
بسم الله الرحمن الرحيم

دانشگاه شاهد

دانشکده فنی و مهندسی

**پایان‌نامه دوره کارشناسی ارشد مهندسی فناوری اطلاعات**

# مدیریت کلید در شبکه‌های اقتضایی سیار

**استاد راهنما:**

**دکتر محمد علی دوستاری**

**استاد راهنمای دوم:**

**دکتر سید حمید حاج سید جوادی**

**پژوهشگر:**

**مریم زارع زاده**

**زمستان ۱۳۹۲**

# صفحه صورتجلسه

| | | |
|---|---|---|
| | **اظهار نامه دانشجو** | شماره:<br>تاریخ: |

اینجانب مریم زارع زاده دانشجوی کارشناسی ارشد رشته مهندسی فناوری اطلاعات، گرایش مهندسی فناوری اطلاعات دانشکده فنی و مهندسی دانشگاه شاهد، گواهی می‌دهم که پایان نامه/ رساله تدوین شده حاضر با عنوان؛ "مدیریت کلید در شبکه‌های اقتضایی سیار" به راهنمایی اساتید محترم جناب آقای دکتر محمد علی دوستاری و آقای دکتر سید حمید سید جوادی، توسط شخص اینجانب انجام و صحت و اصالت مطالب تدوین شده در آن، مورد تأیید است و چنان چه هر زمان، دانشگاه کسب اطلاع کند که گزارش پایان نامه/ رساله حاضر صحت و اصالت لازم را نداشته، دانشگاه حق دارد، مدرک تحصیلی اینجانب را مسترد و ابطال نماید هم چنین اعلام می‌دارد در صورت بهره گیری از منابع مختلف شامل؛ گزارش های تحقیقاتی، رساله، پایان نامه، کتاب، مقالات تخصصی و غیره، به منبع مورد استفاده و پدید آورنده آن به طور دقیق ارجاع داده شده و نیز مطالب مندرج در پایان نامه/ رساله حاضر تاکنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب و یا سایر افراد به هیچ کجا ارایه نشده است. در تدوین متن پایان نامه/ رساله حاضر، چارچوب (فرمت) مصوب تدوین گزارش های پژوهشی تحصیلات تکمیلی دانشگاه شاهد به طور کامل مراعات شده و نهایتاً این که، کلیه حقوق مادی ناشی از گزارش پایان نامه/ رساله حاضر، متعلق به دانشگاه شاهد می‌باشد.

نام و نام خانوادگی دانشجو:

امضاء دانشجو:

تاریخ:

# تقديم

# تشکر و قدردانی

# چکیده

شبکه اقتضایی سیار به دلیل مشخصات منحصر به فرد، نیازمند تضمین مدیریت کلیدهای رمزنگاری است. تمرکز رساله بر روی دو جنبه مهم مدیریت کلید در شبکه اقتضایی سیار شامل توزیع کلید و ابطال کلید است. به منظور پیاده‌سازی امن و کارآمد توزیع کلید خصوصی مرکز صدور گواهی با به کارگیری طرح تسهیم راز آستانه‌ای، یک مدل تصادفی برای فرآیند حملات در نظر گرفته شده است. با ارزیابی مدل پیشنهادی، می‌توان مقدار مناسبی برای آستانه و دوره زمانی به‌روز رسانی مقدار محرمانه، تعیین کرد. همچنین، تأثیر مقدار آستانه بر روی امنیت شبکه به کار گیرنده مرکز صدور گواهی توزیع شده، بررسی گردیده است. از سویی دیگر، ماهیت بی‌سیم و پویایی شبکه اقتضایی سیار، آن را برای انواع حملات امنیتی آسیب‌پذیرتر از شبکه سیمی کرده است. در برخی پروتکل‌های ابطال کلید هر گره، شبکه را نظارت می‌کند و با مشاهده گره بدرفتار، بسته اتهام را به مرکز احراز اصالت ارسال می‌کند. سپس مرکز احراز اصالت، براساس تعداد اتهامات دریافتی و پروتکل ابطال کلید، تصمیم‌گیری می‌کند. در این رساله، مقدار مناسبی برای آستانه اتهامات و زمان تصمیم‌گیری در پروتکل‌های ابطال کلید ارائه شده است. تعداد آستانه پیشنهادی در طرح ابطال کلید به کار رفته و نتایج به کمک شبیه‌سازی مورد ارزیابی قرار گرفته‌اند. بررسی‌ها نشان می‌دهد، آستانه اتهامات پیشنهادی عملکرد طرح ابطال کلید را بهبود می‌بخشد.



**کلید واژه:** مدیریت کلید، شبکه اقتضایی سیار، طرح تسهیم راز، ابطال کلید.

# فهرست مطالب

عنوان | صفحه

# فهرست جدول‌ها

**عنوان** **صفحه**

# فهرست شکل‌ها

**عنوان** **صفحه**

# فصل ۱- مقدمه

## ۱-۱- پیشگفتار

درسال‌های اخیر، تکنولوژی بی‌سیم، سبب بوجود آمدن زمینه‌های کاربردی مختلف در حوزه شبکه‌های کامپیوتری شده است. شبکه اقتضایی سیار[1] (MANET)، کاربرد جدیدی از تکنولوژی بی‌سیم را فراهم می‌کند که شامل گره‌های متحرک و بی‌سیم بوده و از هیچ زیرساخت[2] ثابت و متمرکزی برای برقراری ارتباط بین گره‌ها استفاده نمی‌کند. به طور مختصر می‌توان گفت که MANET، ذاتاً پویا است و توپولوژی شبکه به دلیل تحرک گره‌ها، دائماً تغییر می‌کند. MANET نسبت به شبکه‌های دیگر، در مقابل حملات آسیب‌پذیرتر می‌باشد و برقراری امنیت در این نوع شبکه، کار بسیار دشواری است. از این رو، امنیت در شبکه‌های اقتضایی سیار، به طور چشمگیری مورد توجه محققان است.

## ۱-۲- شبکه اقتضایی سیار

شبکه‌های بی‌سیم به دو دسته شبکه‌های با زیرساخت و شبکه‌های سیار بدون زیرساخت[3] تقسیم می‌شود. شبکه‌های سیار بدون زیرساخت، همان شبکه‌های اقتضایی سیار هستند که به ساختارهای ثابت همانند ایستگاه‌های پایه[4]، نیاز ندارند و گره‌ها می‌توانند به صورت تصادفی و دلخواه، به هر طرف حرکت کرده و خود را سازمان‌دهی کنند. بنابراین توپولوژی شبکه، به سرعت تغییر می‌کند. MANET، هم می‌تواند به صورت جداگانه و مستقل کار کند و هم به شبکه اینترنت متصل شود [۱].

برقراری ارتباط بین گره‌ها از طریق امواج رادیویی است. دو گره در صورتی همسایه محسوب می‌شوند که در محدوده رادیویی همدیگر قرار گرفته باشند. هر گره، قادر است با گره‌هایی که در برد رادیویی یکسان قرار دارند، به صورت مستقیم ارتباط داشته باشد. در غیر این صورت، برای برقراری ارتباط با گره‌هایی در خارج از محدوده رادیویی، باید از گره‌های میانی و ارسال گام به گام پیام‌ها استفاده شود. به عبارت دیگر، گره‌ها به عنوان مسیریاب[5] عمل می‌کنند و ترافیک به صورت گام به گام، از گره مبدأ به گره مقصد ارسال می‌شود. از این رو به آن‌ها، شبکه‌های بی‌سیم اقتضایی

[1] Mobile Ad hoc NETwork
[2] Infrastructure
[3] Infrastructureless
[4] Base station
[5] Router

چندگامی[1] نیز گفته می‌شود. این شبکه‌ها در میادین جنگ، در هنگام وقوع حوادثی همچون سیل، زلزله، طوفان، پزشکی و غیره مورد استفاده قرار می‌گیرند.

## ۱-۳- اهمیت امنیت در شبکه

در نیم قرن گذشته بروز تحولات عظیمی در زمینه فناوری اطلاعات و ارتباطات، دگرگونی عمده‌ای را در عرصه‌های مختلف حیات بشری به دنبال داشته است. انسان همواره از فناوری استفاده نموده و حیات بشری مملو از نوآوری و تأثیر فناوری‌های ارتباطات و اطلاعات می‌باشد. از جمله فناوری‌های مهم، شبکه‌های کامپیوتری می‌باشد. علیرغم تمامی مزایا و دستاوردهای این شبکه، دریچه‌ای از تهدیدات امنیتی برای تمامی کاربران، گشوده است. امروزه با گسترش کاربرد شبکه‌های کامپیوتری و وابستگی هرچه بیش‌تر آن به کسب و کار؛ محافظت از اطلاعات، به منزله شاهرگ حیاتی محسوب می‌گردد.

اطلاعات به عنوان یکی از با ارزش‌ترین و حساس‌ترین دارایی‌های سازمان می‌باشد و دستیابی، عرضه به موقع و مناسب اطلاعات مورد نیاز، همواره دارای نقش محوری و سرنوشت‌ساز است. حفظ و نگهداری اطلاعات، شرط لازم برای تداوم فرآیند کسب و کار سازمان‌ها می‌باشد. در معرض آسیب قرار گرفتن داده‌ها و اطلاعات حساس، تجاوز به حریم خصوصی کاربران، استفاده از کامپیوتر کاربران برای حمله به سایر کامپیوترها، از جمله اهداف حمله‌کنندگانی است که با بهره‌گیری از آخرین فناوری‌های موجود، حملات خود را سازماندهی و بالفعل می‌نمایند. با توجه به ماهیت حملات، می‌بایست در انتظار نتایج نامطلوب متفاوتی بود. از این رو باید به موضوع امنیت اطلاعات و ایمن‌سازی کامپیوترها و شبکه‌های کامپیوتری، توجه جدی شود و از فرآیندهای متفاوتی در جهت مقاوم‌سازی آنان، استفاده گردد.

## ۱-۴- انگیزه انتخاب موضوع

در دهه گذشته یا پیش از آن، تکنولوژی‌های موبایل و بی‌سیم پیشرفت گسترده‌ای داشته است. با کاهش هزینه دستگاه‌های قابل حمل همچون تلفن همراه و رایانه کیفی[2]، دسترس‌پذیری به سرویس‌ها و ارتباطات سیار بی‌سیم، گسترش یافته است. به دلیل تبادل اطلاعات مهم و دسترسی به سرویس‌های پرداخت بر روی کانال‌های حفاظت نشده، توسعه امنیت در کاربردهای سیار بی‌سیم ضروری است.

---

[1] Multi-hop
[2] Laptop

نوعی از شبکه که به طور رایج کاربرد دارد، MANET است. در سال‌های اخیر، به دلیل سرعت، سهولت و هزینه کم برای برقراری شبکه، توجه بسیاری به MANET شده است. اما تبادل اطلاعات بر روی MANET به دلیل فقدان زیرساخت مشخص، نیازمند به توسعه مکانیزم‌های امنیتی است.

MANET، به عنوان تکنولوژی و کاربردهای جدید، چالش‌های امنیتی جدیدی را به شبکه محول می‌کند [۲]. MANET، شبکه بی‌سیمی است که تنها از گره‌های متحرک تشکیل شده است. لازم است در MANET تمام گره‌ها خود، یعنی بدون کمک از هیچ موجودیت خارجی یا زیرساخت توسعه یافته، قادر به تشکیل و نگه‌داری شبکه باشند. بعلاوه، گره‌های شبکه باید تمام عملیات شبکه به خصوص مسیریابی[۱] را انجام دهند. ویژگی بیان شده با عنوان خود سازمان‌ده[۲]، مطرح می‌باشد. شبکه‌های اقتضایی، به عنوان مجموعه خود سازمان‌ده از کاربران متحرک، نیاز به پروتکل‌های متفاوت از پروتکل‌های پیشنهادی برای شبکه‌های سیمی یا بی‌سیم متمرکز دارند. ویژگی خود سازمان‌ده با دیگر ویژگی‌های MANET ترکیب و منجر به تشکیل شبکه به روش کم هزینه و سریع شده است.

MANET، با هدف کاربردهای خاص طراحی شده است، به طوری که نیازمند به هیچ گونه ابزار مرکزی همچون مسیریاب‌ها، سیستم‌های تشخیص نفوذ[۳] یا مدیریت اعتماد متمرکز که قسمتی از شبکه باشد، نیست. به عبارتی دیگر در این شبکه‌های اقتضایی، هر گره خود به عنوان فرستنده باید مسیر را به مقصد مورد نظر از طریق گره‌های واسط ناشناخته، شناسایی کند.

به دلیل دارا بودن ویژگی‌های منحصر به فرد، MANET در زمینه‌های مختلف شامل نظامی، دولتی، سلامت و غیرنظامی کاربرد دارد. در ابتدا MANET به منظور کاربرد نظامی، مانند برقراری ارتباط فوری در طی مأموریت‌ها در مناطق جنگی و نقاط آسیب‌پذیر [۳]، طراحی شد. بررسی‌های گسترده بر روی کاربرد نظامی، منجر به استفاده از این نوع شبکه در کلاس‌های درس مجازی، اتصال و خواندن تجهیزات پزشکی در بیمارستان‌ها، اشتراک‌گذاری اطلاعات، خانه‌های هوشمند[۴]، شبکه‌های خصوصی بی‌سیم، شبکه‌های فوری برای کنفرانس و ملاقات، بازی‌های شبکه‌ای و کاربردهای دیگر شده است [۲].

با وجود اینکه کاربردهای نظامی و سلامت نیاز به امنیت زیادی دارد، اما MANET به دلیل لینک‌های ارتباطی بی‌سیم، مستعد حملات مختلفی است و باید هر نوع ارتباط در این شبکه حفظ شود. ارتباطات بی‌سیم، هیچ گونه حفاظت فیزیکی فراهم نمی‌کنند. حمله بر روی این کانال‌ها، به

[1] Routing
[2] Self-organization
[3] Intrusion Detection Systems
[4] Smart buildings

دلیل عدم نیاز به تجهیزات پرهزینه برای دسترسی یا مجاورت به شبکه، به آسانی است. حملات غیرفعال[۱] در MANET همانند شنود[۲] و حملات فعال[۳] از جمله دستکاری[۴]، جعل کردن[۵]، پاسخ دادن[۶]، بازپخش کردن[۷] پیام‌ها و حملات جعل هویت[۸] است. همچنین MANET به دلیل حفاظت فیزیکی ضعیف و دسترس‌پذیری گره‌های متحرک که آن‌ها را برای خطر کشف[۹]، مستعد می‌کند، نیازمند به حفاظت مخصوص می‌باشد [۲].

اهمیت امنیت در شبکه‌های بی‌سیم از آن جهت است که نسبت به شبکه سیمی، به سهولت در معرض شنود قرار دارند و هیچ گونه محافظت فیزیکی از رسانه انتقال وجود ندارد. به عبارتی دیگر، از آنجایی که هر گره در MANET نقش مسیریاب را دارد، امنیت در این شبکه‌ها نسبت به شبکه معمولی، اهمیت دو چندان خواهد داشت. به عنوان نمونه اگر یک گره MANET، در دسترس گره بدرفتار[۱۰] قرار گیرد، ممکن است که گره به عنوان دروازه[۱۱] عمل کرده و در تمام شبکه اختلال ایجاد کند. به عبارت دیگر در شبکه‌های معمولی نیاز به چنین امنیتی نخواهد بود و اغلب در محیط معمولی، درخواست حفظ حریم خصوصی[۱۲] برای حفظ امن اطلاعات شخصی است. به دلیل اینکه ارتباطات اینترنت و بی‌سیم بر روی رسانه انتقال ناامن، منتقل می‌شوند باید مانع شد تا شنودکنندگان و کاربران غیرقانونی پیام‌ها را ضبط کنند. بنابراین باید ارتباطات امن، یک فاکتور حیاتی برای طراحی MANET باشد [۴].

به منظور خنثی کردن شنود لازم است پیام‌های محرمانه[۱۳]، رمز شوند. هر دو رمزنگاری[۱۴] و حفظ صحت داده[۱۵] به کلیدهای رمز نیاز دارند. بنابراین عملکرد و امنیت شبکه، وابسته به نگهداری کلیدهای رمزنگاری است که این کلیدها برای رمز کردن داده‌های مبادله شده، به منظور حفظ محرمانگی[۱۶] داده‌ها به کار می‌رود. در کاربردهای حیاتی از شبکه‌های اقتضایی، حمله‌کنندگان فعال و غیرفعال در تلاش برای کشف برخی اطلاعات خصوصی شبکه یا از بین بردن عملیات شبکه در

---

[1] Passive
[2] Eavesdropping
[3] Active
[4] Modification
[5] Fabricating
[6] Replaying
[7] Relaying
[8] Impersonation
[9] Compromise
[10] Malicious
[11] Gateway
[12] Privacy
[13] Secret
[14] Cryptography
[15] Data integrity
[16] Confidentiality

MANETها می‌باشند. در چنین موقعیتی طراحی پروتکل مدیریت کلید[1]، نقش مهمی در حفظ امنیت شبکه دارد. سرویس‌های امنیتی براساس مکانیزم‌های رمزنگاری، کلیدهای رمزنگاری را فرض می‌کنند که برای طرفین ارتباط قبل از ارتباطات امن، توزیع خواهد شد. مدیریت امن این کلیدها، یکی از مهمترین عناصر ضروری برای کامل کردن توابع رمزنگاری برای سیستم است، زیرا زمانی که مدیریت کلید ضعیف باشد، مفهوم دقیق امنیت، دچار ضعف است [۵].

مدیریت کلید ضروری‌ترین فاکتور ارتباط امن، صرف نظر از کاربرد است. طراحی و پیاده‌سازی هر نوع مکانیزم امنیتی، نیاز به اشتراک‌گذاری مقدار محرمانه (معمولاً کلید رمزنگاری نامیده می‌شود) برای برقراری ارتباط امن بین دو یا بیش‌تر طرفین ارتباط می‌باشد. مدیریت کلیدهای رمزنگاری، نقش حیاتی در فراهم کردن ارتباط امن، قوی و قابل اطمینان ایفا می‌کند [۶].

مدیریت کلید، قسمت اساسی سیستم رمزنگاری است که برای شبکه ارتباطی امن استفاده می‌شود. تأثیر سیستم رمزنگاری، وابستگی شدیدی به کارآیی، نیرومندی و امنیت سیستم مدیریت کلید دارد. به ویژه مدیریت کلید با تولید کلید[2]، توزیع کلید[3]، به‌روز رسانی کلید[4]، ابطال کلید[5] و ارائه سرویس‌های گواهی[6] مطابق با سیاست‌های امنیتی که توسط سازمان تعریف شده، شبکه امن را فراهم خواهد کرد [۷].

راه‌حل‌های مدیریت کلید موجود، در ابتدا براساس توپولوژی‌های شبکه معمولی که سیمی و ثابت هستند، طراحی شده‌اند. زیرساخت فراهم شده در چنین شبکه‌هائی سیمی، مکانیزم‌های اساسی برای مدیریت کلید مؤثر را پشتیبانی می‌کند. در مقابل، شبکه‌های اقتضایی بی‌سیم براساس تعریف، به هیچ عناصر زیرساخت ثابت ندارد. بعلاوه گره‌های شبکه‌های اقتضایی به خصوص شبکه حسگر بی‌سیم[7]، چندین محدودیت مختلف همانند محدودیت حافظه و قابلیت محاسباتی را دارند. این اشکالات ذاتی آن را برای به کار بردن راه‌حل معمولی همانند زیرساخت کلید عمومی[8] (PKI)، دشوار می‌سازد. گره‌های شبکه برای حملات مختلف، آسیب‌پذیر هستند. یک حمله‌کننده تنها باید گره ضعیف را شناسایی و تخریب[9] کند تا به صورت بالقوه، کل شبکه را مختل کند. یک راه برای کاهش این تهدید، پیاده‌سازی راه‌حل رمزنگاری با مدیریت کلید قوی است [۸].

---

[1] Key management
[2] Key generation
[3] Key distribution
[4] Key updating
[5] Key revocation
[6] Certificate
[7] Wireless sensor network
[8] Pubilc Key Infrastructure
[9] Corrupt

## ۱-۵- هدف رساله

از جمله مسائل امنیتی در MANET، مدیریت کلید است که به عنوان مکانیزمی برای پوشش اعتماد بین کاربران به کار می‌رود تا سرویس‌ها و کاربردهای امن را برای شبکه فراهم کند. دو مؤلفه با اهمیت در مدیریت کلید، توزیع کلید و ابطال کلید می‌باشد.

در برخی از طرح‌های توزیع کلید، کلید خصوصی مرکز صدور گواهی با طرح تسهیم راز[۱] آستانه‌ای، در بین n گره توزیع شده است. در این روش تنها با همکاری t گره، کلید مورد نظر بازیابی خواهد شد. تا زمانی که کمتر از t گره در معرض کشف قرار بگیرند، گره بدرفتار نخواهد توانست کلید محرمانه به اشتراک گذاشته را بازسازی کند و همچنان امنیت سیستم فراهم می‌باشد. از این رو در این مدل‌ها، انتخاب مقدار مناسب آستانه t، اهمیت بالایی دارد. هیبنگ[۲] و چانگلان[۳] [۹]، با فرض این که رخداد حملات براساس یک فرآیند پواسون[۴] رخ می‌دهد، روشی برای تعیین مقدار مناسب آستانه، ارائه داده‌اند. اما برای مدل‌سازی حملات، یک ضعف فرآیند پواسون این است که در آن نرخ رخداد حملات، ثابت بوده و به زمان بستگی ندارد. فرآیند پواسون ناهمگن[۵] (NHPP) حالت تعمیم یافته‌ای از فرآیند پواسون است که در آن نرخ رخداد وقایع به صورت تابعی از زمان در نظر گرفته می‌شود [۱۰]. بنابراین، در این رساله قصد داریم رخداد حملات را براساس NHPP، در نظر گرفته و مقدار مناسبی برای t، با استفاده از تحلیل‌های عددی، مورد بررسی قرار دهیم.

یکی دیگر از مسائل مورد توجه، مسئله ابطال کلید است. ابطال کلید، شامل حذف گواهی گره‌هایی است که به عنوان حمله‌کننده بر روی گره‌های مجاور، شناسایی شده‌اند. به عبارتی دیگر اگر گره‌هایی در معرض خطر کشف قرار گرفته یا بدرفتار شناخته شوند، باید فوراً از شبکه و ادامه فعالیت در آن حذف شوند [۱۱]. تاکنون انواع مختلفی از تکنیک‌های ابطال کلید به منظور افزایش امنیت پیشنهاد شده است. روش‌های موجود برای ابطال کلید را می‌توان به دو دسته مبتنی بر رأی‌گیری[۶] و بدون رأی‌گیری طبقه‌بندی کرد. در روش مبتنی بر رأی‌گیری، مکانیزم ابطال کلید براساس نظرات گره‌های مجاور خواهد بود. در تکنیک بدون رأی‌گیری، با تأیید هر گره با گواهی معتبر، کلید گره حمله‌کننده ابطال می‌شود [۱۲]. در مکانیزم مبتنی بر رأی‌گیری به دلیل همکاری و جمع‌آوری نظرات گره‌های مجاور، فرآیند ابطال کلید، زمان‌بر است. در این روش،

---

[1] Secret sharing
[2] Haibing
[3] Changlun
[4] Possion process
[5] Nonhomogeneous Poisson process
[6] Voting