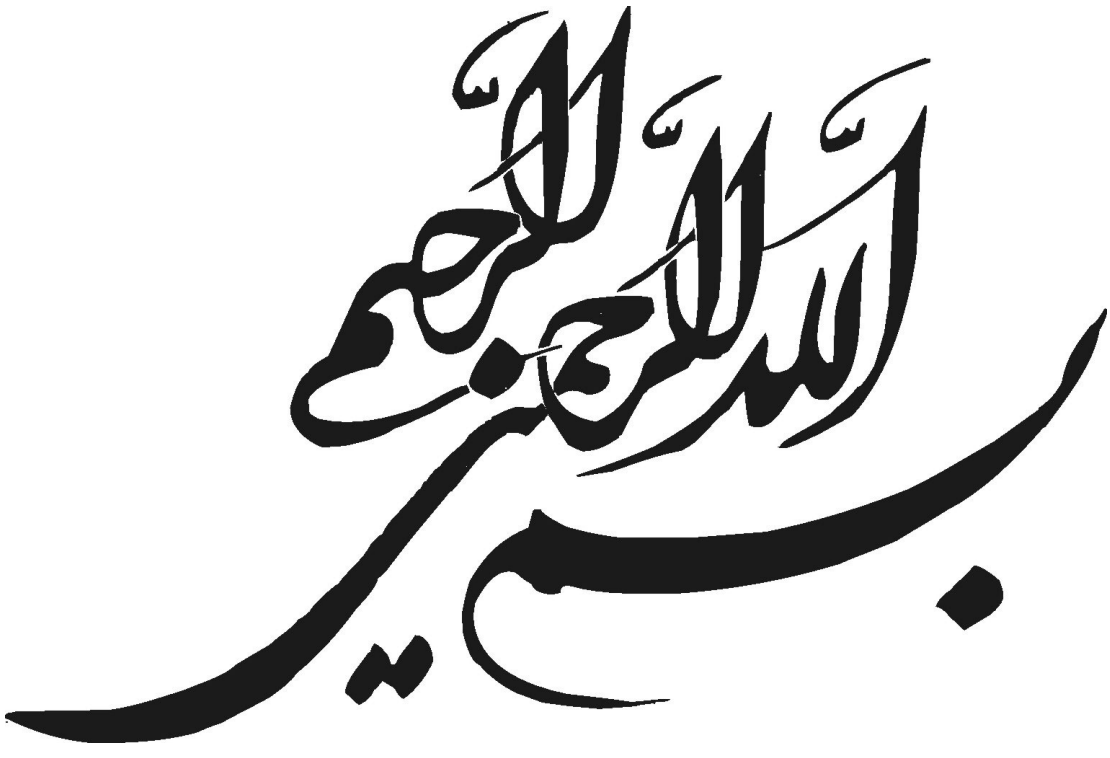
بسم الله الرحمن الرحيم

دانشگاه یزد

دانشکده ریاضی

گروه علوم کامپیوتر

پایان‌نامه

جهت دریافت درجه کارشناسی ارشد

علوم کامپیوتر

روش توزیع کلید تصحیح توأم در شبکه‌های حسگر بی‌سیم

استاد راهنما:

دکتر محمدرضا هوشمنداصل

استاد مشاور:

دکتر رضا رضائیان

پژوهش‌گر:

ندا عزتی

مهر ۱۳۹۲

تقدیم به

پدر و مادرم عزیزم

که از نگاهشان صلابت

از رفتارشان محبت

و از صبرشان ایستادگی را آموختم.

سپاس‌گزاری

سپاس خداوندگار حکیم را که با لطف بی‌کران خود، آدمی را زیور عقل آراست.

در آغاز وظیفه خود می‌دانم از استاد گران‌قدر، جناب آقای دکتر محمدرضا هوشمنداصل، که در تمام مراحل انجام این پروژه راهنمای این‌جانب بودند، صمیمانه تشکر و قدردانی کنم. چرا که ایشان به تمام و کمال رسم استادی را هم در زمینه علمی و هم در کمالات انسانی به‌جای آوردند.

از جناب آقای دکتر رضا رضائیان که زحمت مطالعه و مشاوره این پایان‌نامه را تقبل فرمودند، کمال امتنان را دارم.

همچنین از جناب آقای دکتر سید ابوالفضل شاهزاده‌فاضلی و جناب آقای دکتر فرید (محمد) مالک که داوری این پایان‌نامه را پذیرفتند و این‌جانب را از نظرات سودمند خود بهره‌مند ساختند، سپاسگزارم.

در پایان بوسه می‌زنم بر دستان پدر و مادر عزیزم و بعد از خدا، ستایش می‌کنم وجود مقدس‌شان را و تشکر می‌کنم از خواهران و برادران عزیزم و دوستان مهربانم به پاس عاطفه سرشار و گرمای امید بخش وجودشان، که در این سردترین روزگاران، بهترین پشتیبان من بودند.

چکیده

مدیریتِ ایجاد ارتباط امن بین گره‌های حسگر توسط الگوریتم‌های رمزنگاری، مسئله‌ی بسیار مهمی است و هدف فراهم آوردن روش ارتباط امن بین گره‌ها به صورت پویا است.

پروتکل‌های موجود در شبکه‌های سنتی را نمی‌توان مستقیماً به شبکه‌های حسگر بی‌سیم انتقال داد. این مشکل، ناشی از پویا بودن شبکه‌های حسگر بی‌سیم است و از طرفی احتمال از بین رفتن بسته‌ها در این شبکه‌ها بسیار زیاد است؛ بنابراین لازم است تا برای این نوع شبکه‌ها پروتکل‌های مناسب طراحی شوند. در این نوع شبکه‌ها برای اجرای یک پروتکل رمزنگاری نیاز به توزیع کلید نشست‌ها است و چون بسته‌ی متناظر با کلید ممکن است به عللی از جمله مشکلات شبکه یا خارج شدن از محدوده‌ی شبکه از دست رود؛ در نتیجه از روش توزیع کلید خود تصحیح استفاده می‌شود. در این الگوریتم، هر کاربر می‌تواند تعداد ثابتی پیام فراگیر از دست داده شده را با داشتن اولین و آخرین پیام فراگیر در نشست‌های متوالی که عضو آن بوده است بازیابی کند. هرچند الگوریتم توزیع کلید خود تصحیح، بر دو مشکل پویا بودن شبکه‌های حسگر بی‌سیم و از دست دادن بسته‌ها غلبه کرده است، اما به هر حال دارای محدودیت‌هایی هم است. اهم این محدودیت‌ها عبارت‌اند از ثابت بودن حداکثر تعداد کاربرانی که مدیرِ کلید در هر نشست آن‌ها را از عضویت در آن نشست محروم می‌کند. محدودیت بعدی، در ثابت بودن حداکثر تعداد بسته‌هایی است که یک کاربر می‌تواند در طول نشست‌هایی که عضویت آن‌ها را دارا است از دست بدهد. روش توزیع کلید تصحیح توأم، به دنبال رفع کردن دو محدودیت ذکر شده است که در این پایان‌نامه به این موضوع پرداخته می‌شود.

فهرست مطالب

فصل ۱

مقدمات

۱.۱ رمزنگاری

در این فصل مفاهیم مورد نیاز مطرح می‌شوند.

یک سیستم رمزنگاری از دو سیستم رمزگذاری و رمزگشایی تشکیل شده است. منظور از رمزنگاری[۱]، الگویی ریاضی یا منطقی برای تأمین امنیت در تبادل اطلاعات است. رمزنگاری، الگوریتمی برای تغییر پیام است به‌طوری که تنها، شخصی که از کلید و الگوریتم مطلع است بتواند پیام اصلی را از پیام رمز شده به‌دست آورد و شخصی که از یک یا هر دو آن‌ها اطلاعی ندارد نتواند به‌آسانی به پیام اصلی دسترسی پیدا کند. **رمزگذاری** عملیاتی است که طی آن اطلاعات اولیه (که به آن متن آشکار گفته می‌شود) با استفاده از یک الگوریتم (که الگوریتم رمز نامیده می‌شود) و یک کمیت محرمانه (که به آن کلید رمز گفته می‌شود) به متن غیر قابل فهم دیگری (که به آن متن رمز گفته می‌شود) تبدیل می‌شود به‌نحوی که بدون دسترسی به کلید رمز، دستیابی به اطلاعات اولیه از روی متن رمز شده غیر ممکن باشد. به عملیات معکوس رمزگذاری، **رمزگشایی** گفته می‌شود که به معنای بازیابی متن آشکار با دانستن و استفاده از کلید رمز است.

الگوریتم‌های رمزنگاری متعددی وجود دارند که می‌توان آن‌ها را در دو دسته کلی متقارن و نامتقارن دسته‌بندی کرد. در الگوریتم‌های رمزنگاری متقارن [۲]، کلید مورد استفاده برای رمزگذاری و رمزگشایی پیام یکسان است. اما در الگوریتم‌های رمزنگاری نامتقارن[۳]، از دو کلید استفاده می‌شود. یکی از این کلیدها که تنها، می‌توان با آن پیامی را رمز کرد، کلید عمومی و دیگری را که تنها با استفاده از آن می‌توان پیام رمز شده‌ای را رمزگشایی کرد، کلید خصوصی می‌نامند. لازم به ذکر است که کلید عمومی می‌تواند در اختیار همگان قرار گیرد، اما کلید خصوصی در نزد صاحب آن به صورت محرمانه برای رمزگشایی نگه‌داری می‌شود. به‌علاوه محاسبه‌ی کلید خصوصی با استفاده از کلید عمومی کاری بسیار مشکل و هزینه‌بر است.

پروتکل[۴] عبارت است از قراردادی که بین طرفین یک نشست مورد توافق قرار می‌گیرد و برای برقراری ارتباط از آن استفاده می‌شود.

---

[۱] Cryptography

[۲] Symmetric Key Cryptographic Algorithms

[۳] Unsymmetric Key Cryptographic Algorithms

[۴] Protocol

به صورت کلی سه نوع روش انتقال داده وجود دارد:

۱. نقطه به نقطه[۵] یا تک پخشی[۶]: داده‌های ارتباطی از طریق اتصالات و گره‌های[۷] میانی به طور مستقیم بین یک مبدأ و یک مقصد مبادله می‌شوند.

۲. چند پخشی[۸]: داده‌های ارتباطی از طریق اتصالات و گره‌های میانی به طور مستقیم بین یک و چند مقصد و نه همه‌ی گره‌های شبکه مبادله می‌شوند.

۳. پخشی عمومی[۹]: به آن داده پراکن نیز می‌گویند و در آن همه‌ی کاربران به یک کانال مشترک متصل شده‌اند و داده‌ها از طریق آن کانال منتشر می‌شوند و تمام کاربران به داده‌های روی کانال دسترسی دارند. مانند: انتشار رادیویی

متحد شدن گروهی برای دستیابی به هدفی یکسان را **ائتلاف**[۱۰]، گویند.
تَبانی[۱۱]، نوعی از ائتلاف است که گاهی اوقات به صورت سری و غیر قانونی و گاهی با فریب‌کاری، اغفال، کلاهبرداری از حقوق قانونی افراد و گاهی توسط قانون خاص یا به‌دست آوردن مزایای غیر منصفانه صورت می‌گیرد. درمدت زمانی معین تمامی اعمال تحت تاثیر تبانی قرار می‌گیرند.

۲.۱ نظریه‌ی گروه، حلقه و میدان

تعریف ۱.۲.۱. (گروه) ([۲۰]) فرض کنید G یک مجموعه نا تهی است و $\oplus$ یک عمل دو تایی روی G باشد. G تحت عمل $\oplus$ تشکیل یک گروه[۱۲] می‌دهد، هرگاه خواص زیر برقرار باشند:

---

[۵] Point to Point

[۶] Unicast

[۷] Node

[۸] Multi-Cast

[۹] Broad-Cast

[۱۰] Coalition

[۱۱] Collusion

[۱۲] Group

۱. بسته بودن نسبت به $\oplus$ یا

$$a \oplus b \in G \qquad \forall a, b \in G$$

۲. شرکت پذیری نسبت به $\oplus$ یا

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c \qquad \forall a, b, c \in G$$

۳. وجود عنصر همانی در G نسبت به $\oplus$ یا

$$\exists\, e \in G, \forall a \in G \qquad a \oplus e = e \oplus a = a.$$

۴. وجود معکوس در G نسبت به $\oplus$ یا

$$\forall a \in G\ \exists\, b \in G \qquad a \oplus b = b \oplus a = 1.$$

در این صورت گروه G تحت عمل $\oplus$ را با دو تایی مرتب $(G, \oplus)$ نمایش می‌دهیم.

تعریف ۲.۲.۱. (مرتبه‌ی یک گروه) مرتبه‌ی یک گروه متناهی G عبارت است از تعداد اعضای مجموعه G که آن را با $|G|$ نشان می‌دهند. اگر $|G|$ متناهی باشد G را یک گروه متناهی و در غیر این صورت، آن را یک گروه نامتناهی می‌نامند.

تعریف ۳.۲.۱. (گروه آبلی) اگر $(G, \oplus)$ یک گروه باشد که دارای ویژگی زیر که به ویژگی جابه‌جایی معروف است باشد، آن‌گاه G را گروه آبلی[۱۳] می‌گویند.

$$a \oplus b = b \oplus a. \qquad \forall a, b \in G$$

تعریف ۴.۲.۱. (زیر گروه) فرض کنید $(G, \oplus)$ یک گروه باشد. اگر H زیر مجموعه‌ای ناتهی از G باشد و H تحت عمل $\oplus$ یک گروه باشد آن‌گاه H را یک زیر گروه[۱۴] G نامند و به صورت $H \leq G$ نشان داده می‌شود.

لم ۵.۲.۱. ([۱۹]) اگر $(G, \oplus)$ یک گروه باشد و $H \subseteq G$؛ آن‌گاه H یک زیر گروه G است، هرگاه به ازای هر $a, b \in H$ داشته باشیم : $a \oplus b^{-1} \in H$.

---

[۱۳] Abelian Group

[۱۴] Subgroup

تعریف ۶.۲.۱. (گروه دوری) فرض کنید G گروهی از مرتبه‌ی m باشد، اگر عضوی مانند g در G پیدا شود، به نحوی که توان‌های متوالی آن به شکل $g^1, g^2, \ldots, g^m$، تمام عناصر G را تولید کند؛ که $g^2 = g \oplus g, \ldots, g^{n+1} = g^n \oplus g$. در این صورت G را گروه دوری[۱۵] نامند.

تعریف ۷.۲.۱. (حلقه) مجموعه ناتهی R به همراه دو عمل دو تایی $\oplus$ و $\otimes$ روی آن را حلقه[۱۶] نامیم، هرگاه شرایط زیر برقرار باشند:

۱. $(R, \oplus)$، یک گروه آبلی باشد. عضو همانی آن را[۰] نامیم.

۲. عمل دوم (یعنی $\otimes$) روی R باید دارای خواص شرکت‌پذیری باشد.

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c. \qquad \forall\, a, b, c \in R$$

۳. عمل دوم بر روی عمل اول دارای خاصیت پخش‌پذیری از چپ و راست باشد.

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c). \qquad \forall\, a, b, c \in R$$

$$(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a). \qquad \forall\, a, b, c \in R$$

۴. عمل دوم نیز باید دارای عضو همانی باشد و آن را با ۱، نشان می‌دهیم. به عبارت دیگر:

$$\exists\, 1 \in R, \forall\, a \in R \qquad a \otimes 1 = 1 \times a = a.$$

تعریف ۸.۲.۱. (حلقه‌ی جابجایی) هرگاه مجموعه $(R, \oplus, \otimes)$، یک حلقه باشد و همچنین عمل دوم آن نیز در شرط جابجایی صدق کند، آن‌گاه به چنین حلقه‌ای، حلقه‌ی جابجایی[۱۷] می‌گویند. یعنی:

$$a \otimes b = b \otimes a. \quad \forall\, a, b \in R$$

تعریف ۹.۲.۱. (میدان)

اگر $(F, \oplus, \otimes)$، یک حلقه‌ی جابجایی باشد و هر عضو F نسبت به عمل $\otimes$ نیز دارای معکوس باشد، به آن

---

[۱۵] Cyclic Group

[۱۶] Ring

[۱۷] Commutative Ring