"رمزنگاری توسط ابر خم های بیضوی و پیشنهاد پروتکل توافق کلید گروهی برای شبکه های موردی مبتنی بر ناحیه با استفاده از ابر خم های بیضوی"

نویسندگان: ۱- سید عباس کاظمی، ۲- مهدی جوانمرد، ۳- سید علی رضوی ابراهیمی

(۱) دانشگاه پیام نور، دانشجوی کارشناسی ارشد گروه علمی مهندسی کامپیوتر و فناوری اطلاعات، Sakazemi2006@yahoo.com
(۲) استادیار دانشگاه پیام نور و رئیس شبکه دانشگاههای مجازی کشورهای اسلامی، Info@Javanmard.com
(۳) استادیار سازمان مرکزی - دانشگاه پیام نور ، Dr_ali_razavi@yahoo.com

چکیده

رمزنگاری علم تبادل و نگهداری امن اطلاعات است. انواع سیستم های رمزنگاری متقارن و نامتقارن هستند. ارتباط گروهی امن یکی از چالش های سیستم های رمزنگاری است. پروتکل توزیع کلید دیفی– هلمن در زمینه تبادل کلید اساسی است و همچنین پایه اکثر پروتکل های توافق کلید گروهی است که دارای مشکل حمله مردی در میانه است. برای رفع این عیب می توان از مسائل سخت ریاضی همچون لگاریتم گسسته، خم های بیضوی، ابر خم های بیضوی بهره برد. در سیستم رمزنگاری **RSA** طول کلید ۱۰۲۴ بیت است که با خم های بیضوی طول کلید ۱۶۰ بیت و با ابر خم های بیضوی طول کلید را به ۵۳ ، ۵۱ بیت می توان کاهش داد. همچنین پروتکل توافق کلید گروهی برای شبکه های موردی مبتنی بر ناحیه با استفاده از ابر خم های بیضوی پیشنهاد شده در این مقاله در حافظه مصرفی، پردازش، پهنای باند، انرژی مصرفی نسبت به پروتکل های با ساختار مشابه کارآمدتر می نماید.

واژه‌های کلیدی: رمزنگاری، شبکه های موردی، ابر خم های بیضوی، پروتکل توافق کلید گروهی با ابر خم بیضوی.

۱- مقدمه

رمزنگاری (Cryptography) علم تبادل و نگهداری امن اطلاعات است. محیط های نظامی و امنیتی بستر استفاده و گسترش این علم بوده است. امروزه پیشرفت سریع فناوری اطلاعات و انجام الکترونیکی بسیاری از داد و ستدها بر نقش اساسی این علم افزوده است. به گونه ای که میتوان گفت بدون استفاده از علم رمزنگاری، تجارت الکترونیک و دولت الکترونیکی هیچگونه کاربردی نخواهند داشت. هنگامی که با امنیت دیتا سر و کار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم، این سه موضوع یعنی محرمانگی (Confidentiality) ، احراز اصالت (Authentication) و جامعیت (Integrity) در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می توانند از رمزنگاری استفاده کنند. اغلب این مساله باید تضمین شود که پیغام فقط می تواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مساله باشد رمزنگاری نام دارد. رمزنگاری هنر نوشتن بصورت رمز است بطوریکه هیچکس بغیر از دریافت کننده مورد نظر نتواند محتوای پیغام را بخواند.

برای محافظت از دیتای اصلی (Plaintext) ، آنرا با استفاده از یک کلید (رشته ای محدود از بیتها) بصورت رمز درمی آوریم تا کسی که دیتای حاصله را می خواند قادر به درک آن نباشد. دیتای رمز شده (Ciphertext) بصورت یک سری بی معنی از بیتها بدون داشتن رابطه مشخصی با دیتای اصلی بنظر می رسد. برای حصول متن اولیه دریافت کننده آنرا رمزگشایی می کنند.یک شخص ثالث (مثلا"یک هکر) می تواند برای اینکه بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمز نوشته شده را رمزشکنی (Cryptanalysis) کند. بخاطر داشتن وجود این شخص ثالث بسیار مهم است.

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید، الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیشتر آنها بعنوان استانداردها یا مقالات ریاضی منتشر شده اند. کلید، یک رشته از ارقامی دودویی (صفرو یک) است که به خودی خود بی معنی است. رمزنگاری مدرن فرض می کند که الگوریتم شناخته شده است یا می تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده سازی تغییر می کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

طراحی الگوریتم های رمزنگاری مقوله ای برای متخصصان ریاضی است. طراحان سیستمهایی که در آنها از رمزنگاری استفاده می شود، باید از نقاط قوت و ضعف الگوریتم های موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم گیری داشته باشند. اگر چه رمزنگاری از اولین کارهای شانون (Claude Shannon) در اواخر دهه ۴۰ بشدت پیشرفت کرده است و هم اکنون نیز با ورود به سایت بنیاد شانون (Claude Shannon Institute) درقسمت رمزنگاری مشاهده می گردد که طراحی نرم افزارها و سخت افزارهای رمزنگاری با خم های بیضوی (Elliptic curve) و ابر خم های بیضوی (Hyperelliptic curve) از شاخه های به شدت در حال کار رمزنگاری هستند، اما کشف رمز نیز پا به پای رمزنگاری به پیش آمده است و الگوریتمهای کمی هنوز با گذشت زمان ارزش خود را حفظ کرده اند. بنابراین تعداد الگوریتمهای استفاده شده در سیستمهای کامپیوتری علمی و در سیستمهای بر پایه کارت هوشمند بسیار کم است[1].

۲- طرح های رمزگذاری

تعریف طرح رمزگذاری: یک طرح رمزگذاری یا دستگاه رمزنگاری یک ۵ تائی (P,C,K,E,D) با خواص ذیل است:

۲-۱- P (Plaintext) یک مجموعه است. این مجموعه فضای متن ساده نامیده می شود. اعضای آن متن ساده نامیده می شوند.

۲-۲- C (Ciphertext) یک مجموعه است. این مجموعه را فضای متن رمز می نامند. اعضای آن متن رمز نامیده می شوند.

۲-۳- K یک مجموعه بوده و فضای کلید (Key) نام دارد. اعضای آن کلید نامیده می شوند.

۲-۴- $E = \{E_k : k \in K\}$ یک خانواده از توابع با تعریف $E_k: P \to C$ است. اعضای آن توابع رمزگذاری (Encryption) نام دارند.

۲-۵- $D = \{D_k : k \in K\}$ یک خانواده از توابع با تعریف $D_k: C \to P$ است. اعضای آن توابع رمزگشایی (Decryption) نام دارند.

۲-۶- برای هر $e \in K$، عضوی چون $d \in K$ وجود دارد که برای هر $p \in P$ رابطه $D_d(E_e(p)) = p$ برقرار است.

به عنوان مثال به یک سیستم رمز که به سیستم رمزی سزار (Caesar cipher) معروف است، اشاره می کنیم. فضای متن ساده، رمز و کلید برابر با $\sum = \{A, B, \ldots, Z\}$ هستند. ما بر این اساس که هر حرف انگلیسی را با عدد شماره متناظرش در ترتیب حروف منهای یک در نظر می گیریم. این توانایی محاسبه با حروف را فراهم می کند.

برای $e \in Z_{26}$ تابع رمزکننده E_e چنین تعریف می شود.

$E_e: \sum \to \sum \quad , \quad x \to (x + e) \bmod 26$

بر این اساس برای $d \in Z_{26}$ تابع رمزگشایی D_d را داریم.

$D_d: \sum \to \sum \quad , \quad x \to (x - d) \bmod 26$

کلیدرمزگشایی متناظر با کلید رمزگذاری e برابر d=e

است. این خاصیت برای تمامی سیستم های رمزنگاری (Cryptosystems) برقرار نیست.

رمز سزار را می توان به سادگی به فرمی اصلاح کرد که در آن فضای متن ساده و متن رمز برابر مجموعه تمامی دنباله های $W = (w_1,w_2,\ldots,w_n)$ با $w_i \in \sum$; $1 \le i < n$ باشد. باز هم فضای کلید Z_{26} است. تابع رمز کننده E_e هر عضو w_i را با $w_i + e \bmod 26$ جایگزین می کند. این نیز دستگاه رمز سزار نامیده می شود[2].

۳- انواع سسیستم های رمزنگاری

در کل دو نوع سیستم رمزنگاری داریم یکی متقارن (Symmetric) و دیگری نامتقارن (Asymmetric) که به شرح آنها در ذیل می پردازیم.

اگر آلیس بخواهد یک پیغام رمز شده را به باب بفرستد از یک کلید رمزنگاری e استفاده کرده و سپس باب کلید رمزگشایی d متناظر با آن را برای به دست آوردن متن ساده به کار می برد.

در یک سیستم رمز اگر همواره کلید رمزگذاری e برابر کلید رمزگشای d بوده، ویا d به سادگی از روی e قابل محاسبه باشد آنگاه سیستم را متقارن می نامیم. اگر آلیس و باب از یک سیستم رمز متقارن استفاده کنند باید قبل از تبادل اطلاعات کلید مخفی e را مبادله کنند. مبادله محرمانه کلید یک مساله اساسی است. کلید e باید محرمانه نگهداری شود زیرا هر کس که به آن دسترسی پیدا کند می تواند کلید رمزگشای d را به دست آورد. رمز سزار مثالی از یک سیستم رمز متقارن است. کلیدهای رمزگذار و رمزگشا در این سیستم برابر هستند.

در یک سیستم رمز نامتقارن کلیدهای d و e متمایز بوده و محاسبه d از روی e شدنی نیست. در چنین سیستم هایی کلید رمزگذار e را می توان به صورت همگانی اعلام نمود. اگر باب بخواهد یک پیغام رمز شده دریافت کند کلید رمزگذاری را به همگان اعلام نموده و کلید رمزگشای متناظر با آن یعنی d را مخفی می کند. هر کسی می تواند e را به کار ببرد و متن رمز شده را برای باب بفرستد. از این رو، e را یک کلید عمومی (Public Key) می نامند. ولی تنها باب قادر به گشودن پیام ها می باشد و از این جهت یک کلید خصوصی نامیده می شود. سیستم های رمز نامتقارن را سیستم های کلید عمومی می نامند.

در سیستم های کلید عمومی غالبا" معرفی دو فضای کلید متفاوت است زیرا کلید های عمومی و خصوصی (Private) شکل های متفاوت دارند. این تنها منجر به تغییر ناچیزی در تعریف رمز می شود[1].

۴- رمزشکنی

شکستن رمز، مرتبط با، حمله (Attack) به سیستم رمز است. در این قسمت این حمله ها را دسته بندی می کنیم. جهت دشوار نمودن حمله به یک سیستم رمز می توان آن را مخفی نگهداری نمود. ولی مشخص نیست که از این طریق چقدر امنیت حاصل می شود زیرا یک حمله کننده به روش های متفاوت می تواند به شناسائی سیستم اقدام کند. از تکه های جدا شده از یک متن رمز می توان تلاشی را در جهت شناخت سیستم رمز انجام داد. ممکن است حمله کننده (Attacker) اقدام به جمع آوری اطلاعات از طریق افراد آشنا به سیستم نماید.

بر این اساس در بحث رمز شکستن فرض بر این است که حمله کننده از نوع سیستم رمز به کار رفته مطلع است. تنها کلیدهای (خصوصی) به کار رفته و متن های ساده را مخفی فرض می کنند. حمله کننده تلاش می کند تا از روی متن رمز متن ساده را به دست آورده و یا حتی کلید به کار رفته راتعیین کند. انواع حمله های موجود به شرح زیر می باشند:

۴-۱- **حمله فقط با متن رمز شده** (Ciphertext-only attack): حمله کننده متن های رمز شده را دارد و با استفاده از آن تلاش می کند که متن ساده متناظر و یا کلید را به دست آورد.

۴-۲- **حمله با متن ساده معلوم** (Known-Plaintext attack): در این روش، حمله کننده یک متن ساده و متن رمز متناظر با آن و یا چند جفت از آنها را در اختیار دارد. او

تلاش می کند که کلید را پیدا کرده و یا بقیه متن رمز را رمزگشایی کند.

۴-۳- **حمله با متن ساده انتخاب شده** (Chosen-Plaintext attack): حمله کننده قادر به رمز کردن متون ساده بوده ولی کلید را نمی داند. او تلاش می کند که کلید را پیدا کرده و یا متون رمز شده دیگری را باز نماید.

۴-۴- **حمله متن ساده تطبیقی** (Adaptive Chosen-Plaintext attack): حمله کننده قادر به رمز گذاری متن های ساده می باشد. او قادر به انتخاب متن های ساده جدید به عنوان تابعی از متن رمزهای به دست آمده می باشد. اما او کلید را نمی داند و تلاش می کند که کلید را به دست آورده و یا متن رمز های دیگر را باز کند.

۴-۵- **حمله با متن رمز شده برگزیده** (Chosen-Ciphertext attack): حمله کننده می تواند رمز گشایی موقت کند ولی کلید را نمی داند. او تلاش می کند که کلید را پیدا کند[3].

۵- انواع حمله به سیستمهای رمز نامتقارن

با فرض اینکه سیستم یک طرفه است، به روشهای زیر می توان به این گونه سیستمها حمله کرد[1]:

۵-۱- **روش جستجوی جامع** (Brute-Force): این روش مبتنی بر جستجوی کل فضای کلید خصوصی است تا کلید مورد نظر به دست آید.

۵-۲- **یافتن روشی برای پیدا کردن کلید خصوصی از کلید عمومی**: برای اکثر سیستمها ثابت نشده که این کار ممکن نیست، پس ممکن است روشی پیدا شود که با داشتن کلید عمومی بتوان کلید خصوصی متناظررا به دست آورد.

۵-۳- **حدس زدن پیام رمز شده**: در صورتی که طول پیام کوتاه باشد. مثلا" اگر یک متن ۵۶ بیتی توسط الگوریتم نامتقارن رمز شود، چون کلید عمومی را همه می دانند می توان تمام متنهای ۵۶ بیتی را آزمایش کرد تا متن مورد نظر پیدا شود.

۵-۴- **حل مساله سخت ریاضی متناظر با الگوریتم**.

۶- توزیع کلید عمومی

معمولا" برای توزیع کلید در الگوریتم متقارن از کلید عمومی استفاده می شود. برای این منظور باید کلید عمومی افراد در شبکه توزیع شود که برای این امر روشهای مختلفی را می توان در نظر گرفت. اما معمولا" کلید عمومی به یکی از روشهای زیر توزیع می شود[4]:

۶-۱- **اعلان** (Announcement): کلید عمومی به همه کاربران ارسال می شود. ارسال می تواند به صورت پخش (Broad cast) باشد یا توسط پست الکترونیک صورت گیرد. نقطه ضعف اصلی این روش این است که کلید عمومی به راحتی جعل (Fiction) می شود، زیرا احراز اصالتی در آن صورت نمی گیرد.

۶-۲- **فهرست** (Directory): در این روش یک فهرست مطمئن وجود دارد که لیست همه کاربران و کلید عمومی آنها را داراست. با فرض اینکه ارتباط بین فهرست و کاربران با احراز اصالت است، بدین ترتیب هر کاربر می تواند کلید عمومی هر کاربر دیگر را به دست آورد. این روش مانند دفترچه تلفن است. نقطه ضعف آن، تمرکز کلیدها در یک فهرست است و از این طریق ممکن است مورد حمله قرار گیرد.

۶-۳- **مرجع مورد اعتماد**: این حالت پیشرفته فهرست عمومی است. در حالت قبل ممکن است که فهرست دارای کلید نباشد(مثلا"دفترچه تلفن)، اما در این روش برای دسترسی به فهرست نیاز به تایید دارد. نقطه ضعف آن تراکم مراجعه به یک نقطه است یعنی در نقطه ای از سیستم گلوگاه (Buttle-Neek) ایجاد می شود.

۶-۴- **گواهی** (Certificate): در این حالت اطلاعات و کلید عمومی کاربران توسط صادر کننده گواهی که مورد تایید همه است امضاء می شود. در این صورت هر فرد گواهی خودش را نگه می دارد و در صورت نیاز به فرد دیگر می فرستد.

یک گواهی معمولا" شامل حداقل اطلاعات زیر است:

- شناسه
- نام کاربر
- کلید عمومی
- تاریخ ایجاد، تاریخ شروع فعالیت و تاریخ انقضاء[3].

۷- توزیع کلید متقارن توسط کلید عمومی

با توجه به اینکه الگوریتم های نامتقارن معمولا" کند هستند اغلب از آنها برای توزیع کلید در الگوریتم های متقارن استفاده می شود. این کلید متقارن را کلید جلسه (Session key) می نامند. یک روش ساده برای تولید کلید جلسه بین دو کاربر این است که ابتدا آلیس کلید عمومی خود را به همراه شناسه خودش به باب ارسال می کند، سپس باب کلید جلسه را با کلید عمومی آلیس رمز می کند و برای آلیس می فرستد و بالعکس. اشکال اساسی این روش آن است که فرد سومی می تواند در وسط قرار گیرد و کلید جلسه را بداند، بدون اینکه آلیس و باب خبر دار شوند(این نوع از حمله را حمله مردی در میانه (Man in the middle attack) می نامند. یکی از روشهای امن که محرمانگی و احراز اصالت را شامل می شود این است که، فرض می شود کلیدهای عمومی قبلا" به یکی از روشهای ارائه شده در بند ۶ (همچون گواهی) مبادله شده اند. به دلیل اینکه در بعضی سیستمها کلید متقارن به طور متناوب عوض می شود و نیز سرعت الگوریتمهای نامتقارن کم است، لذا ترجیح داده می شود از مرکز توزیع کلید (Key distribution center) برای توزیع کلید استفاده شود(یعنی توسط کلید اصلی بین مرکز توزیع کلید و هر کاربر). در این حالت می توان کلید اصلی را توسط الگوریتم نامتقارن مبادله کرد[4].

۸- پروتکل دیفی- هلمن

در این قسمت پروتکل دیفی– هلمن (Diffie–Hellman) را برای تبادل کلید روی کانال ناامن بررسی می کنیم. خود این پروتکل یک سیستم رمز عمومی نیست بلکه پایه ای برای سیستم رمزگذاری الجمال (ElGamal encryption system) است. وضعیت به شرح زیر است.

آلیس و باب می خواهند از یک سیستم رمز متقارن روی یک کانال ناامن استفاده کنند. در ابتدا آنها باید یک کلید مبادله کنند. سیستم تبادل کلید دیفی – هلمن این امکان را به آلیس و باب می دهد تا از کانال ناامن برای تبادل کلید استفاده کنند. هر کسی می تواند به تبادل کلید توجه داشته باشد اما اطلاعات به دست آمده را نمی توان در تشخیص کلید مخفی به کار برد. پروتکل دیفی – هلمن را می توان همچون سنگ بنایی برای رمز نگاری کلید عمومی لحاظ کرد. امنیت مبادله کلید دیفی – هلمن بر پایه مساله لگاریتم گسسته (Discrete Logarithm Problem) است و بستگی به مساله تجزیه اعداد صحیح ندارد.

روش کار پروتکل دیفی – هلمن به شرح ذیل است. آلیس و باب می خواهند توافقی روی یک کلید مخفی داشته باشند. تماس آنها از طریق یک کانال ناامن امکان پذیر است. ابتدا آنها روی یک عدد اول بزرگ p و یک ریشه اولیه به هنگ p، مانند g، با شرط $2 \le g \le p-2$ توافق می کنند. عدد p و ریشه اولیه g به صورت عمومی اعلام می شود. پس آلیس و باب از کانال ناامن خود برای حصول به این توافق استفاده می کنند. اکنون یک عدد صحیح $a \in \{0,1,..,p-2\}$ به صورت تصادفی انتخاب می کند. او مقدار زیر را محاسبه می کند:

$A = g^a \bmod p$

عدد A برای باب ارسال می شود ولی نمای a مخفی نگهداشته می شود. باب عدد صحیح $b \in \{0,1,..,p-2\}$ را تصادفی انتخاب می کند. مقدار زیر توسط باب محاسبه می شود:

$B = g^b \bmod p$

عدد B برای آلیس ارسال می شود. باب نیز یک نمای b را مخفی نگه می دارد. برای تعیین کلید مخفی مشترک، آلیس مقدار $B^a \bmod p = g^{ab} \bmod p$ و باب نیز مقدار $A^b \bmod p = g^{ab} \bmod p$ را محاسبه می کنند. کلید مشترک برابر K است[5]. $K = g^{ab} \bmod p$

۹- امنیت پروتکل دیفی- هلمن

استراق سمع کننده اسکار، اعداد p، g، A، B را می فهمد ولی اطلاعی از a و b، لگاریتم های گسسته A و B در پایه g، ندارد. او می خواهد از p، g، A، B کلید مخفی

$K = g^{ab} \bmod p$ را به دست آورد. این به مساله دیفی – هلمن معروف است. اگر اسکار بتواند لگاریتم گسسته را حل کند آنگاه مساله دیفی – هلمن را نیز حل می کند. در واقع با محاسبه لگاریتم گسسته B در پایه g، یعنی b، کلید $K= A^b$ را تعیین می کند. این تنها راه شناخته شده برای حل مساله دیفی – هلمن است. تاکنون هیچ کس ثابت نکرده است که اگر اسکار بتواند مساله دیفی – هلمن را بشکند آنگاه قادر به حل مساله لگاریتم گسسته نیز خواهد بود. یک چنین اثباتی یک مساله باز مهم در رمزنگاری کلید عمومی است. مادامیکه حل مساله دیفی – هلمن مشکل باشد هیچ استراق سمع کننده ای قادر به تعیین کلید خصوصی بر اساس اطلاعات اعلام شده عمومی نخواهد بود. ولی این تنها نوع حمله ممکن روی پروتکل دیفی – هلمن نیست.

در حمله مردی در میانه، اسکار از این واقعیت که آلیس نمی تواند مطمئن باشد که پیام دریافتی در واقع از طرف باب است استفاده می کند. اسکار تمامی پیام های بین آلیس و باب را تفسیر می کند. اسکار خودش را جای باب وانمود کرده و با آلیس مبادله کلید می کند. او همین کار را نیز با باب انجام می دهد. هر وقت که باب پیام رمز شده ای برای آلیس می فرستد از کلید مبادله شده با اسکار استفاده می کند. ولی او فکر می کند که این کلید تماس آلیس است. اسکار پیام دریافت شده را باز کرده و با ایجاد تغییرات دلخواه در آن برای آلیس می فرستد. برای حل مشکل حمله مردی در میانه برای پروتکل تبادل کلید دیفی – هلمن باید در انتهای پروتکل، احراز اصالت طرفین تایید شوند[5].

۱۰- خم های بیضوی

درمقاله از روش رمزنگاری خم های بیضوی (Elliptic curve cryptography) استفاده می شود که اولین بار زمانی کشف شد که گروهی در حال ایجاد روشی برای اندازه گیری مساحت بیضی بودند. این بررسی ریاضی دانان را به سمت معادلاتی با خواص ویژه هدایت کرد که از آنها می شد به راحتی در رمزنگاری استفاده کرد. این خم ها معادلاتی به شکل عمومی $y^2+axy+by=x^3+cx^2+dx+e$ هستند. در این معادله a ، b ، c ، d و e اعداد حقیقی هستند که باید شرایط ساده ای را ارضاء کنند[1].

در این خم ها به یک نقطه صفر یا نقطه در بی نهایت نیاز است که با O نمایش داده می شود. اگر سه نقطه از خم روی یک خط راست قرار گیرد، مجموع آنها برابر O خواهد بود. فرضهای زیر موجب می شوند تا روابط محاسباتی مورد نیاز فراهم شود:

۱) O عضو خنثی جمع است، یعنی O- = O و در نتیجه برای هر نقطه P رابطه P + O = P برقرار است.

۲) اگر خط عمودی خم را در نقاط P , Q قطع کند در این صورت مختصات x آن دو نقطه یکی خواهد بود، آن گاه فرض می شود خط منحنی را در نقطه O نیز قطع می کند. بنابراین P + Q + O = O یعنی P = -Q.

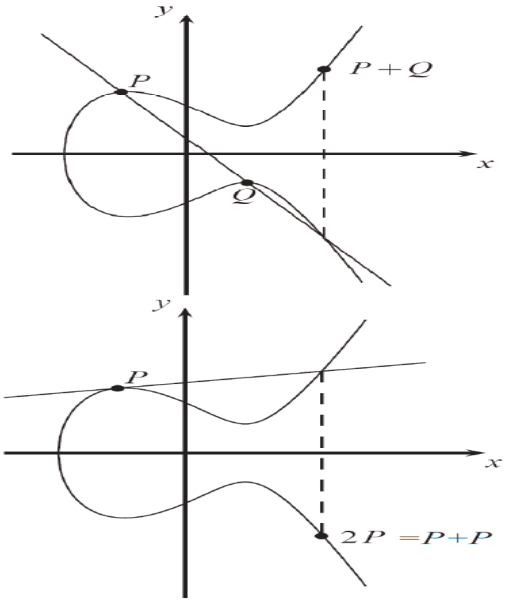
به عبارت دیگر منفی نقطه ای مانند P نقطه دیگری است با x یکسان ولی y منفی شده.

۳) برای جمع دو نقطه P و Q (که x های متفاوتی دارند) یک خط رسم می کنیم که از آن دو نقطه بگذرد. با فرض اینکه خط فوق مماس بر منحنی نباشد، حتما" آن را در نقطه ای مانند R نیز قطع می کند. (شکل ۱ بالا) پس خواهیم داشت:P + Q + R = O. یعنی P + Q = -R.

۴) برای دو برابر کردن نقطه P، یک خط مماس بر منحنی در نقطه P رسم می شود و محل تلاقی خط و منحنی (بجز نقطه P) را S می نامیم. (شکل ۱ پائین) آنگاه P+P+S = O یا 2P = -S (این حالت خاصی از خاصیت قبلی است).

خواص جمع از قبیل شرکت پذیری و جابجایی نیز وجود دارند. ضرب نیز به عنوان تعمیم جمع قابل تعریف است.

در الگوریتمهای رمزگذاری از خم های بیضوی در میدانهای متناهی استفاده می شود. در این روش خم را به صورت $y^2 = x^3 + ax + b \bmod p$ در نظر می گیریم(همراه با نقطه O در بی نهایت) که در آن p عدد اول و a و b اعداد صحیح غیرمنفی هستندکه در رابطه $4a^3+27b^2\neq 0 \bmod p$ صدق می کنند.



شکل ۱: روابط محاسباتی خم های بیضوی [۱].

قاعده جمع در $E_p(a,b)$ مشابه حالت کلی است یعنی:

الف) $P + O = P$

ب) اگر $P = (x,y)$ آنگاه $P + (x,-y) = O$ پس $-P = (x,-y)$

ج) اگر $P = (x_1,y_1)$ و $Q = (x_2,y_2)$ ، $P \neq Q$ آنگاه $P + Q = (x_3,y_3)$ به طوریکه داریم :

$$\left(c = \frac{y_2 - y_1}{x_2 - x_1} P \neq Q\right) \text{یا} \left(c = \frac{3x_1^2 + a}{2y_1} P = Q\right)$$

اگر

$$x_3 = c^2 - x_1 - x_2 \mod p$$
$$y_3 = c(x_1 - x_2) - y_1 \mod p$$

ضرب نیز به صورت تکراری از جمع قابل تعریف است.

جمع و ضرب در رمزنگاری خم های بیضوی متناظر با ضرب و توان در رمزنگاری کلید عمومی RSA (Ron Rivest, Adi Shamir and Leonard Adleman) است. متناظر با تجزیه (Factoring) اعداد در RSA باید یک مساله سخت برای رمزنگاری خم های بیضوی پیدا کرد. به عنوان مثال اگر $P,Q \in E_p(a,b)$ دراین صورت با دانستن $k < P$ و P آنگاه $Q = kP$ به سادگی محاسبه می شود، اما با دانستن P و Q پیدا کردن k ساده نیست[6].

۱۱- پروتکل توزیع کلید مبتنی بر خم های بیضوی

مراحل توزیع کلید در این روش مانند روش دیفی- هلمن است و به صورت زیر بیان می شود[6]:

الف) عدد اول p(حدود 2^{180}) و دو عدد a و b انتخاب شود $E_p(a,b)$.

ب) یک نقطه مولد مانند $G = (x_1,y_1)$ در $E_p(a,b)$ انتخاب شود. توجه باید شود که کوچکترین مقدار n که در رابطه $nG = O$ صدق می کند باید یک عدد اول بزرگ باشد. $E_p(a,b)$ و G پارامترهای توزیع کلید هستند.

مراحل توزیع کلید بین A و B به صورت زیر است:

۱) A عدد $n_A < n$ را انتخاب می کند و سپس $P_A = n_A \times G$ را به B می فرستند.

۲) B عدد $n_B < n$ را انتخاب می کند و سپس $P_B = n_B \times G$ را به A می فرستند.

۳) A کلید جلسه را به این صورت محاسبه می کند.
$K = n_A \times P_B$

۴) B کلید جلسه را به این صورت محاسبه می کند.
$K = n_B \times P_A$

بدیهی است که $n_B \times P_A = n_A \times P_B$.

با توجه به اینکه کلید جلسه به صورت (x ، y) است، معمولا" x یا تابعی از x به عنوان کلید در نظر گرفته می شود[14].

۱۲- ابر خم های بیضوی

تعریف ۱ - فرض کنیم $\overline{F}$ بستار جبری میدان F می باشد. یک ابر خم بیضوی از درجه یا جنس (Genus) g $(g \geq 1)$ بر روی F برابر است با معادله: (۱) $C: y^2 + h(x)y = f(x)$ بطوریکه داریم $C \in F[x,y]$ و $h(x) \in F[x]$ یک چند جمله ای حداکثر از درجه g، $f(x) \in F[x]$ یک چند جمله ای تکین از درجه 2g+1 می باشند و ضمنا" این معادله و نیز معادلات مشتقات جزیی آن یعنی $2y + h(x) = 0$ ، $h'(x)y - f'(x) = 0$ دارای جواب مشترک بر روی $\overline{F}$ نمی باشند. نقطه $(x,y) \in \overline{F} \times \overline{F}$ بر روی منحنی C را یک نقطه منفرد (Singular) می نامیم هر گاه این نقطه

بطور همزمان جواب هر سه معادله اشاره شده در بالا باشد[7].

تعریف ۲ - فرض کنیم L یک میدان گسترش یافته از میدان F باشد. مجموعه C(L) شامل همه نقاط گویا (Rational) بر روی C عبارت است از همه نقاط P = (x,y)∈ L × L بطوریکه در رابطه (۱) صدق می کنند به همراه یک نقطه در بی نهایت که با ∞ نمایش داده می شود. مجموعه $C(\overline{F})$ بطور خلاصه C نامیده می شود[7].

تعریف ۳ - فرض کنیم P = (x,y) یک نقطه متناهی بر روی منحنی C باشد.

نقطه مقابل P برابر $\tilde{P}$ = (x,-y-h(x)) می باشد بطوریکه $\tilde{P}$ بر روی C است. ضمنا" نقطه مقابل ∞ را برابر خودش در نظر می گیریم. اگر یک نقطه متناهی P در شرط $P = \tilde{P}$ صدق کندآنرایک نقطه مخصوص می نامیم ودرغیراینصورت آنرایک نقطه معمولی تعریف می کنیم[7].

مساله لگاریتم گسسته ابرخم های بیضوی – P و Q در $J(F_p)$ هستند، مساله لگاریتم گسسته ابر خم های بیضوی عبارت است از: پیدا کردن یک عدد صحیح m که در P=mQ صدق کند[8].

۱۳- مزیت استفاده از ابر خم های بیضوی

در رمزنگاری کلید عمومی برای جایگزینی سیستم های مبتنی بر مساله تجزیه اعداد از سیستم های مبتنی بر مساله لگاریتم گسسته استفاده می شود. در واقع رمزنگاری مبتنی بر خم های بیضوی بعلت اینکه طول کلید را بطور محسوسی نسبت به سیستم های شبه RSA کاهش می دهند، بسیار مورد توجه طراحان سیستم های رمزنگاری قرار گرفتند. طراحان همیشه نیازمند دستیابی به سیستم های رمزنگاری با طول کلید کمتر و سطح امنیتی بالاتر می باشند به همین دلیل آنها به سمت استفاده از ابر خم های بیضوی در رمزنگاری کشیده شدند. در سال ۱۹۸۹ کوبلیتز[9] پیشنهاد استفاده از ابر خمهای بیضوی به عنوان جایگزینی برای خم های بیضوی به منظور طراحی سیستم های رمزنگاری مبتنی بر مساله لگاریتم گسسته ارائه داد. ابر خم های بیضوی تعمیم یافته خم های بیضوی می باشند. به عبارت دیگر یک خم بیضوی یک ابر خم بیضوی از درجه (جنس) یک می باشد. کوتاه بودن طول کلید مزیت اصلی استفاده از ابر خم های بیضوی می باشد. بدین معنی که یک ابر خم بیضوی در مقایسه با یک خم بیضوی برای رسیدن به یک سطح امنیتی نیازمند میدان متناهی کوچکتری می باشد. بعبارت دیگر مرتبه گروه حاصل از تعریف یک ابر خم بیضوی از درجه g بر روی میدان متناهی با q عنصر برابر q^g می باشد. بنابراین برای ساختن یک گروه از مرتبه 2^{160} با استفاده از خم های بیضوی ما نیازمند یک میدان متناهی با 2^{160} عضو می باشیم در حالیکه برای ساختن یک گروه با اندازه مذکور با استفاده از خم های بیضوی از درجه ۲ فقط نیازمند یک میدان متناهی با 2^{80} عضو می باشیم. به همین صورت برای ابر خم های بیضوی از جنس ۳ و ۴ به ترتیب نیازمند یک میدان متناهی با 2^{53} ، 2^{51} می باشیم[7]. البته با توجه به تحقیقات انجام شده بر روی ابر خم های بیضوی از درجه ۴ و بالاتر آشکار شده است که این نوع خم ها دارای سطح امنیتی کمتری می باشند[10]. بر خلاف خم های بیضوی که ما برای حل مساله لگاریتم گسسته امکان استفاده از الگوریتم حساب راهنما (Index calculus) را نداریم در ابر خم های بیضوی امکان استفاده از این حمله وجود دارد که این نقطه ضعف این خم ها در برابر خم های بیضوی می باشد. با توجه به اینکه انجام محاسبات بر روی ابر خم های بیضوی پیچیده تر می باشد، بنابراین مهمترین موارد عملی ساختن سیستم های رمزنگاری مبتنی بر این نوع خم ها عبارتند از :

الف) پیدا کردن ابر خم های مناسب.

ب) بهبود محاسبات ابر خم های بیضوی.

امروزه بطور کاملا" کارایی می توانیم ابر خم های از درجه ۲ و ۳ را بدست آوریم بطوریکه گروه حاصل دارای مرتبه تقریبا" اول باشد[11].

۱۴- توافق کلید گروهی برای شبکه های موردی

برای حفاظت از اطلاعات مهمی که بین دو قسمت یک شبکه ناامن انتقال می یابد باید از کلید مخفی مشترک استفاده کنیم. به کمک پروتکل های توافق کلید می توانیم کلید مخفی مشترک مورد نیاز را تولید کنیم و بدین وسیله امنیت بالای مطلوب شبکه های اطلاعاتی مدرن را فراهم می کنیم. همزمان با رشد استفاده از شبکه های کامپیوتری نیاز به طراحی پروتکل های امن و کارآتر در زمینه رمزنگاری بسیار بیشتر احساس شده، پروتکل های تعیین هویت و توافق کلید از جمله این پروتکل ها می باشند که برای استفاده از سرویس های اینترنت مانند تجارت الکترونیکی بسیار پر کاربرد می باشند. امروزه روش های ساختن یک کلید مخفی مشترک امن و کارآ یکی از موضوعات مهم تحقیقاتی می باشد. برای طراحی یک پروتکل تعیین هویت روش های مختلفی وجود دارد که از جمله قویترین این روش ها می توان به روش چالش – واکنش (Challenge - response) اشاره کرد[5]. در این روش احراز اصالت کننده یک سوال از طرف مقابل (شخص ثابت کننده) می پرسد. شخص ثابت کننده جواب سوال را با استفاده از کلید محرمانه خود محاسبه و حاصل را برای احراز اصالت کننده می فرستد. شخص احراز اصالت کننده با استفاده از این جواب در مورد صحت ادعای شخص مقابل تصمیم می گیرد. یکی از ویژگی های مهمی که طراحان این گونه پروتکل ها به دنبال آن می باشند خاصیت اثبات با اطلاع صفر می باشد. بدین معنی که شخص ثابت کننده بتواند ادعای خود (هویت خود) را به شخص احراز اصالت کننده ثابت کند بدون اینکه امنیت کلید خصوصی خود را از دست بدهد.

برای رسیدن به این منظور پروتکل های تعیین هویت از نوع چالش – واکنش مبتنی بر سیستم کلید عمومی بسیار مفید می باشند. تا کنون چندین ویژگی امنیتی برای پروتکل های توافق کلید ذکر شده است که مهمترین آنها عبارتند از:

۱۴-۱- **امنیت کلید شناخته شده** (Known-key security): این ویژگی بیان می دارد که اگر مهاجم به یک کلید نشست دسترسی پیدا کند توانایی بدست آوردن کلیدهای نشست بعدی را نداشته باشد[12].

۱۴-۲- **امنیت رو به جلو** (Forward secrecy): این ویژگی امنیتی بیان می دارد که در صورت آشکار شدن کلید های خصوصی طولانی مدت کاربران امنیت کلید های نشست قبلی به خطر نیفتد. اگر با آشکار شدن کلید خصوصی طولانی مدت یکی از کاربران، محاسبه کلید های نشست قبلی ممکن نباشد اما با داشتن کلیدهای خصوصی طولانی مدت هر دو طرف چنین امکانی وجود داشته باشد گوئیم پروتکل دارای امنیت رو به جلو جزئی (Partial forward secrecy) است. در صورتی که با داشتن کلید های خصوصی طولانی مدت هر دو طرف نیز محاسبه کلید های نشست قبلی امکان پذیر نباشد گفته می شود پروتکل دارای امنیت رو به جلو کامل (Perfect forward secrecy) است[13].

۱۴-۳- **امنیت در مقابل جعل هویت با کلید آشکار شده** (Key-compromise impersonation): در صورت آشکار شدن کلید خصوصی طولانی مدت طرف A، مهاجمی که این کلید را در اختیار دارد نتواند خود را بجای طرف B به A معرفی کند.

۱۴-۴- **امنیت کلید ناشناخته** (Unkown key security): فرض کنید A و B در حال اجرای پروتکل توافق کلید هستند. مهاجم فعال C نباید بتواند به نحوی در اجرای پروتکل دخالت کند تا بعد از اتمام پروتکل، A بر این باور باشد که با B توافق کلید انجام داده اما B معتقد است با C یک کلید محرمانه مشترک ساخته است.

۱۴-۵- **حمله مردی در میانه**: فرض کنید A و B در حال اجرای پروتکل توافق کلید هستند. در این حمله مهاجم فعال C به نحوی در اجرای پروتکل دخالت می کند تا سبب شود طرفین پروتکل روی کلید های متفاوتی توافق کنند.

۱۴-۶- **احراز اصالت کلید ضمنی** (Implicit key authentication): یک پروتکل توافق کلید دارای ویژگی تائید کلید ضمنی است اگر طرفین پروتکل مطمئن باشند که فقط طرف مقابل آنها توانائی محاسبه کلید نشست را دارد[12].

۱۴-۷- **احراز اصالت کلید صریح** (Explicit key authentication): یک پروتکل توافق کلید دارای ویژگی تائید کلید صریح است اگر طرفین پروتکل مطمئن باشند که طرف مقابل آنها کلید نشست را محاسبه کرده است.

۱۴-۸- **امنیت قوی** (Strong security): این ویژگی بیان می کند که امنیت پروتکل در صورت دسترسی مهاجم به هر یک از زوج های (کلید خصوصی طرف A، کلید خصوصی طرف B) یا (کلید خصوصی طرف B، مقدار تصادفی تولیدی طرف A) یا (کلید خصوصی طرف A، مقدار تصادفی تولیدی طرف B) یا (مقدار تصادفی تولیدی طرف A، مقدار تصادفی تولیدی طرف B) نیز به خطر نیفتد[13].

۱۵- بحث مقدماتی برای پروتکل توافق کلید گروهی برای شبکه های موردی مبتنی بر ناحیه

شبکه های موردی سیار (Mobil adhoc network) به دلایل نظامی در ابتدا برای کاربردهای نظامی وجود آمدند ولی به سرعت در سایر کاربردهای تجاری نیز به کار گرفته شدند[16]. شکل ۲ نمونه ای از کاربرد شبکه های موردی.



شکل۲: سناریو میدان نبرد [14]

در ارتباطات گروهی در این شبکه ها با فرستادن اطلاعات به طور همزمان به چندین مقصد، به جای آنکه n انتقال برای n عضو، مانند ارتباطات نقطه به نقطه صورت گیرد، تنها یک ارسال برای دستیابی تمام اعضا مورد نیاز است. استاندارد های موجود برای ارسال اطلاعات به چند مقصد به طور همزمان نیازمند سازوکارهایی برای محافظت در برابر شنود (sniffing)،جعل (spoofing)، سرقت نشست (Session hijacking) هستند. بنابراین استفاده از ارسال چند پخش (Multi cast) بدون در نظر گرفتن ویژگی های امنیتی این تهدید را ایجاد می کند که داده ها دست کاری، سرویس و محتواهای ارسالی دزدیده شود.

یک روش برای امن کردن تمام پیام های گروهی، استفاده از رمزنگاری کلید عمومی است. ولی الگوریتم های رمزنگاری نامتقارن یا کلید عمومی از نظر محاسباتی ۱۰۰۰ برابر کندتر از الگوریتم های رمزنگاری متقارن هستند[1]. علاوه بر آن، برای امن کردن ارتباطات بین یک گروه با n کاربر با استفاده از این تکنیک، هر عضو باید n-1 کلید عمومی تائید شده را ذخیره کند. به علاوه اگر هر کاربر بخواهد یک پیام امن را به هریک از کاربران گروه ارسال کند، باید پیام های زیادی را (به تعداد دریافت کنندگان) رمز وارسال کند، این نتایج منجر به هزینه زیاد محاسباتی و مخابراتی گسترده می شود. روش دیگر، استفاده از رمزنگاری کلید متقارن توسط یکی از دو روش زیر است:

الف) کلیدی که دو به دو به اشتراک گذاشته شده باشد.

ب) استفاده از یک کلید مشترک گروهی

استفاده از کلید های دو به دو مشترک از نظر حافظه و تعداد فرآیندهای رمزنگاری و ارسال مورد نیاز مانند روش رمزنگاری کلید عمومی، روش موثر و کارآمدی نمی باشد و استفاده از کلید گروهی مشترک به نظر راه حل مناسبی می باشد.

استفاده از رمزنگاری کلید متقارن مبتنی بر کلید گروهی مشترک نیازمند تولید و توزیع چنین کلیدی به تمام اعضای مجاز گروه می باشد. با در نظر گرفتن اینکه اگر تمام اعضای

گروه بر یک کلید نشست مشترک گروهی به توافق برسند، تمام پیام های گروه با استفاده از این کلید به اشتراک گذاشته شده، می توانند رمز شوند.

اگر فرض شود که مهاجم از هیچ طریقی امکان دسترسی به کلید گروهی را نداشته باشد، آنگاه ارتباط بین اعضای گروه محافظت شده است. بنابراین یکی از چالش های اصلی طراحی در سامانه های ارتباطی گروهی امن و قابل اعتماد، ایجاد یک کلید گروهی مشترک قابل دسترسی برای تمام اعضای گروه از طریق یک روش امن و کارآمد می باشد[17].

۱۶- پیشنهاد پروتکل توافق کلید گروهی برای شبکه های موردی مبتنی بر ناحیه با استفاده از رمزنگاری با ابر خم های بیضوی

۱۶-۱- مقدمه

امنیت در شبکه های موردی بی سیم یکی از چالش های اصلی است. ایجاد توافق کلید گروهی. برای ارتباطات گروهی امن در شبکه های موردی در این راستاست. در این روش یک کلید مشترک برای تمام اعضای گروه لازم است. تغییرات این کلید مذکور به هنگام افزایش عضو جدید به گروه و یا حذف یک عضو فعال از گروه می بایستی این کلید مشترک به هنگام سازی شود. در این مقاله یک پروتکل پیشنهاد می شود که امن، مقیاس پذیر و کارآمد و مبتنی بر ناحیه برای توافق کلید گروهی در شبکه های موردی و بی سیم و پویا است. این پروتکل توسط ساختار دولایه ای و شمای جدید تغییر کلید گروهی پیاده سازی می شود. ایده این است که گروه به زیر گروه هائی ناحیه بندی می شود، و هر زیر گروه در درون خودش از روشی درون گروهی مبتنی بر ابر خمهای بیضوی دیفی - هلمن پیروی می کند. برای ارتباطات بین گروهی، روش برون گروهی از یک ساختار درختی مبتنی بر ابر خمهای بیضوی دیفی - هلمن پیروی می کند. این پروتکل با رویکرد مبتنی بر ناحیه، تعداد پیامهای به روزرسانی را کاهش داده، باعث می شود بار محاسباتی بین میزبان های هر زیر گروه توزیع شود.

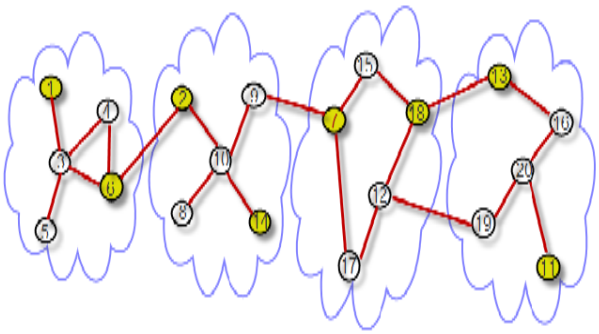
۱۶-۲- انگیزه

برای ایجاد یک پروتکل کلید گروهی کارآ در ارتباطات و محاسبات، یک پروتکل توافق کلید گروهی برای شبکه های موردی مبتنی بر ناحیه با استفاده از ابر خم های بیضوی پیشنهاد می شود که باعث می شود نسبت به پروتکل های با ساختار مشابه از قدرت پردازشی، حافظه مصرفی، انرژی مصرفی شبکه به نحو موثرتری استفاده گردد.

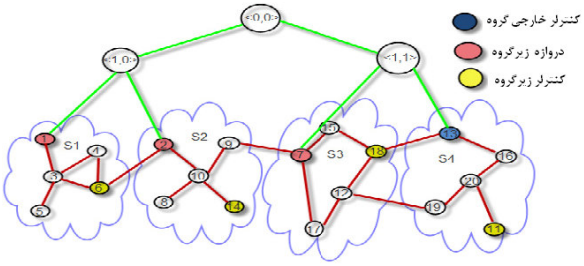
۱۶-۳- مدل سیستمی

هدف این مقاله پیشنهاد یک پروتکل استقرار کلید گروهی کارآ برای ارتباطات و محاسبات در شبکه های موردی است. ایده به این صورت است که چند پخشی گروهی پیامها بین زیر گروه ها تقسیم شود. هر زیر گروه برای خود یک کلید مشترک برای همه اعضاء زیر گروه دارد. هر زیر گروه یک گره کنترلر و یک گره دروازه دارد. در هر زیر گروه گره کنترلر (Controller) زیر گروه کنترل کننده زیر گروه است و گره دروازه (gateway) کنترل کننده کنترلر های زیر گروه هاست.(یا اینکه کل گروه توسط دروازه کنترل می شود.)

برای مثال در شکل ۳، هر عضو به تعدادی زیر گروه تقسیم می شوند و همه زیر گروه ها توسط یک ساختار درختی همچون شکل ۴ به هم متصل می شوند.

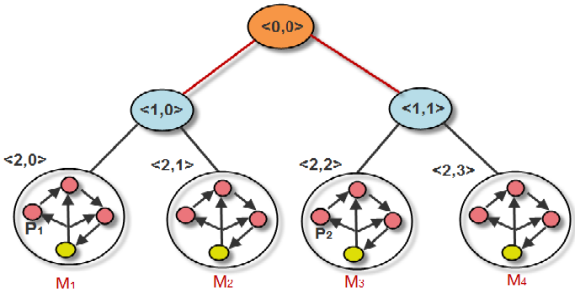


شکل۳: تقسیم اعضاء گروه به زیر گروه ها[15]



شکل۴: پیوند زیر گروه ها با ساختار درختی[15]

هر زیر گروه دارای کلید زیر گروه خود است که این کلید برای همه اعضای گروه به اشتراک گذاشته می شود.هر زیرگروه دارای گره کنترلر گروه است که در آن زیر گروه، کنترل کننده زیر گروه است و آخرین عضوی است که به گروه پیوسته است و گره دروازه برای اتصال زیر گروه ها به هم مورد بهره برداری گره های عضو گروه قرار می گیرد. گره دروازه در گروه دارای بیشترین قدرت پردازشی، حافظه، باطری انرژی است. تمام گره های عضو به تعدادی از زیر گروه و تمام زیر گروه ها در یک ساختار درختی طبقه بندی می شوند.همانطور که در شکل ۵ نشان داده شده است[14].



شکل۵: تقسیم گروه به زیر گروهها[15]

۱۶-۴- الگوریتم

الگوریتم پروتکل توافق کلید مبتنی بر ناحیه به شرح است:

الف) فرمت دهی زیرگروه ها

تعداد اعضاء هز زیر گروه $N / S < 100$ است.

در جایی که N اندازه گروه است و S تعداد زیر گروه ها است.

با فرض این که در هر زیر گروه به همان تعداد عضو وجود دارد.

ب) پروتکل توافق کلید موثر در میان اعضاء گروه پیاده سازی می شود. توسط سه فاز ذیل:

۱) پیدا کردن کنترل کننده زیر گروه برای هر زیر گروه.

۲) پروتکل مدیریت توافق کلید گروهی دیفی – هلمن مبتنی بر ابر خمهای بیضوی استفاده میکند از یک کلید عمومی تولید شده برای هر زیر گروه.

۳) هر کنترل کننده گروه (داخلی یا خارجی) کلید عمومی محاسبه شده را به همه اعضاء توزیع می کند.

۱۶-۵- پویایی شبکه

طبیعت ذاتی شبکه پویایی آن است. یعنی تعدادی از اعضاء به شبکه متصل می شوند و تعدادی نیز شبکه را ترک می کنند. به هر نحو، سیستم مدیریت کلید گروهی می بایستی امنیت شبکه را حفظ نماید. شرایط گوناگونی برای این پروتکل متصور است که در ذیل به آنها می پردازیم:

۱۶-۵-۱- یک عضو به شبکه متصل می شود.

وقتی گره ای به شبکه متصل می شود در ابتدا به عنوان کنترلر زیر گروه در نظر گرفته می شود. پس از این کار، کنترلر زیر گروه قبلی مجوزش و کلید عمومی خود را به این عضو جدید می فرستد. این عضو جدید کلید عمومی را دریافت کرده و به عنوان کنترلر زیرگروه فعالیت اش را آغاز می کند. سپس کنترل جدید زیر گروه کلید جدید زیر گروه را تولید می کند. و سپس کلید تولید شده جدید را به همه اعضاء زیر گروه به صورت چند پخشی ارسال می کند.

۱۶-۵-۲- یک عضو شبکه را ترک می کند.

وقتی عضوی زیر گروه را ترک می کند.برای حصول به امنیت رو به جلو، عضو ترک کننده به کنترلر زیر گروه اطلاع می دهد. کنترلر زیر گروه مقدار کلید خصوصی اش را تغییر می دهد، سپس مقدار عمومی را محاسبه و مقدار عمومی را به همه اعضاء باقیمانده زیر گروه پخش همگانی می کند.هر عضو دوباره کلید را محاسبه می کند و مجوزش و کلید

عمومی خود را برای محاسبه کلید مشترک زیر گروه برای زیر گروه جدید ارسال می کند.

۱۷- نتیجه گیری

سیستم رمزنگاری RSA یک سیستم استاندارد با کاربردهای متفاوت است. با توجه به بهبود های ارائه شده در این مقاله از جمله سیستم های رمزنگاری مبتنی بر خم های بیضوی و ابر خم های بیضوی در کاربردهایی که با کمبود انرژی، پهنای باند کم، قدرت پردازشی کم، طول کلید کمتر به شدت مواجه هستند (از جمله شبکه های موردی) می توان از جابجایی سیستم های ارائه شده استفاده کرد. همچنین پروتکل توافق کلید گروهی برای شبکه های موردی مبتنی بر ناحیه با استفاده از ابر خم های بیضوی پیشنهاد شده در این، به مراتب بهبود را در حافظه مصرفی، پردازش، پهنای باند، انرژی مصرفی نسبت به پروتکل های قبلی و با ساختار مشابه ارائه می دهد.

سپاسگزاری

امید است در چند ماه آینده در روند اجرای پایان نامه اینجانب در مورد ارزیابی پروتکل پیشنهاد شده در این مقاله کار اصلی ارائه گردد. در اینجا از کلیه اساتید اینجانب در دانشگاه پیام نور علی الخصوص جناب آقایان دکتر مهدی جوانمرد (استاد راهنمای پایان نامه)، دکتر سید علی رضوی ابراهیمی (استاد مشاور پایان نامه)، دکتر احمد فراهی (استاد درس سمینار) تشکر و قدردانی صمیمانه دارم، این مقاله مستخرج از پایان نامه بنده در دانشگاه پیام نور با عنوان "بهبود پروتکل توافق کلید گروهی برای شبکه های موردی مبتنی بر ناحیه با استفاده از ابر خم های بیضوی" است، همچنین بر خود واجب می دانم از تلاش های استاد گرانقدر دانشگاه شهید دکتر بهشتی جناب آقای دکتر سید محمد تقی روحانی رانکوهی در دوران تحصیل کارشناسی صمیمانه تشکر کنم.

مراجع

[1] Christof Paar, Jan Pelzl, *Understanding Cryptography*, Springer, pp. 3-6,19,150-152,239-243, 2010.
[2] Buchmann, Johannnes, *Introduction to cryptography*, Springer, pp. 69-70, 2004.
[3] Menezes, Alfred, *Handbook of applied cryptography*, CRC Press, pp. 41-42, 1997.
[4] Stallings, William, *Cryptography and network security, Fourth Edition*, prentice Hall, pp. 290-300, 2005.
[5] Kumar, K., Nafeesa, B.J., Sumathy, V., *A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Ad Hoc Networks using Chinese Remainder Theorem*, International Journal of Computer Science & Emerging Technologies (IJCSET) Volume 1 Issue 2, pp 72-82, 2010.
[6] Blake ,Seroussi ,Smart, *Advances in Elliptic Curve Cryptography*, London Mathematical Society Lecture Note Series. 317,Cambridge University Press, pp. 242-250, 2005.
[7] Menezes Alfred, Yi-Hong Wu, Robert J. Zuccherato, Balasingham, *An elementary introduction to hyperelliptic curves*, Published as Technical Report CORR 96-19, Department of C&O, University of Waterloo, Ontario,Canada, November 1996.
[8] Hoffstein, Pipher, Silverman, *An Introduction to Mathematical Cryptography*, Springer, pp. 480-483, 2010.
[9] Koblitz N., Hyperelliptic cryptosystems, Journal of Cryptology, pp. 1, 139-150, 1989.
[10] Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology Euro crypt 2000, vol. 1807, Springer-Verlag, Berlin, pp. 19–34, 2000.
[11] Balamohan, Balasingham, Accelerating the scalar multiplication on genus 2 hyperelliptic curve cryptosystems, thesis of master, 3,12, 2009.
[12] Meng-bo Hou,Qiu-liang Xu, *A one-round ID-based authenticated key agreement protocol with enhanced security*, Intelligent Control and Information Processing (ICICIP), pp 194-197, 2011.
[13] Min Xie, Libin Wang, *One-round identity-based key exchange with Perfect Forward Security*, Information Processing Letters 112, pp 587–591, 2012.
[14] Kumar, K., Nafeesa, B.J., Sumathy, V., *Cost Effective Region-Based Group Key Agreement Protocol for Ad Hoc Networks Using Elliptic Curve Cryptography*, Advanced Computing, Networking and Security, Lecture Notes in Computer Science, Volume 7135, pp 505-514, 2012.
[15] Kumar, K., Nafeesa, B.J., Sumathy, V., *A Novel Approach Towards Cost Effective Region-Based Group Key Agreement Protocol for Peer - to - Peer Information Sharing in Mobile Ad Hoc Networks*, International Journal of peer-to-peer networks (IJP2P) Vol.1, No.1, pp 10-28, 2010.
[۱۶] سید عباس کاظمی، احمد فراهی، "مرور و ارزیابی کارآئی سه پروتکل مسیریابی شبکه های موردی سیار در محیط گرید با استفاده از نرم افزار NS2"، مجموعه مقالات پنجمین همایش تخصصی دانشگاه پیام نور استان تهران – مرکز شمیرانات، اردیبهشت ماه ۱۳۹۱.

[۱۷] مرتضی عریفی، محمود گردشی، "ارائه یک پروتکل کارآمد توافق کلید گروهی تصدیق پویا مبتنی بر شناسه"، مجله علمی – پژوهشی علوم و فناوری های پدافند غیر عامل، شماره۲ ،تابستان ۱۳۹۰،ص ۱۵۰-۱۳۹.