بسم اللّه الرّحمن الرّحيم

دانشگاه صنعتی امیرکبیر

(پلی‌تکنیک تهران)

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پایان نامه برای دریافت درجه کارشناسی ارشد مهندسی فناوری اطلاعات

گرایش امنیت اطلاعات

مدل سازی و بهبود روش های ابطال گواهی کلید عمومی در شبکه سیار موردی

نگارش:

افشین لامعی

استاد راهنما:

دکتر مهران سلیمان فلاح

زمستان ۱۳۸۶

بسمـه تعالـی

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)
معاونت پژوهشی

فرم اطلاعات پایان نامه
کارشناسی ارشد و دکترا

تاریخ: .....

پیوست: .....

نام و نام خانوادگی:	افشین لامعی	**دانشجوی آزاد** ■	**بورسیه** □	**معادل** □
شماره دانشجوئی:	۸٤۱۳۱۰۱۲	**دانشکده:** مهندسی کامپیوتر	**رشته تحصیلی:**	فناوری اطلاعات
نام و نام خانوادگی استاد راهنما:	دکتر مهران سلیمان فلاح			
عنوان پایان نامه به فارسی:	مدل سازی و بهبود روش های ابطال گواهی کلید عمومی در شبکه سیار موردی			
عنوان پایان نامه به انگلیسی:	Modeling and Improving Public Key Certificate Revocation Schemes in Mobile Ad hoc Networks			
نوع پروژه:	**کارشناسی ارشد** ■ / **دکترا** □	**کاربردی** □	**بنیادی** □	**توسعه ای** ■ **نظری** □
تاریخ شروع:	۱۳۸۵/۸/۱۵	**تاریخ خاتمه:** ۱۳۸۶/۱۰/۳۰	**تعداد واحد:** ۶	
سازمان تأمین کننده اعتبار:				
واژه های کلیدی به فارسی:	ابطال گواهی، شبکه سیار موردی، مدل سازی صوری، منطق زمانی، نیازمندی			
واژه های کلیدی به انگلیسی:	Formal Modeling, Certificate Revocation, Mobile Ad hoc Network, Requirement, Temporal Logic			

نظرها و پیشنهادها به منظور بهبود فعالیت های پژوهشی دانشگاه:

استاد راهنما:

دانشجو:

امضاء استاد راهنما: **تاریخ:**

نسخه ۱: معاونت پژوهشی

نسخه ۲: کتابخانه و به انضمام دو جلد پایان نامه به منظور تسویه حساب با کتابخانه و مرکز اسناد و مدارک علمی

تقدیم به

پدر

مادر

و همسرم

تقدیر و تشکر

بر خود لازم می‌دانم از راهنمایی‌ها و حمایت‌های بی‌دریغ استاد ارجمند، جناب آقای دکتر مهران سلیمان فلاح، در کلیه مراحل انجام این پایان نامه صمیمانه تقدیر و تشکر نمایم. همچنین از همسر بزرگوارم که در طول تحصیل من همواره مشوّق و همراهم بود، بسیار متشکرم.

از کمک دوست عزیزم آقای مهندس امین شالی در بخش زبان رِبکا تشکر می‌کنم.

همچنین از استادان گرامی سرکار خانم دکتر مرجان سیرجانی و جناب آقای دکتر بابک صادقیان جهت قبول زحمت داوری این پایان نامه بسیار متشکرم.

چکیده

در سال های اخیر مکانیزم‌هایی برای ابطال گواهی کلید عمومی در شبکه‌های سیار موردی (MANETs) پیشنهاد شده است. ویژگی‌های طبیعی اینگونه شبکه‌ها، همچون عدم وجود زیرساخت مخابراتی ثابت و سرویس دهنده‌های دائمی، امکان استفاده از روش‌های سنتی ابطال گواهی را منتفی کرده است. به علاوه، کمبود منابع پردازشی و ذخیره سازی نودها به عدم سازگاری راه حل‌های مرسوم در این نوع شبکه‌ها دامن زده است. با وجود تلاش‌های انجام شده، نبود شناخت دقیق از نیازمندی های ابطال گواهی به طور کلی و به طور خاص در شبکه‌های سیار موردی باعث شده است که راه حل‌های ارائه شده از نظر صحت و کارآیی دارای کمبودهایی باشند که از دید طراحان به دور مانده است.

در این پایان نامه، نیازمندی های یک مکانیزم ابطال گواهی کلی را بیان می‌کنیم. در واقع این نیازمندی ها به صورت مجرّد بیان می‌شوند تا بتوان از آنها در درستی یابی مکانیزم های مختلف موجود و یا پیشنهاد راه حل های جدید استفاده نمود. سپس این نیازمندی ها را با استفاده از منطق زمانی به شکل صوری بیان می‌کنیم. همچنین نشان می‌دهیم که نیازمندی های ما در یافتن برخی مشکلات ناشناخته راه حل های موجود مفید است. به‌علاوه، پیشنهادهایی برای بهبود برخی از این مشکلات ارائه می‌نماییم. در این راه از زبان توصیف ربکا برای درستی یابی مدل های بهبود یافته استفاده می‌کنیم.

کلمات کلیدی: ابطال گواهی، شبکه سیار موردی، مدلسازی صوری، منطق زمانی، نیازمندی.

فهرست مطالب

فصل یکم: مقدمه

۱-۱ شبکه سیار موردی

امروزه با گسترش استفاده از ابزارهای سیار همچون لپ تاپ ها، PDA ها، تلفن هـا و حـس گرهـای بی‌سیم، بر اهمیت شبکه سیار موردی[۱] افزوده شده است. شبکه سیار موردی مجموعه ای از وسایل، بـا اتصال بی سیم است که همگی با هم مجموعه‌ای از گره‌های خود مختار را تشکیل داده و بـه صـورت نامتمرکز، یک شبکه رادیـویی پویـا[۲]، خـاص منظـوره و چنـدگام[۳] مـی سـازند. ایـن شـبکه هـا دارای

---

[۱] Mobile Ad hoc Network

[۲] Dynamic

[۳] Multi-hop

توپولوژی پویا هستند؛ این بدان معنا است که در هر زمان ممکن است گره ای به شبکه وارد شده ویا از آن خارج شود. به بیان دیگر اندازه شبکه ثابت نیست. همچنین، گره ها می توانند آزادانه حرکت کنند. از آنجایی که این شبکه ها معمولاً برای کاربردی خاص طراحی شده‌اند، به آنها شبکه‌های خاص منظوره یا موردی گفته می شود. در این شبکه‌ها، ارتباطات به صورت همکاری محور[۱] بوده و بسته‌ها توسط گره‌های میانی مسیریابی می‌شوند. بنابراین، لازم است هر گره از توانایی مسیریابی بسته‌ها برخوردار باشد. علاوه بر مسیریابی، بسیاری از پروتکل های دیگر نیز بر مبنای همکاری نودها طراحی شده است. نظر به اینکه گره‌ها سیار می‌باشند، معمولاً قدرت محاسباتی و عملیاتی محدودی داشته و مسأله مصرف بهینه انرژی در آنها از اهمیت خاصی بر خوردار است.

بی‌نیازی از ساختار و خود سازمانده بودن از خواصی به شمار می رود که این شبکه‌ها را برای محدوده وسیعی از کاربردها نظیر کاربردهای نظامی، کاربردهای کنترلی و شبکه‌های حسگر[۲]، کاربردهای اضطراری[۳] و دیگر شرایطی که امکان تشکیل شبکه‌های بی‌سیم مبتنی بر زیرساخت از نظر محدودیتهای فنی، عملی، اقتصادی و زمانی امکان پذیر نیست، مناسب ساخته‌است. علاوه بر آن، با در نظر گرفتن اینکه همه افراد و دستگاه‌ها در آینده به سیستمهای ارتباطی مجهز خواهند شد، این شبکه‌ها نقشی مهم در به واقعیت پیوستن رویای شبکه‌های نسل آینده[۴] و پیاده‌سازی عملی شعار ارتباطات همه جا، همه وقت و در هر صورت خواهند داشت.

در این شبکه ها در صورتی که دو گره، که در داخل محدودهٔ ارسالِ بی سیم یکدیگر قرار ندارند، بخواهند با هم ارتباط برقرارکنند، از گره‌هایی که در حد فاصل این دو گره قرار دارند استفاده می کنند. به این دلیل، به آنها چندگام گفته می شود. ویژگی ذاتی این شبکه ها بدون زیر ساخت بودن آنها است. در این شبکه‌ها، مرکز سوئیچینگ، ایستگاه پایه[۵]، نقطهٔ دستیابی[۶] و دیگر تجهیزات متمرکز، که در سایر شبکه‌های بی سیم استفاده می‌شوند، وجود ندارد. بنا براین، به دلیل هزینه کمتر و سهولت استفاده، شبکه های بی سیم سیار موردی در بسیاری از کاربردها انتخاب بهتر و حتی تنها گزینه هستند.

---

۱ Collaborative

۲ Sensor networks

۳ Emergency

۴ Next generation networks (NGN)

۵ base station

۶ Access Point

۱-۲ امنیت در شبکه سیار موردی

مطالعات اولیه در MANET بیشتر به حل مشکلات بنیادی این شبکه‌ها، همچون مسیریابی، پرداخته است. اما امروزه، تمرکز بیشتر بر امن سازی پروتکل های پیشنهاد شده و نیز ارائه راه کارهای امنیتی بهتر قرار گرفته است. در [DjKh05] مروری بر راه حل های امنیتی ارائه شده در لایه‌های مختلف MANET انجام شده است.

اهداف امنیت در شبکه های سیار موردی، همچون دیگر شبکه‌ها، برقراری محرمانگی، صحت، و دسترس پذیری است. اما، برقراری این اهداف درMANET با معضلات جدی مواجه است. غیر قابل اعتماد بودن پیوندهای بی سیم میان گره‌ای، توپولوژی پویا و عدم امکان برپایی ساختار های متمرکز امنیتی باعث آسیب پذیری بیشتر این شبکه ها نسبت به حملات می شوند[CHB03]. با توجه به کاربردهای عمده این شبکه‌ها در موارد حساس مانند جمع‌آوری و انتقال اطلاعات در صحنه‌های نبرد نظامی و یا امداد و نجات در شرایط بحرانی، اهمیت موضوع برقراری امنیت دوچندان می‌گردد. با در نظر گرفتن طبیعت خودمختار و بی‌زیرساخت این شبکه‌ها و عدم وجود اعتماد بین گره‌ها و اعضای شبکه از یک سو و نیاز به همکاری گره‌ها در انتقال اطلاعات، امنیت از یک سرویس جانبی به یک الزام برای کارکردهای عادی شبکه تبدیل می‌شود. در کنار مسأله مسیریابی و انتقال اطلاعات، موضوعات دیگر نظیر کشف نفوذگران و عناصر بدرفتار، حفظ محرمانگی اطلاعات و فراهم آوردن سرویسهای حریم خصوصی[۱] و بسیاری دیگر از موضوعات امنیتی، مسائل باز فراوانی را جهت مطالعات بیشتر ایجاد کرده است.

۱-۲-۱ زیرساخت کلید عمومی در MANET

یکی از بسترهای بنیادی خدمات امنیتی، چه در شبکه های سنتی و چه در MANET، زیرساخت کلید عمومی[۲] یا PKI است. خدمات PKI شامل تولید زوج کلیدهای عمومی- خصوصی، امضای گواهی کلید عمومی، توزیع گواهی و ابطال آن می‌باشد. این خدمات در شبکه های سنتی به واسطه دسترسی به زیرساخت های متمرکز و قوی، به راحتی پیاده سازی شده است. استانداردهایی چون X.509 ، SPKI ، PGP و مانند آن برای توصیف فرمت گواهی و پروتکل های مدیریت گواهی پیشنهاد شده‌اند [SBY06]. در شبکه سیار موردی، با در نظر داشتن مشکلات ذکر شده، ارائه این خدمات نیازمند ارائه

---

۱ Privacy

۲ Public Key Infrastructure

روش های جدید و مناسب است. مهم ترین چالش در برقراری PKI ، چگونگی پیاده سازی مسئول گواهی یا CA است. تا کنون طرح هایی چون [ZhHa99] ، [KZLLZ01] و [ACDM06] که از سیستم اشتراک سرّ آستانه ای برای توزیع اختیارات CA میان نودها استفاده کرده اند، بیشتر مورد توجه قرار داشته اند. همچنین طرح هایی چون [CBH03] و [LLKL04] نیز با استفاده از ایجاد شبکه اعتماد، مشابه PGP ارائه گردیده که در آنها هر نود مستقلاً یک CA برای نودهای همسایه است.

۱-۲-۲ ابطال گواهی در MANET

ابطال گواهی[۱] یکی از مهم ترین مسائلی است که در هر سیستم مدیریت کلید عمومی مطرح است. وقتی یک گواهی صادر می‌شود، تا زمان مشخصی، که درون خود گواهی قید شده است، اعتبار دارد و پس از آن منقضی می‌شود. گاه لازم است گواهی را پیش از منقضی شدن، به دلایلی چون افشای کلید خصوصی ابطال نمود. اهمیت مسأله آن است که کاربران بر اساس اعتماد به گواهی یکدیگر از خدمات PKI بهره مند شده و با هم ارتباط امن برقرار می‌کنند. بنابراین، باید تضمین کنیم که امکان اعتبار سنجی گواهی، برای کسانی که این اعتبار برای آنها مهم است، همواره وجود دارد.

در شبکه های سنتی، راه حلهای متعددی از جمله روش لیست ابطال گواهی[۲] ، وضعیت ابطال گواهی[۳] ، درخت ابطال گواهی[۴] و پروتکل آنلاین وضعیت گواهی[۵] پیشنهاد شده است[NaNi00]. اما به دلیل عدم تعریف دقیق از نیازمندی های ابطال گواهی، درستی یابی و مقایسه این روش ها به دشواری امکانپذیر است.

برقراری روش های سنتی ابطال گواهی در MANET ناممکن است. زیرا این روش ها همگی با فرض وجود یک CA ثابت، و نیز مبتنی بر دسترسی دائمی به سرویس دهنده ها و دایرکتوری های متمرکز، همچنین امکان ذخیره سازی، تبادل و پردازش ساختمان داده های بسیار حجیم هستند. بنابراین، باید در MANET به دنبال راه حل های جدیدی باشیم.

اگر چه تلاش‌هایی برای حل مسأله ابطال گواهی در MANET انجام شده است، این موضوع کماکان به عنوان یک مسأله باز مطرح است[Tse06]. در بسیاری از راه حل های PKI در MANET همچون

---

[۱] Certificate Revocation

[۲] Certificate Revocation List

[۳] Certificate Revocation Status

[۴] Certificate Revocation Tree

[۵] Online Certificate Status Protocol

[ZhHa99]، [WeTh01]، [BHKPW04]، [KKA03] و [RPT04] اصولاً به مسأله ابطال گواهی پرداخته نشده است. در روش های مبتنی بر اشتهار همچون [KZLLZ01] و [ACDM06] ، نحوه قضاوت مجموعه ای از نودها در مورد رفتار یک نود، مبنای ابطال یا عدم ابطال گواهی است و ابطال به صورت جمعی انجام می‌شود. در روش های مبتنی بر شبکه اعتماد، مانند [CBH03]، هر نود گواهی مشتریان خود را به طور مستقل باطل می‌کند.

۱-۳ نوآوریهای این پایان نامه

در این پایان نامه، با بررسی دقیق جوانب مختلف مسأله، یک تعریف جامع و مانع از فرآیند ابطال گواهی و طرف های درگیر در آن، صرفنظر از محیط پیاده سازی آن ارائه شده است. سپس نیازمندی های ابطال گواهی ابتدا به شکل غیر صوری و پس از آن به شکل صوری بیان گردیده است. نیازمندی های ذکر شده در حقیقت به طور شهودی در هر مکانیزم ابطال گواهی (نه فقط در MANET) مورد نیاز هستند. نیازمندی ها به شکل کاملاً مجرد توصیف شده اند، تا بتوان از آنها در تحلیل راه حل های موجود و ارائه طرح های جدید چه در MANET و چه در شبکه های سنتی استفاده نمود. برای دستیابی به این نیازمندی ها، سناریوهای مختلفی با حضور انواع طرف های درگیر در زیرساخت کلید عمومی به دقت بررسی شده است. همچنین برای نشان دادن کاربرد هر نیازمندی، مثال هایی از مراجع مختلف انتخاب شده است.

در بیان نیازمندی‌ها به شکل صوری از منطق زمانی[۱] برای بیان ویژگی های مورد نظر در یک سیستم واکنشی[۲] [MaPn93] استفاده شده است. این زبان توصیف کننده تقدم و تأخّر رخدادها، در یک ترتیب خاص یا در تمام حالتهای[۳] سیستم است. با استفاده از بیان صوری نیازمندی ها، شرایط درستی عملکرد سیستم ابطال گواهی را بیان کرده ایم.

در گام بعد، چند راه حل موجود ابطال گواهی در MANET را مدل سازی نموده ایم. به این منظور از زبان ربکا[۴] که ابزاری برای توصیف سیستم های همروند و توزیع شده است [SMSB05] استفاده کرده‌ایم. این مدل‌ها را با استفاده از RMC [۵] بررسی نموده ایم. نتایج درستی یابی مدل ها بر اساس

---

۱ Temporal Logic

۲ Reactive System

۳ States

۴ Rebeca

۵ Rebeca Model checker

نیازمندی‌های به دست آمده نشان می‌دهد که برخی نیازمندی‌ها در این راه حل ها برآورده نشده اند. در مطالعه موردی نیازمندی ها، در برخی موارد، پیشنهادهایی نیز برای بهبود طرح های موجود ارائه و نتیجه این پیشنهادها درستی یابی شده است.

۱-٤ ساختار پایان نامه

در فصل دوم به مرور کارهای قبلی، شامل روش های سنتی ابطال گواهی و روش های ابطال گواهی در MANET، می‌پردازیم. فصل سوم به بیان نیازمندی های ابطال گواهی اختصاص دارد. در فصل چهارم نیازمندی‌ها را به روش صوری بیان می‌نماییم. فصل پنجم به مطالعه موردی و پیشنهاد بهبود روش‌ها اختصاص دارد. در فصل ششم، نتایج و پیشنهاد برای ادامه تحقیق در موضوع پایان نامه آمده است.

فصل دوم: مکانیزم‌های موجود برای ابطال گواهی

۲-۱ مقدمه

روش‌های سنتی ابطال گواهی به طور گسترده در منابع مختلف معرفی و از جنبه‌های متفاوت بررسی شده اند. این روش ها بر اساس معیارهای مختلفی دسته بندی شده اند که در اینجا به برخی از این دسته بندی ها اشاره می‌کنیم.

- *نحوه پاسخ دهی به درخواست ها ممکن است آفلاین یا آنلاین باشد.* آفلاین به روش هایی اطلاق می‌شود که وضعیت ابطال گواهی از پیش مشخص شده و معمولاً توسط CA در دسترس کاربر قرار می‌گیرد. آنلاین به روش هایی گفته شده که وضعیت گواهی در همان زمان درخواست کاربر، تولید شده و پروتکلی با قدم ها و پیام های مشخص برای تبادل این اطلاعات با کاربر ارائه شده است.
- *اطلاعات داده شده به کاربر می‌تواند اثبات کننده یا نفی کننده باشد.* مثلاً در روش های مبتنی بر لیست، نبودن یک گواهی در لیست سیاه یا لیست گواهی های ابطالی، به معنی معتبر بودن یا حتی وجود آن گواهی در سیستم نیست، زیرا لیست سیاه تنها حاوی جملات منفی است.

روش هایی که گواهی های معتبر را نگهداری و در مورد آنها اطلاع می‌دهند، اثبات کننده و روش هایی که گواهی های باطل شده را نگهداری می‌کنند، نفی کننده هستند.

- *نحوه توزیع اطلاعات وضعیت گواهی میان کاربران ممکن است بر اساس مکانیزم رانش[۱] یا کشش[۲] باشد.* در مکانیزم های کششی، تصمیم گیرنده باید متناوباً وضعیت گواهی را، مثلاً با پرسش از CA ، بررسی کند. در مکانیزم های رانشی، آخرین وضعیت گواهی، بدون نیاز به مراجعه برای تصمیم گیرنده ارسال می‌شود.

در اینجا، شناخته شده ترین روش‌ها را بررسی می‌نماییم و تلاش می‌کنیم تصویری از مهم‌ترین ویژگی های آنها را که در طراحی راه حل های MANET مورد توجه بوده است به دست آوریم.

۲-۲ روش های مبتنی بر لیست

در این دسته از روش ها، از ساختمان داده لیست برای مدیریت گواهی های ابطال شده استفاده می-شود.

۲-۲-۱ لیست گواهی های ابطالی (CRL)

این روش در سال ۱۹۸۸ برای اولین بار توسط ITU-T که در آن زمان CCITT نام داشت، تحت استاندارد X.509 ارائه شد و در سال ۱۹۹۳، نگارش دوم استاندارد X.509 که شامل نگارش بهبود یافته CRL نیز بود توسط ITU-T و ISO/IEC معرفی شد[HaFo98] . CRL لیستی از گواهی های ابطال شده است که دارای امضا و مهر زمانی[۳] است. هر یک از ورودی های لیست شماره سریال یک گواهی ابطال شده است. معمولاً اطلاعات دیگری چون تاریخ تولید لیست، تاریخ ابطال گواهی، دلیل ابطال و تاریخ به روز رسانی بعدی هم در CRL درج می‌شود.

لیست تولید شده به صورت متناوب به دایرکتوری های عمومی که در دسترس همه کاربران است ارسال می‌شود. کاربر برای اطلاع از وضعیت گواهی، CRL را از دایرکتوری دانلود می‌کند. سپس امضای مسئول گواهی را راستی آزمایی نموده و تاریخ انتشار لیست را بررسی می‌کند. در صورت موفقیت آمیز بودن بررسی ها، شماره سریال گواهی مورد نظر درون لیست جستجو می‌شود. در صورتی که گواهی مربوطه در لیست قید نشده باشد، کماکان معتبر است. به عنوان مثال، یک وزارتخانه ممکن است به صورت هفتگی برای گواهی های کارمندانش CRL منتشر کند. کارمندان در صورت تمایل

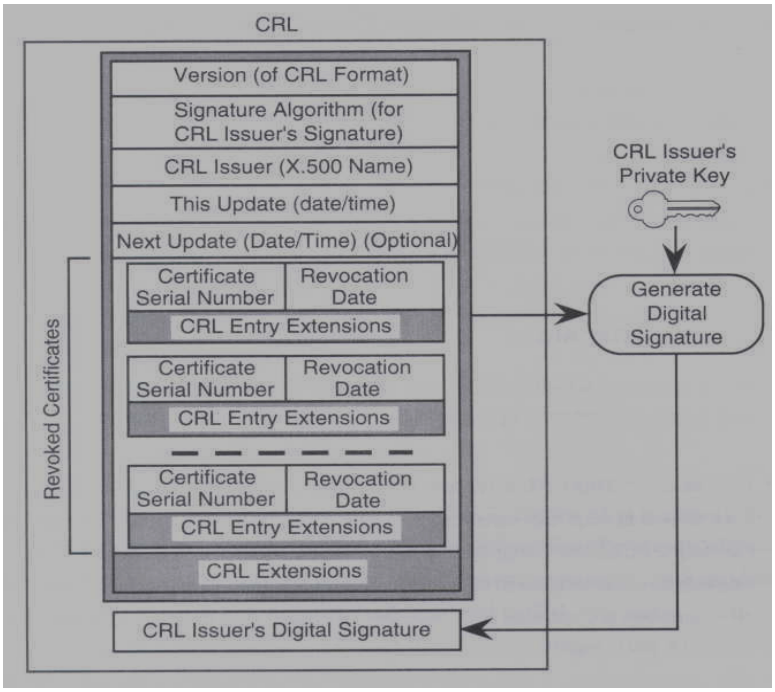
---

۱ Push

۲ Pull

۳ Time Stamp

می‌توانند جدیدترین CRL را دانلود کرده و اعتبار گواهی های مربوطه را به کمک آن بررسی کنند. شکل زیر که بر گرفته از متن استاندارد X.509 است، فرمت یک CRL را نشان می‌دهد.



شکل ۲-۱- ساختار CRL [HaFo98]

برای بررسی ویژگی های روش CRL به موارد زیر توجه می‌کنیم.

الف- روش CRL کاملاً شهودی است.

ب- اندازه CRL تابعی خطی از تعداد گواهی های منتشر شده در سیستم است. بنابراین CRL ها معمولاً بسیار حجیم هستند. برای جلوگیری از رشد بیش از حد لیست، روش هایی چون حذف گواهی های منقضی شده و یا تکه تکه نمودن CRL پیشنهاد شده است [Mye98] .

ج- تبادل CRL های حجیم میان دایرکتوری ها و کاربران، درصد قابل توجهی از پهنای باند شبکه را اشغال می‌کند. با توجه به اینکه کاربران علاقه مند به داشتن تازه ترین CRL هستند، معمولاً درخواست دانلود CRL در لحظات پس از انتشار آن بسیار زیاد بوده وباعث ازدحام در شبکه[۱] می‌شود [Zhe03] .

---

[۱] Congestion

د- عدم وجود یک گواهی خاص در CRL ، لزوماً به معنای اعتبار آن، و فراتر از آن حتی به معنای وجود این گواهی در سیستم، نیست. زیرا CRL حاوی جملات نفی است نه اثبات [Riv98] .

۲-۲-۲ وضعیت ابطال گواهی (CRS)

این روش در سال ۱۹۹۵ توسط Micali با عنوان سیستم ابطال گواهی معرفی شد و یک سال بعد با عنوان وضعیت ابطال گواهی توسط وی بهبود یافت [Woh00]. هدف آن است که هزینه تبادل دائمی میان کاربر و دایرکتوری کاهش یابد. در اینجا کاربر تنها اطلاعاتی در مورد اعتبار یا ابطال گواهی مورد نظر دریافت می‌کند، نه همه گواهی ها.

روش کار به این صورت است که مسئول گواهی دو عدد N و Y_{365} را به گواهی X.509 اضافه می-کند. این دو فیلد با استفاده از اعداد تصادفی N_0 و Y_0 به صورت زیر توسط CA ساخته می‌شوند. (f یک تابع درهم ساز است)

$$Y_{365} = f^{365}(Y_0)$$
$$N = f(N_0)$$

دایرکتوری به صورت روزانه توسط مسئول گواهی با ارسال مقدار C متناظر هر گواهی بروز می‌شود. مقدار C برای هر روز از سال، به صورت زیر محاسبه می‌شود.

الف- $C = Y_{365-i} = f^{365-i}(Y_0)$ برای گواهی معتبر.

ب- $C = N_0$ برای گواهی باطل شده.

دایرکتوری برای پاسخ به درخواست بررسی وضعیت یک گواهی، جدیدترین مقدار C گواهی مربوطه را ارسال می‌کند. مقدار C می‌تواند مستقیماً توسط صاحب گواهی به عنوان اثبات اعتبار گواهی به طرف اعتماد کننده ارائه شود.

مهم ترین برتری این روش نسبت به CRL ، هزینه کمتر برای درخواست های ارسالی کاربران به دایرکتوری است. مزیت دیگر آن است که مقدار C می‌تواند تعداد دسترسی های مستقیم به دایرکتوری را کم کند. در [Woh00] عدم امکان جعل C توسط دایرکتوری (به دلیل محرمانه بودن Y_0) هم به عنوان مزیت این روش بیان شده است. مهم ترین ضعف این روش، افزایش تعداد ارتباطات مسئول گواهی با دایرکتوری است [NN00] .

۲-۳ روش های مبتنی بر درخت

در این دسته از روشها از ساختمان داده درخت برای سازماندهی گواهی های ابطال شده به صورت مرتب استفاده می‌شود.