواست موجود و در دسترس باشند، به عبارت دیگر مکانیسم‌های امنیتی نباید به صورتی بکار گرفته شوند که افراد مجاز با اهداف مجاز و مفید نتوانند به داده‌ها دسترسی پیدا کنند [۱۰، ۳].

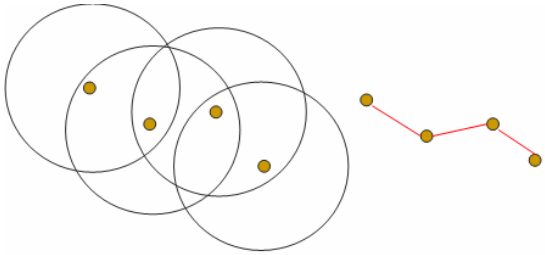
تعیین اعتبار شامل روش‌هایی است که از راه‌هایی حمایت می-کند که تنها کاربران مجاز بتوانند به منابع شبکه دسترسی پیدا کنند یا به بیان دیگر هویت ادعا شده توسط کاربران قبل از برقراری ارتباط اثبات شود [۶].

در شبکه‌ها، تعیین اعتبار می تواند برای مثال شامل روش‌هایی باشد که با آن‌ها تشکیل گروهی از نودها کنترل می‌شود به طوریکه فقط نودهای مجاز بتوانند گروه‌ها را شکل داده یا خراب کنند و یا به آن‌ها وارد شده یا خارج شوند. تعیین اعتبار همچنین می‌تواند به معنای روش‌هایی باشد که نودها در ابتدای ورود به شبکه برای وارد شدن به سیستم شبکه استفاده می‌کنند تا بتوانند با دیگر نودها ارتباط برقرار کنند [۱۰].

۲-۲- تعیین اعتبار در MANET

تعیین اعتبار یک موضوع کاربردی در شبکه‌های متحرک اقتضایی می‌باشد، زیرا در معماری یک MANET از آن‌جایی که هیچ ساختار شبکه ثابت و تعریف شده‌ای وجود ندارد یک نود متحرک در این شبکه، همانگونه که در شکل (۲) نشان داده شده است، بسته-های داده را یا مستقیماً یا از طریق نودهای همسایه به نود مقصد می‌فرستد. این موقعیت به توجهات امنیتی احتیاج دارد زیرا همیشه نمی‌توان به این نودهای همسایه اطمینان کرد، چرا که بعضی از کاربران مغرض می‌توانند در مسیر یا محدوده مسیریابی بسته‌های

داده را استراق سمع کنند یا ترافیک زیادی را فرستاده و منجر به حمله توقف خدمات (DoS) شوند [۱].



شکل (۲): نحوه انتقال بسته‌های داده در MANET [۱۱]

برخلاف ارتباط از طریق اینترنت، مکانیسم‌های سنتی امنیت مثل پروتکل‌های تعیین اعتبار و تکنیک‌های رمزنگاری داده نمی‌توانند بدون ساختار رسمی اعطای گواهی یا توزیع کلید در این شبکه بر MANET منطبق شوند. این مسئله شدیداً در مقابل دیگر شبکه‌های متحرک مانند Mobile IP یا تلفن‌های همراه است که نودها برخلاف متحرک بودنشان همیشه زیر نظر مدیریت هستند.

براساس خصوصیات این شبکه، تقسیم نودهای همسایه به دو گروه مطمئن و نامطمئن بسیار مهم است. به طور کلی، توجهات امنیتی در MANET به یک فرد تعلق ندارد بلکه به یک گروه از نودها مثل یک شرکت یا پروژه مربوط است. به عبارت دیگر آماده شدن در مقابل تهدیدات امنیتی در یک MANET بیشتر بر مبنای تشخیص اعضای قانونی گروه است که در مرحله اول انجام می‌گیرد.

زمانی که تعیین اعتبار اعضای گروه در MANET کامل شد، فاز بعد محافظت از ارتباط بین خود اعضای گروه است چرا که در پروتکل‌های تعیین اعتبار، دو مسئله تعیین اعتبار و جامعیت داده‌ای نمی‌توانند از یکدیگر جدا باشند. زیرا در یک ارتباط کافی نیست طرف‌های ارتباط بدانند که پیام از عضو قانونی آمده ولی مطمئن نباشند که در طول راه به طور غیر مجاز تغییر نکرده است و یا بالعکس مطمئن باشند که پیام به طور غیر مجاز تغییر نیافته ولی ندانند که از طرف چه کسی آمده است. استفاده از یک کلید مشترک گروه برای رمزنگاری و رمزگشایی پیام می‌تواند به این نیاز جامعیت داده‌ای پاسخ دهد. اما چیزی که در اینجا مهم‌تر و پیچیده‌تر است مدیریت و توزیع کلید گروه است که بعضی موارد باید در این زمینه رعایت شوند: ۱) اعضای قانونی باید بتوانند در یک شبکه شلوغ که توپولوژی شبکه و نودهای متحرک به طور پویا تغییر می‌کنند، کلید گروه را بدست آورند. ۲) حتی اگر پیامی بین عضو جدید و دیگر نودها استراق سمع شد، کلید گروه نباید برای غیر اعضا آشکار شود.

در اینجا یک پروتکل تعیین اعتبار اعضای گروه براساس دانش[۱۴] در MANET بدون ساختار ارائه می‌شود که شامل دو فاز ساختار تعیین اعتبار اعضای گروه و ساختار مدیریت کلید رمز گروه[۱۵] می‌شود. بعد از پایان این دو فاز اعضای تایید شده یک کلید رمز را دریافت کرده‌اند و می‌توانند ارتباطی امن با دیگر اعضای قانونی گروه برقرار کنند. در ادامه این پروتکل و تکنیک‌های استفاده شده در آن شرح داده خواهند شد.

۳- پروتکل تعیین اعتبار اعضای گروه براساس دانش

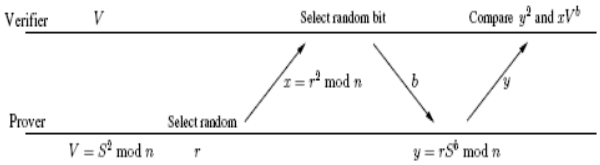
همان‌طورکه گفته شد این پروتکل از دو فاز تشکیل شده است. در فاز اول که وظیفه تعیین اعتبار را بر عهده دارد از اثبات با دانش صفر (ZKP) استفاده می‌شود و در فاز دوم که برای ایجاد ارتباط امن بین اعضای گروه و جامعیت داده‌ای، کلید رمز گروه را مدیریت می‌کند از رمزنگاری سطح آستانه استفاده می‌شود.

در ادامه ابتدا هر یک از این دو روش شرح داده شده و بعد استفاده از این دو روش در پروتکل و طراحی آن بیان می‌شود.

۳-۱- اثبات با دانش صفر (ZKP)

پروتکل ZKP، یک اثبات محاوره‌ای است که در آن طرف اول (prover) به طرف دوم (verifier) ثابت می‌کند که اطلاعات خاصی را دارد بدون آنکه این اطلاعات را آشکار کند. در این پروتکل، یک طرف پرسشی را به دیگری ارسال کرده و طرف مقابل پاسخ می‌دهد. زمانی این پاسخ درست است که کلید طرف مقابل رمز مشترک را داشته باشد. به چنین روشی پروتکل پرسش-پاسخ[۱۶] گفته می‌شود. همانطور که در شکل (۴) نشان داده شده یک دور نمونه در ZKP شامل قدم‌های زیر است:

۱. یک پیام (commitment) از طرف اول فرستاده می‌شود.
۲. یک پرسش از طرف دوم فرستاده می‌شود.
۳. از طرف اول یک پاسخ در مقابل پاسخ ارسال می‌شود.
۴. ممکن است پروتکل بارها تکرار شود.
۵. براساس پاسخ‌دهی طرف اول در تمام دورها، طرف دوم تصمیم می‌گیرد که آیا اثبات را قبول کرده یا رد کند.



شکل (۳): روال ZKP [۱]

برای انجام چنین کاری روش‌های مختلفی وجود دارد که یکی از این روش‌ها که در این پروتکل استفاده شده در ادامه توضیح داده می‌شود.

روال شناخت شامل مراحل مکالمه است که ثابت می‌کند prover مربع یک عدد خاص را می‌داند بدون اینکه هیچ اطلاعاتی راجع به خود عدد آشکار کند.

همان‌طور که در شکل (۳) نشان داده شده است، prover ابتدا مقدار $V = S^2 \bmod N$ را، برای اثبات ادعای خود که می‌گوید S را می‌داند، محاسبه می‌کند (عدد N مقداری مشخص دارد و حاصلضرب دو عدد اول بزرگ است) و باید چند دور مکالمه را انجام دهد. در هر دور prover یک عدد تصادفی r را انتخاب می‌کند و $x = r^2 \bmod N$ را به verifier می‌فرستد که به نوعی ارسال درخواست ارتباط نیز هست. اکنون verifier یک بیت تصادفی b را انتخاب و به prover می‌فرستد که به نوعی پاسخ به درخواست او نیز هست. Prover با $y = rS^b \bmod N$ پاسخ می‌دهد. برای اثبات ادعای prover، verifier y^2 را محاسبه و با xV^b مقایسه می‌کند. اگر دو مقدار برابر باشند اثبات ادعا پذیرفته شده و اگر برابر نبودند اثبات رد می‌شود.

۳-۲- رمزنگاری سطح آستانه

این تکنیک براساس به اشتراک گذاشتن یک رمز بین نودها است.

یک رمزنگاری سطح آستانه (n, t) (که $n \geq t$ است) روشی است که در آن اجازه می‌دهد یک مجموعه حداقل t نودی از n نود بتوانند یک عمل رمزنگاری را با هم انجام دهند (دسترس پذیری)، در حالیکه برای t-1 نود پیدا کردن رمز حتی با توطئه هم امکان پذیر نباشد (محرمانگی).

از این روش برای تولید کلید گروه هم استفاده می‌شود. براساس این روش برای اینکه اجازه دهیم هر t نود از n تا یک رمز داده شده را بسازند، یک چندجمله‌ای بصورت زیر از درجه t-1 باید ساخته شود که ضریب ثابت آن (S) رمز است و بقیه ضرایب اعداد تصادفی هستند:

$$y = f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \ldots + a_1 x + S \qquad (۱)$$

در این حالت هر یک از این n اشتراک یک جفت (x_i , y_i) از اعداد هستند که $f(x_i) = y_i , x_i \in \{1 \ldots n\} , x_i \neq 0$. اکنون با استفاده از هر t اشتراک چندجمله‌ای به صورت یکتا ساخته می‌شود و می‌توان S را با استفاده از درون‌یابی لاگرانژ پیدا کرد:

$$l_i = \prod_{j=1, j\neq i}^{j=t} \frac{j}{j-i} \qquad (۲)$$

با این حال با t-1 یا کمتر نود نمی‌توان رمز را پیدا کرد. در روش رمزنگاری سطح آستانه (n, t)، کلید رمز گروه S به n سهم تقسیم می‌شود $(s_1, s_2, \ldots, s_n)$، و هر سهم مربوط به یک نود می‌شود. به $(s_1, s_2, \ldots, s_n)$ سهم بندی (n, t) از S، می‌گوییم.

۴- طراحی پروتکل

۴-۱- مروری بر پروتکل

هر دو فاز تعیین اعتبار اعضای گروه و مدیریت کلید رمز گروه برای ایجاد یک ارتباط امن گروهی در MANET روال‌هایی ضروری هستند. در ادامه مروری بر نحوه کار پروتکل تعیین اعتبار براساس دانش آورده شده است که از دو تکنیک شرح داده شده در بالا به عنوان پیش نیاز استفاده می‌کند.

در ابتدا ساختار تعیین اعتبار اعضای گروه شرح داده می‌شود. در این پروتکل علاوه بر رمزنگاری و رمزگشایی ارتباط گروه، کلید رمز یک گروه برای برای تشخیص گروهی که یک نود متحرک عضو آن است هم استفاده می‌شود. به عبارت دیگر هر کلید رمز گروه می‌تواند به عنوان یک شناسه[۱۷] یکتا تعریف شود. در این پروتکل مجموعه کلیدهای یک نود متحرک "دانش[۱۸]" نامیده می‌شود و دانش یک نود همه گروه‌هایی که نود قبلاً عضو آن‌ها بوده را مشخص می‌کند.

وقتی یک نود متحرک می‌خواهد عضو یک گروه جدید شود، به دنبال اعضای قانونی گروه در همان شبکه می‌گردد و تلاش می‌کند تا با آن‌ها ارتباط برقرار کند. این اعضای قانونی گروه دانش نود را شناسایی کرده، با اطلاعات "مورد نیاز برای عضویت در گروه" که قبلاً تعریف شده مقایسه و ارزیابی می‌کنند که آیا نود می‌تواند به گروه ملحق شود یا نه.

در این روش شناخت دانش، دشمن نباید بتواند موفق شود تا هیچ اطلاعات بامعنایی را بدزدد حتی اگر اطلاعات ردوبدل شده بین نود جدید و دیگر اعضا را استراق سمع کرده باشد. در این راستا از الگوریتم ZKP برای تشخیص کلید رمز گروه بدون آشکار شدن اطلاعات، استفاده می‌شود. در ZKP نود جدید مانند prover رفتار می‌کند و اعضای قانونی گروه مانند verifier. در یک نشست ZKP، verifier احتیاج ندارد از کلید رمز برای شناخت کلید استفاده کند؛ در عین حالیکه دانش نود شامل کلید رمز گروه‌هایی است که قبلاً در آنها عضو شده، کلید تاییدی[۱۹] که به هر کلید محرمانه مربوط است نیز در اطلاعات مورد نیاز برای عضویت در گروه مربوطه قرار دارد که برای شناخت کلید از آن استفاده می‌شود.

پس از اینکه شناخت دانش کامل شد، نود جدید آماده است تا کلید رمز گروه را به عنوان عضو جدید گروه بگیرد. برای ساختار مدیریت کلید رمز گروه از رمزنگاری سطح آستانه استفاده می‌شود. کلید رمز گروه به n سهم تقسیم می‌شود و بعد با پاسخ t نود رمز توسط نود جدید دوباره تولید می‌شود. سپس وقتی نود کلید رمز گروه را دریافت کرد، پروتکل تشخیص می‌دهد که نود به گروه جدید ملحق شده و اطلاعات عضویت گروه جاری او را ارتقا می‌دهد. به زبان دیگر دانش نود قدم به قدم با بدست آوردن کلید رمز گروه‌های مختلف ارتقا می‌یابد.

۴-۲- نهادها

قبل از شرح مدل ارتباطی پروتکل سه نهاد استفاده شده در آن معرفی می‌شوند: ۱) عضو جدید ۲) مجموعه دارای کلید[۲۰] ۳) آغازگر.

عضو جدید، نود متحرکی است که می‌خواهد عضو گروهی در شبکه شود. این نود در ابتدا یک عضو احتمالی گروه است، و بعد سهم‌ها را از t تا عضو دارای کلید می‌گیرد و کلید رمز گروه را تولید می‌کند. او باید کلید شناخت مربوط به کلید رمز گروه را براساس درخواستش بداند.

مجموعه دارای کلید یک مجموعه (n عضوی) از اعضای قانونی گروه است. این واحد دارای سهم خود از کلید رمز گروه و اطلاعات لازم برای عضویت در گروه‌ها (یعنی لیستی از کلیدهای شناخت) است. او دانش عضو جدید را بررسی می‌کند و سهم خود از کلید را به او می‌دهد. مجموعه دارای کلید مانند verifier در ZKP رفتار می‌کند.

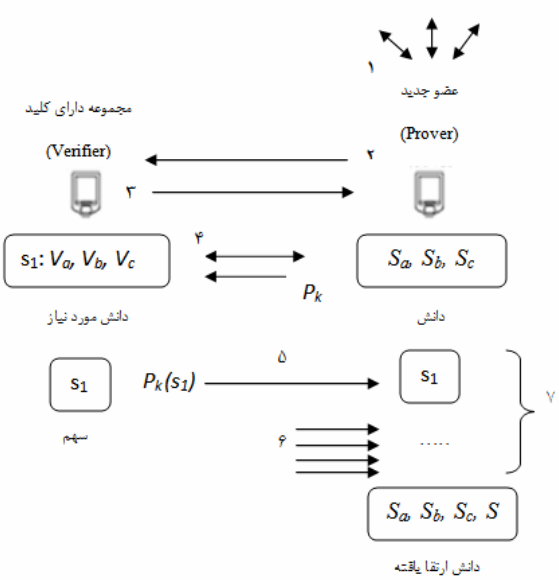
در هر گروه یک *آغازگر* به عنوان نهاد ابتدایی وجود دارد که فقط در فاز شکل‌گیری اولیه گروه ظاهر می‌شود.

۴-۳- مدل ارتباطی

قدم‌های بعد جریان ارتباط بین عضو جدید و مجموعه دارای کلید را، همان‌طورکه در شکل (۴) نشان داده شده است، بیان می‌کنند:

۱. عضو جدید آدرس IP مجموعه‌های دارای کلید را برای یک کلید رمز S پیدا می‌کند.
۲. عضو جدید درخواست را به مجموعه دارای کلید انتخاب شده برای بدست آوردن سهم S می‌فرستد.
۳. مجموعه دارای کلید به درخواست پاسخ می‌دهد.
۴. عضو جدید و مجموعه دارای کلید برای نشست ZKP شروع به پرسش و پاسخ می‌کنند تا تشخیص داده شود که آیا عضو جدید اطلاعات لازم برای عضویت را دارد یا نه. مجموعه دارای کلید در طول نشست ZKP کلید عمومی (P_k) عضو جدید را بدست می‌آورد.
۵. مجموعه دارای کلید سهم خود از رمز را بصورت امن به عضو جدید می‌دهد.
۶. همه مراحل بالا t بار برای مجموعه‌های دارای کلید مختلف اجرا می‌شود.
۷. در نهایت عضو جدید S را از t سهم دریافت شده توسط رمزنگاری سطح آستانه تولید می‌کند.

در هر قدم از ۲ تا ۵، پروتکل یک مقدار زمان مشخص[۲۱] تعریف می‌کند تا عضو جدید روال را با مجموعه دارای کلید انتخاب شده قطع کند، زیرا ممکن است در حین ارتباط مجموعه دارای کلید شبکه را ترک کند. وقتی عضو جدید روال را قطع می‌کند بعد از پایان زمان مزبور شروع به ارتباط با مجموعه دارای کلید دیگری می‌کند.



شکل (۴) : جریان ارتباط بین prover و verifier

از آن‌جایی که پروتکل برای شناخت دانش احتیاج به نشست‌های ZKP زیادی دارد ممکن است در مراحل پرسش و پاسخ به ردوبدل تعداد زیادی پیام بین اعضای گروه برای تعیین اعتبار نیاز باشد و منجر به پایین آمدن کارایی پروتکل شود. برای حل این مشکل می‌توان از ZKP بصورت موازی استفاده کرد طوری که در هر بار ارسال چندین پیام فرستاده شود.

۴-۴- تنظیمات اولیه

فاز راه‌اندازی برای تنظیمات اولیه پروتکل شامل دو قدم است: ۱) تنظیمات اولیه گروه ۲) تنظیمات اولیه نود.

تنظیمات اولیه گروه شامل تعیین اطلاعات لازم برای عضویت، تعیین مقدار کلید رمز گروه، و تعریف (n, t) برای رمزنگاری سطح آستانه است. آغازگر این مقادیر را مشخص می‌کند، یک چند جمله‌ای برای رمزنگاری سطح آستانه محاسبه می‌کند، و سهم‌ها و اطلاعات لازم برای عضویت مربوط را بین مجموعه های دارای کلید توزیع می‌کند. بعد از پایان این فاز آغازگر کار خود را در شبکه پایان می‌دهد، همه اطلاعات مربوط به مکانیسم تولید کلید مشترک را پاک می‌کند، و یک مجموعه دارای کلید معمولی می‌شود.

روال تنظیمات اولیه نود - که معمولاً تنها زمانی که نود بوت می‌شود انجام می‌گیرد – فقط یک بار برای هر نود احتیاج است و وظیفه اصلی او آماده کردن "دانش اولیه" است. بعد نود از این دانش اولیه استفاده می‌کند و در دفعات بعد آن را ارتقا می‌دهد. در این پروتکل فرض می‌شود که دانش اولیه توسط شرکتی که نود در آن کار می‌کند یا ISP که معمولاً توسط آن وصل می‌شود، صادر می‌گردد.

۵- نتیجه

در این مقاله به خصوصیات شبکه‌های متحرک اقتضایی که چالش-های امنیتی را برای این شبکه‌ها فراهم می‌کنند توجه گردید. با توجه به ویژگی‌های خاص این شبکه‌ها نمی توان در آن‌ها از مکانیسم‌های سنتی امنیت استفاده کرد. در ادامه پروتکلی برای تعیین اعتبار در این شبکه‌ها ارائه شد که از دو فاز اصلی تشکیل می‌شود. در فاز اول نودها برای ورود به یک گروه تعیین اعتبار می-شوند و برای این کار از روش اثبات با دانش صفر استفاده می‌شود و در فاز دوم با استفاده از پروتکل رمزنگاری سطح آستانه، کلید رمزی برای برقراری ارتباط امن بین اعضای قانونی به اشتراک گذاشته می-شود و به این ترتیب جامعیت داده‌ای فراهم می‌گردد.

در این پروتکل کلید رمز گروه لزوماً باطل نمی‌شود. زیرا کلید گروه در این پروتکل به عنوان دانش استفاده می‌شود و دانش باید برای مدت زمان طولانی نگه داشته شود. با این حال ایجاد یک مکانیسم هوشمند و قابل توسعه ابطال کلید گروه که سازگاری پروتکل براساس دانش ما را حفظ می‌کند ممکن است در آینده مورد نیاز باشد.

مراجع

[1] Asaeda, Hitoshi, Rahman, Musfiq, Manshaei, Mohammad Hossein, Fukuzawa, Yasuko, *Implementation of Group Member Authentication Protocol in Mobile Ad-hoc Networks*, 2004.

[2] Tsudik, G., Steiner, M., Waidner, M., *Key agreement in dynamic peer groups*, IEEE Transactions on Parallel and Distributed Systems, August 2000.

[3] Zhou, Lidong, Haas, Zygmunt J., *Securing Ad Hoc Networks*, Cornell University, 1999.

[4] Kong, J., Zerfos, P., Luo, H., Zhang, L., *Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks*, Proc. IEEE ICNP, November 2001.

[5] Steiner, M., Ateniese, G.,Tsudik, G., *"New multiparty authentication services and key agreemwnt protocols"*, IEEE Journal of Selected Areas in Communications, 18(4):1-13, 2000.

[6] Kärpijoki, Vesa, *Security in Ad Hoc Networks*, Helsinki University of Technology, 2000.

[7]Humayun Bakht, *Understanding Mobile Ad hoc Networks*, http://www.computingunplugged.com/issues/issue200406/00001301001.html, last visited: April 2008.

[8]Uyen Trang Nguyen, *Mobile Ad-hoc Networks: Issues and Challenges*, http://www.cse.yorku.ca/course_archive/2006-07/F/6590/Notes/MANET_issues.ppt, last visited: April 2008.

[9] Humayun Bakht, *A focus on the challenges of mobile ad-hoc networks*, http://www.computingunplugged.com/issues/issue200408/00001346001.html, last visited: April 2008.

[10] UCLA EE, Kurpinski, Chris, Kim, Sungha, *Security in ad hoc networks*, http://nesl.ee.ucla.edu/courses/ee206a/2002s/student_presentations/SP09_KimKurpinski.ppt, last visited: April 2008.

[11] Iyer, Sridhar, *Mobile Ad Hoc Networks*, http://www.it.iitb.ac.in/~sri/talks/manet.ppt, last visited: April 2008.

زیرنویس‌ها

[1] Mobile Ad-Hoc Network
[2] Zero Knowledge Proof
[3] Threshold Cryptography
[4] Wireless Networks
[5] Access Point
[6] Adaptability
[7] Hop
[8] Denial of Service (DoS)
[9] Authentication
[10] Group Key Agreement
[11] Quality of Service
[12] Security-Sensitive
[13] Integrity
[14] Knowledge-based Group Member Authentication Protocol
[15] Secret Group Key Management

[16] Challenge-Response Protocol
[17] Identifier
[18] Knowledge
[19] Verification key
[20] Share Holder
[21] Timeout