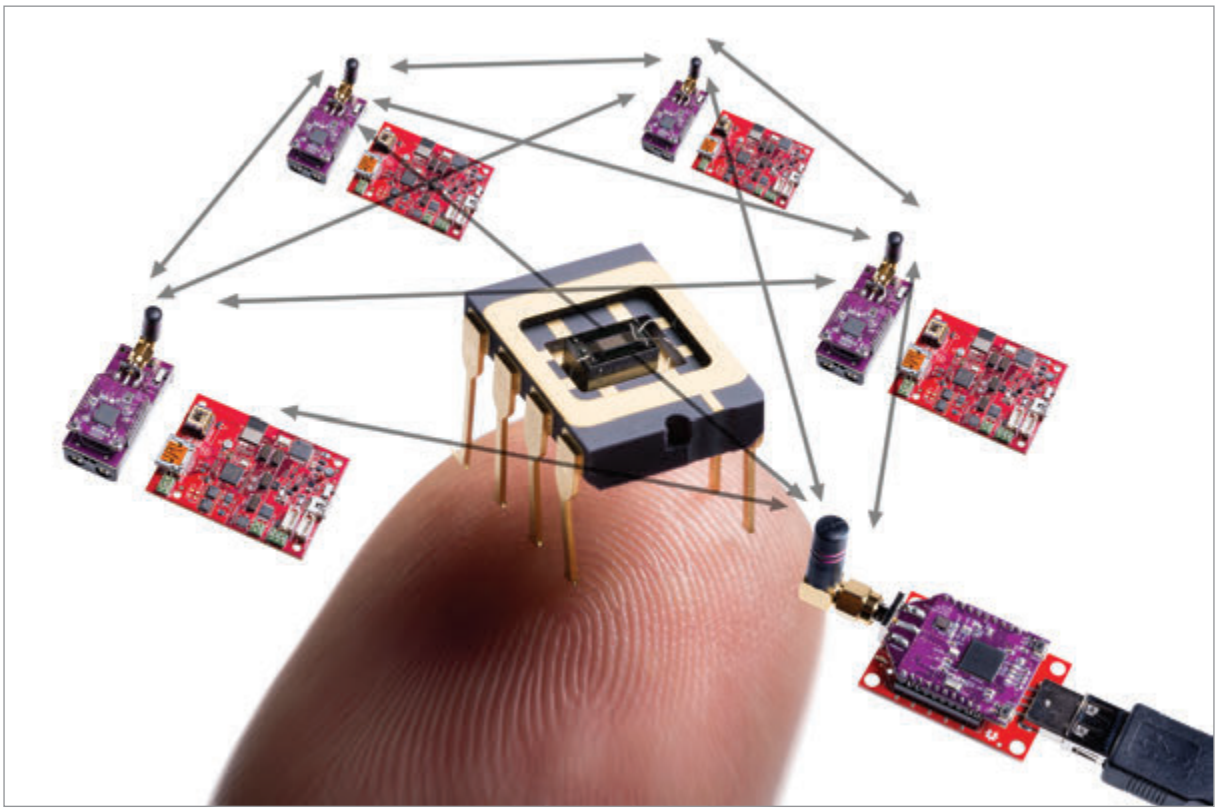
برگردان : محمد پژوهش‌فر



سیستم رمزی انعطاف پذیر و کاربرد آن در شبکه های حسگر بی سیم

۱- مقدمه

هدف اصلی شبکه حسگر بررسی پدیده ها و انتقال اطلاعات به ایستگاه مرکزی می باشد. انتظار می رود محاسبات پیچیده در ایستگاه مرکزی انجام شوند. با این حال، انتقال داده های غیرضروری می تواند منجر به افزایش بار ارتباطی گره های حسگری گردد که در نزدیکی ایستگاه مرکزی قرار دارند. پردازش درون شبکه ای به کاهش ترافیک ارتباطات زاید کمک می کند. پردازش درون شبکه ای همچنین منجر به تجمع ترافیک چندجانبه در شبکه های حسگر بی سیم می گردد. علاوه بر این، استفاده های خصمانه و بدون توجه و محیط ارتباطی ناامن تهدیدهای امنیتی را برای خوانش های حسگر ایجاد می کنند.

در شبکه های حسگر بی سیم، گره های جمع کننده داده ها را از گره های حسگر دریافت کرده و آنها را قبل از ارسال نتایج به ایستگاه مرکزی جمع بندی می کنند. اگر داده های رمزی باشند، گره های جمع کننده باید داده ها را رمزگشایی کرده و بعد از جمع بندی آنها را مجددا رمزگذاری نموده و سپس به hop بعدی ارسال کنند. ایمنی Hop-by-hop منجر به افزایش مصرف منابع در شبکه های حسگر بی سیم دارای منابع محدود می گردد و این امر ریسکی برای حریم خصوصی خوانش های حسگرها می باشد. این فرایند اغلب در شبکه های حسگر بی سیم با نام جمع آوری ایمن داده ها به روش Hop-by-hop شناخته می شود. در این روش، گره های واسط عامل دشواری ایمنی پروتکل های شبکه های حسگر بی سیم می گردند. بنابراین، اطمینان از حریم خصوصی خوانش های حسگر در گره های واسط منجر به ایجاد پروتکل های جمع آوری ایمن داده ها می گردد.

پردازش داده های رمزنگاری شده در طی دهه های اخیر به طور گسترده ای مورد مطالعه قرار گرفته است. هم ریختی ارائه شده توسط ریوست و همکارانش منجر به تغییر پذیری سیستم های رمزی گردیده و کاربردهای جالبی در شبکه های حسگر بی سیم با منابع محدود می گردد. با این حال، هم ریختی دارای تاثیرات معکوسی نیز بر روی عملکرد سایر معیارهای امنیتی از جمله انسجام و تازگی داده ها دارد. علاوه بر این، روش های سنتی سازگاری خوبی با مدل های امنیتی نهایی که از تجمع حمایت می کند، ندارند. در این فصل، ما به بررسی سیستم های رمزی قابل تغییر استفاده شده توسط پروتکل های شبکه های حسگر بی سیم مختلف خواهیم پرداخت. فصل پیشنهادی به درک سیستم های رمزی مختلف استفاده شده توسط پروتکل های WSN برای پردازش خوانش های حسگر در گره های واسط کمک می کند. بحث ارائه شده در این فصل، نه تنها منجر به شناخت سیستم های رمزی مختلف می گرد، بلکه درک مقالات تحقیقاتی مختلف ارائه شده در WSN ها را تسهیل کرده و از این سیستم های رمزی استفاده می کند.

ادامه این فصل به شرح زیر سازماندهی شده است. در بخش ۶،۲، ما تاثیر پردازش درون شبکه بر روی نیازمندی های امنیتی از جمله حریم خصوصی، انسجام و تازگی را مورد بررسی قرار

می دهیم. در بخش ٦,٣، ما به بررسی هم ریختی حریم خصوصی می پردازیم. بخش ٦,٤، سیستم های رمزی قابل تغییری که بر پایه رمزنگاری متقارن ایجاد شده اند و در چندین پروتکل WSN به کار برده شده اند را بررسی می کند. در بخش ٦,٥، ما سیستم های رمزی قابل تغییر را ارائه می دهیم که مبتنی بر رمزنگاری کلید نامتقارن بوده و در پروتکل های WSN به کار برده شده اند. بخش ٦,٦، با تاکید بر روی نتایج حاصل، فصل را به پایان می رساند.

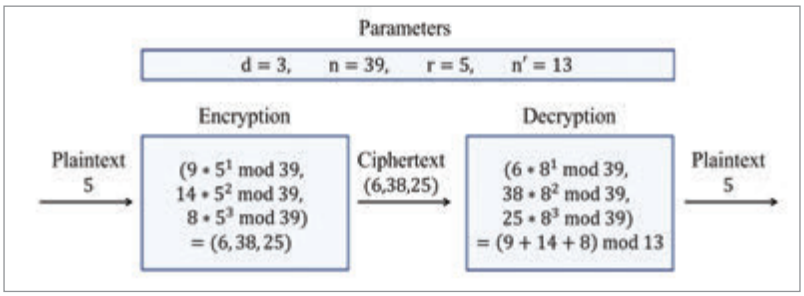
۲- تاثیر پردازش درون شبکه ای

شبکه های حسگر بی سیم در معرض حملات گسترده ای قرار دارند. این حملات شامل استراق سمع، تحلیل ترافیک، نقض انسجام، حملات بازپخش، حملات فیزیکی، حملات عدم ارائه خدمات و ... می باشند. علاوه بر این، حملات عدم ارائه خدمات در WSN ها شامل مجموعه ای از حملات از جمله حملات ،wormhole ،Sybil sinkhole و سیل می باشند. با این حال، به دلیل محدودیت های فضایی، ما بررسی انواع مختلف حملات و ضدحملات آنها را حذف می کنیم، اما اطلاعات مربوط به آنها را می توان در مقالات مرتبط مشاهده نمود.

پردازش درون شبکه ای دارای تاثیر شدیدی بر روی امنیت پروتکل های شبکه حسگر دارد. نیازمندی های متناقض از جمله پردازش در مسیر و ایمنی نهایی را نمی توان با استفاده از مکانیسم های امنیتی سنتی به دست آورد. علاوه بر این، WSN ها شباهت های زیادی با شبکه های مرسوم از جمله شبکه های بی سیم دارند و نیازمندی های امنیتی WSN ها همانند شبکه های سنتی می باشد. با این حال، نیازمندی های امنیتی شبکه های حسگر بی سیم تاثیر قابل توجهی بر روی جمع آوری داده های درون شبکه و پردازش داده های رمزی دارد. در این بخش، ما تاثیر پردازش درون شبکه بر روی موارد امنیتی ضروری از جمله حریم خصوصی، انسجام و تازگی را مورد بررسی قرار می دهیم.

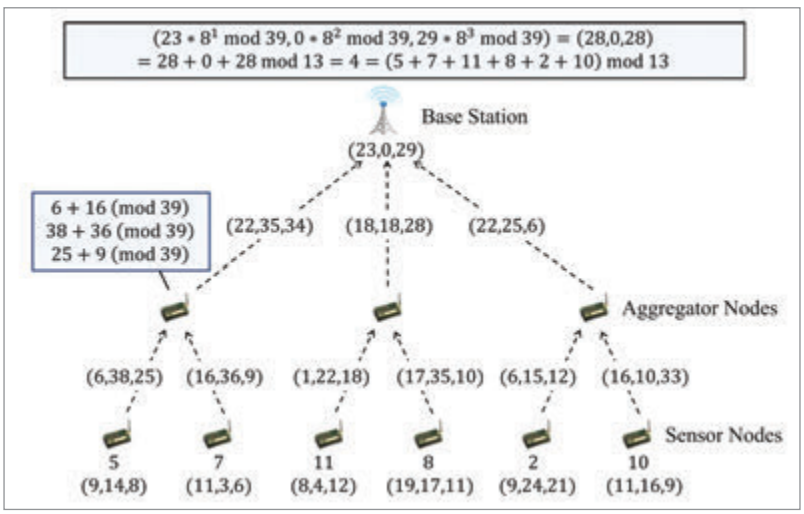
۲-۱- حریم خصوصی

استفاده در محیط های خصومت آمیز و فقدان محافظت فیزیکی منجر به آسیب پذیری گره های حسگر نسبت به حملات دستگیری گره می گردند. بنابراین، گره هایی که خوانش های حسگر را به صورت خام پردازش می کنند، هدف های اصلی حمله کنندگان هستند. اگر گره های نزدیک تر به ایستگاه مرکزی دستگیر شوند، می توانند تاثیر زیادی بر روی حریم خصوصی خوانش های جمع آوری شده از حسگرهای داشته باشند. یکی از راه



تصویر ۱- رمزگذاری و رمزگشایی با استفاده از سیستم رمزی Domingo-Ferrer

تصویر ۲- جمع آوری داده مبتنی بر درخت با استفاده از سیستم رمزی Domingo-Ferrer



حل ها برای مقابله با حملات دستگیری گره ها، پردازش خوانش های رمزگذاری شده حسگرها بدون رمزگشایی آنها در گره های جمع کننده واسط می باشد. هم ریختی حریم خصوصی به پردازش داده های رمزگذاری شده با استفاده از پارامترهای عمومی کمک می کند. اگرچه هم ریختی حریم خصوصی در برابر حمله کنندگان منفعل عملکرد محافظتی خوبی دارد، با این حال، خوانش های حسگر را نسبت به حمله کنندگان فعال آسیب پذیر می سازد که هدف آنها تغییر یا وارد کردن داده های تقلبی به شبکه می باشد.

۲-۲- انسجام

پردازش درون شبکه ای داده های اصلی را تغییر می دهد. از این رو، مکانیسم های سنتی نمی توانند انسجام نهایی را در شبکه های مبتنی بر داده تائید کنند. تائید انسجام نهایی یکی از مسائل تحقیقاتی به شمار می رود. با این حال، پارمر و جینوالا امکان محافظت از انسجام نهایی در WSN های دارای منابع محدود را نشان دادند. به طور خلاصه، تائید انسجام در شبکه های مبتنی بر داده نیازمند تائید انسجام در گره های واسط و همچنین ایستگاه مرکزی می باشد و نیازمند تائید انسجام خوانش های جمع شده و متراکم می باشد. مانع اصلی در دستیابی به این اهداف به شرح زیر می باشند: (۱) استفاده از هم ریختی حریم خصوصی قابل تغییر نه تنها به گره های جمع کننده اصیل کمک می کند، بلکه به حمله کننده نیز در تغییر داده های رمزگذاری شده یاری می کند. (۲) جمع آوری منجر به تغییر نمود داده های اصلی می گردد. از این رو، تائید صحت داده های جمع آوری شده به فرایندی چالش برانگیز تبدیل می شود.

۲-۳- تازگی

تازگی نقش مهمی را در صحت خوانش های جمع آوری شده حسگر ایفا می کند. محافظت از بازپخش با استفاده از کانتر یا nonce به روش سنتی صرفا منجر به محافظت بازپخش hop-by-hop می گردد. این نوع محافظت فقط دشمنان خارجی را در نظر می گیرد. با این حال، شبکه های حسگر ممکن است دارای گره های واسط باشند. محافظت بازپخش در برابر گره های دستگیر شده برای صحت اطلاعات جمع آوری شده ضروری می باشد.

۳- هم ریختی حریم خصوصی

هم ریختی خصوصی (یا پردازش داده های رمزنگاری شده) یکی از ویژگی های سیستم های رمزی می باشد که از پردازش داده های رمزگذاری

شده بدون رمزنگاری حمایت می کند. این ویژگی توسط پروتکل های مختلف WSN ها به منظور ارائه حریم خصوصی برای خوانش های حسگر در گره های واسط خطرپذیر به کار برده می شود.

همانطور که در معادله ۱ نشان داده شده است، کلید رمزنگاری و کلید رمزگشایی می تواند برای برخی از سیستم های رمزی از جمله سیستم رمزی Domingo–Ferrer یکسان باشد.

(1) - $Dk(Ek(x) + Ek(y)) \bmod n = (x + y) \bmod n$

همانطور که در معادله۲ نشان داده شده است، کلید رمزگشایی و کلید رمزنگاری می تواند برای برخی از سیستم های رمزی از جمله سیستم رمزی Paillier متفاوت باشد.

(2) - $D_{k'}(E_k(x) * E_k(y)) \bmod n = (x + y) \bmod n$

۱-۳- هم ریختی حریم خصوصی: افزودن

همانطور که در معادله۳ نشان داده شده است، سیستم رمزی CMT از عملیات هم ریختی مازاد بر داده های رمزنگاری شده استفاده می کند. علاوه بر این، سیستم های رمزی پیشنهادی توسط Koblitz، Okamoto و Uchiyama، Paillier و Domingo–Ferrer از عملیات هم ریختی مازاد بر داده های رمزی حمایت می کنند.

(3) - $D_k(E_k(x) * E_k(y)) \bmod n = x * y \bmod n$

۲-۳- هم ریختی حریم خصوصی: ضرب

سیستم رمزی RSA از هم ریختی حریم خصوصی تکثیری حمایت می کند. هم ریختی حریم خصوصی تکثیری امکان محاسبه داده های رمزنگاری شده را فراهم می آورد. همانطور که در معادله ٤ نشان داده شده است، رمزگشایی محصول دو متن منجر به نتیجه یکسانی می گردد.

(4) - $D_{k'}(E_k(x) * E_k(y)) \bmod n = x*y \bmod n$

۳-۳-هم‌ریختی‌حریم‌خصوصی:OR‌اختصاصی

سیستم رمزی Goldwasser–Micali از نظر عملیات X–OR دارای هم ریختی می باشد. همانطور که در معادله ٦,٥ نشان داده شده است، به منظور محاسبه X–OR در متن های عادی، سیستم رمزی Goldwassar–Micali محصول متن رمزی را محاسبه می کند. در بخش ٦,٥,٣، ما سیستم رمزی Goldwassar–Micali و استفاده آن در شبکه حسگر بی سیم را مورد بررسی قرار خواهیم داد.

(5) - $D_{k'}(E_k(x) * E_k(y)) \bmod n = x \oplus y \bmod n$

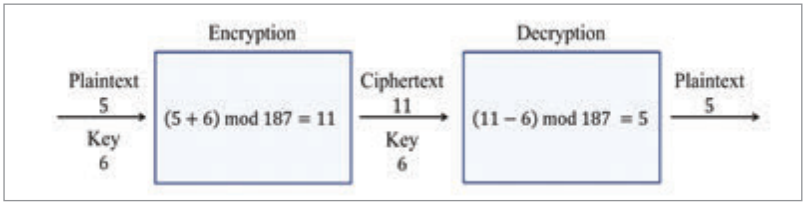
۴- هم ریختی حریم خصوصی مبتنی بر رمز متقارن

در این بخش، ما دو سیستم رمزی قابل تغییر مبتنی بر رمز متقارن را مورد بررسی قرار خواهیم داد که عبارتند از Domingo–Ferrer و CMT. بررسی دقیق سیستم های رمزی و استفاده آنها در شبکه های حسگر بی سیم توسط پارمار و جینوالا ارائه شده اند. از این رو، در این بخش ما صرفا روشی مناسب برای تحلیل این سیستم های رمزی را ارائه می دهیم.

۱-۴- سیستم رمزی Domingoo–Ferrer

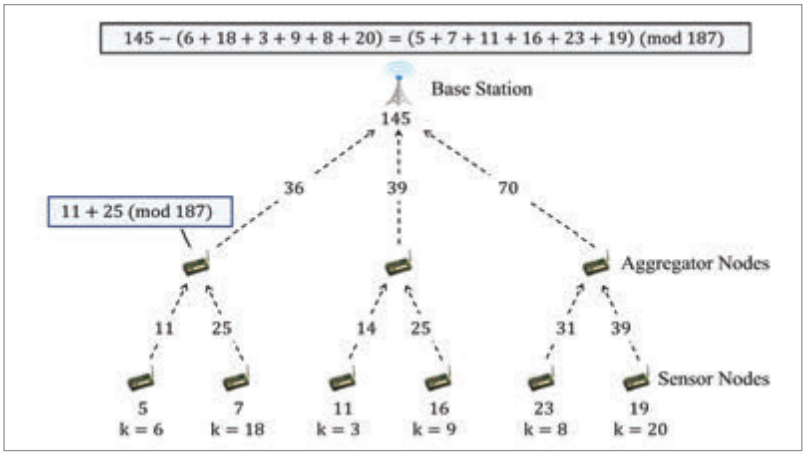
سیستم رمزی Domingo–Ferrer از پردازش داده های رمزنگاری شده در صورتی که داده ها با استفاده از یک رمز یکسان رمزنگاری شده اند، پشتیبانی می کند. در سیستم رمزی Domingo–Ferrer، اندازه پارامتر d بر روی اندازه متن رمزی تاثیر دارد. سیستم رمزی مبتنی بر رمز متقارن از پارامتر رمزی r برای رمزگذاری استفاده کرده و r-1 را برای رمزگشایی محاسبه می کند.

همانطور که در تصویر ۲ نشان داده شده است، هر متن عادی به d زیرمتن تقسیم شده است و هر زیرمتن نیز با استفاده از پارامتر رمزی r و یک پارامتر عمومی n رمزگذاری می شود.



تصویر ۳- رمزگذاری و رمزگشایی با استفاده از سیستم رمزی CMT

تصویر ٤- جمع آوری داده های مبتنی بر درخت با استفاده از سیستم رمزی CMT



سیستم رمزی	مدیریت رمز	عملیات	گسترش پیام
Castellucia	ایستگاه مرکزی رمز متمایزی را با هر گره در شبکه به اشتراک می گذارد	$\oplus \ \ominus \ \otimes_c$	۱
Domingo-Ferrer	ایستگاه مرکزی یک رمز جهانی را در شبکه به اشتراک می گذارد	$\oplus \ \ominus \ \otimes \ \otimes_c$	$\frac{d \times n}{n'}$

جدول ۱- مقایسه سیستم های رمزی قابل تغییر مبتنی بر رمز متقارن

همانطور که در توپولوژی جمع آوری داده های مبتنی بر درخت شرح داده شده در تصویر ۲ مشخص است، گره جمع آوری کننده محاسبات داده های رمزگذاری شده را با استفاده از پارامتر عمومی n انجام می دهد. رمزگشایی در ایستگاه مرکزی انجام شده و نیازمند روند معکوس پارامتر رمزی r می باشد. علاوه بر این، عملیات رمزگشایی نیازمند محصول نردبانی r-1 و مختصات متن رمزی جمع آوری شده می باشد.

۲-۴- سیستم رمزی CMT

Castellucia et al، رمز Verna، را به منظور ارائه طرح جمع آوری افزایشی ایمن پیشنهاد نمود که اغلب با عنوان سیستم رمزی CMT خوانده می شود. در سیستم رمزی CMT، همانطور که در تصویر ۳ نشان داده شده است، عملیات رمز توسط افزودن متن عادی و رمز انجام می شود، این در حالی است که عملیات رمزگشایی با کاهش رمز از متن رمز انجام می گیرد. اگرچه رمزگذاری و رمزگشایی عملیات کریپتوگرافی بهینه از نظر محاسباتی هستند، ایجاد رمزهای شبه تصادفی منجر به افزایش سربار محاسباتی

می گردد.
همانطور که در تصویر ٤ نشان داده شده است، هر گره حسگر افزودن متن عادی و رمز خود برای ایجاد متن رمز را انجام می دهد. متن رمزی دریافتی در گره های جمع آوری کننده با استفاده از افزایش مدولار جمع آوری می شود. ایستگاه مرکزی در سیستم رمزی CMT کلید جمع آوری شده را از متن رمزی جمع آوری شده به منظور دستیابی به متن عادی کسر می کند.

در جدول ۱، ما مقایسه سیستم های قابل تغییر مبتنی بر رمز متقارن را ارائه داده ایم.

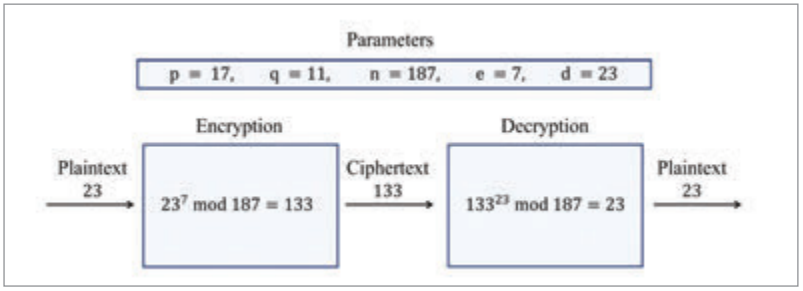
- $\oplus$ — افزودن هم ریختی
- $\ominus$ — کسر هم ریختی
- $\otimes$ — ضرب هم ریختی
- $\otimes$ — ضرب هم ریختی به همراه یک ضریب ثابت
- n — عدد صحیح ایجاد شده به صورت تصادفی
- n' — عدد صحیح n'>1 به طوری که n'|n
- d — متن ساده باید به بخش های d>2 تقسیم شود.

۵- هم ریختی حریم خصوصی مبتنی بر رمز نامتقارن

سیستم هار رمزی مبتنی بر رمز نامتقارن به طور گسترده در پروتکل های WSN ها به کار برده می شوند. بررسی دقیق سیستم های رمزی مبتنی بر رمز نامتقارن و کاربرد آنها در پروتکل های WSN توسط پارمار و جینوالا ارائه شده است. از این رو، در این بخش ما صرفا به معرفی سیستم های رمزی مبتنی بر رمز نامتقارن استفاده شده توسط چندین پروتکل WSN اکتفا می کنیم.

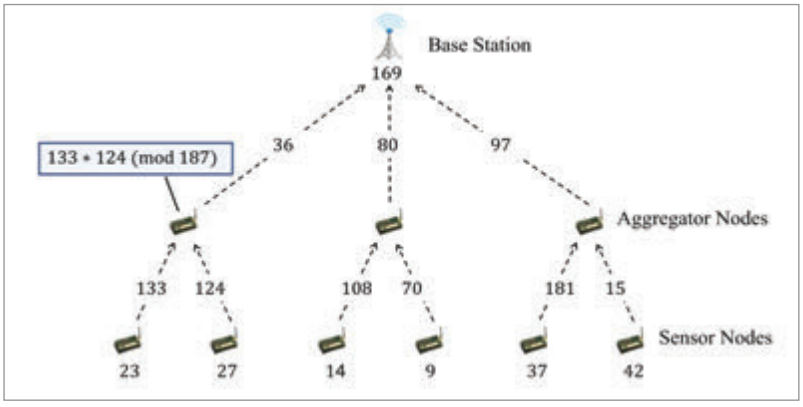
۵-۱- سیستم رمزی RSA

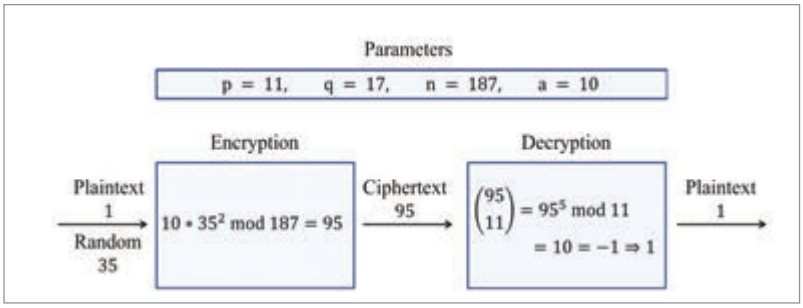
در سال ۱۹۷۸، ریوست، شامیر و آدلمن روشی را برای اجرای سیستم های رمزی رمز نامتقارن ارائه کردند که اغلب با نام سیستم رمزی RSA خوانده می شود. امنیت سیستم رمزی RSA به تعامل پذیری فاکتور گیری اعداد بزرگ بستگی دارد. مزیت سیستم رمزی RSA در مقایسه با سایر سیستم های رمزی مبتنی بر رمز نامتقارن این است که فاقد گسترش پیام می باشد و این بدین معناست که متن عادی و متن رمزی مربوط دارای اندازه یکسانی هستند $(m, c \in \mathbb{Z}_n)$. با این حال، مزیتی که منجر به محدودیت گسترش پیام می شود بدین دلیل است که سیستم رمزی RSA از اجزای تصادفی در طی رمزگذاری استفاده نمی کند. از این رو، بزرگترین مزیت عدم گسترش پیام،



تصویر ٥- رمزگذاری و رمزگشایی با استفاده از سیستم رمزی RSA

تصویر ٦- جمع آوری داده مبتنی بر درخت با استفاده از سیستم رمزی RSA





تصویر ۷- رمزگذاری و رمزگشایی با استفاده از سیستم رمزی Goldwasser-Micali

بزرگترین ایراد سیستم رمزی RSA به شمار می رود. علاوه بر این، به دلیل ماهیت قطعی سیستم رمزی RSA، این امر از نظر معنایی ناامن می باشد.
سیستم رمزی RSA از عملیات هم ریختی ضربی برای داده های رمزگذاری شده پشتیبانی می کند. با این حال، کاربرد داده های جمع آوری شده پنهان نیازمند پشتیبانی از هم ریختی جمعی می باشد. بنابراین، پروتکل های جمع آوری داده پنهان به منظور اطمینان از حریم خصوصی خوانش های حسگر در گره های واسط در سیستم رمزی RSA به کار برده نشده اند. با این حال، این سیستم از جمله اولین سیستم های رمزی مبتنی بر رمز نامتقارن است که در WSN ها برای ارزیابی امکان پذیری سیستم هاهی رمزی مبتنی بر رمز نامتقارن مورد بررسی قرار گرفته است.

۵-۲- مثال

در این بخش، ما مثالی از سیستم رمزی RSA را ارائه می دهیم. شایان ذکر است که به منظور سهولت محاسبه، ما از پارامترهای کوچک استفاده کرده ایم. با این حال، آن را می توان برای پارامترهای واقع بینانه تر نیز بسط داد. همانطور که در تصویر ٥ نشان داده شده است، متن ساده m=23 با استفاده از رمز e=7 و پارامتر عمومی N=187 رمزگذاری می شود، این در حالی است که متن رمزی C=133 با استفاده از d=23 و پارامتر عمومی n=187 رمزگشایی می شود. در اینجا، کلید رمزگذاری e به صورت عمومی قابل دسترس می باشد، این در حالی است که امنیت سیستم رمزی RSA به پنهان بودن رمز خصوصی d بستگی دارد. این مثال نشانگر ماهیت قطعی سیستم رمزی RSA می باشد که در آن اگر e و n ثابت باشند، هر متن عادی m به همان متن رمزی c تبدیل می شود.
سیستم رمزی RSA امکان عملیات هم ریختی

ضربی برای داده های رمزگذاری شده را فراهم می آورد. همانطور که در تصویر ٦ مشاهده می شود، گره های برگ خوانش های حسگر را با استفاده از رمز عمومی e رمزگذاری می کنند، این در حالی است که گره های واسط محصول متن های رمزی را با استفاده از پارامتر عمومی n محاسبه می کنند. ایستگاه مرکزی متن رمزی را با استفاده از رمزخصوصی d رمزگشایی می کند. متن رمزی حاصل دریافتی در ایستگاه مرکزی در صورتی که رمزگشایی شود، نتیجه ای همانند جمع آوری متن های عادی ارائه می دهد.

۳-۵- سیستم رمزی Goldwasser–Micali

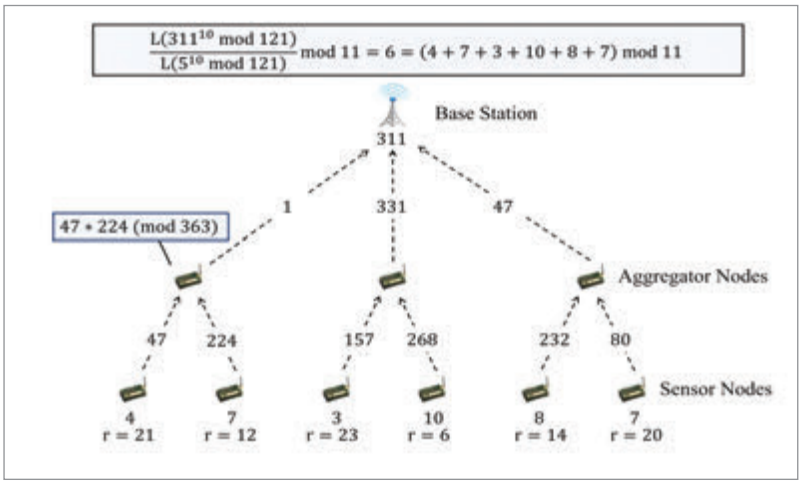
سیستم رمزی Goldwasser–Micali اولین سیستم مبتنی بر تعامل پذیری مشکل residuosity می باشد. Goldwasser و Micali به بررسی مفهوم امنیتی معنایی پرداختند. در سیستم رمزی Goldwasser–Micali، متن عادی به عنوان یک صفر یا یک ارائه می شود. همانطور که در تصویر ۷ نشان داده شده است، بیت ۱ را می توان با استفاده از رمزعمومی a و پارامتر عمومی n رمزگذاری نمود. رمزگشایی در سیستم رمزی Goldwasser–Micali به محاسبه نماد لژاندر نیاز دارد. علاوه بر این، سیستم رمزی Goldwasser–Micali به پرایم های رمزی p و q برای رمزگشایی متن رمزی نیاز دارد.

در تصویر ۸، مثالی برای نمایش رمزگذاری، رمزگشایی و مجموع عملیات در سیستم رمزی Goldwasser–Micali نشان داده شده است. همانطور که در تصویر ۸ مشاهده می شود، متن های رمزی به منظور دستیابی به اثر X-OR در متن های عادی در کره های واسط تکثیر شده اند. گره های جمع کننده نیازمند پارامتر n برای جمع آوری متن های رمزی هستند. ایستگاه مرکزی در سیستم رمزی Goldwasser–Micali، متن های رمزی جمع آوری شده را با استفاده از نماد لژاندر و پارامتر رمزی p رمزگشایی می کند.

۴-۵- سیستم رمزی Okamoto-Uchiyama

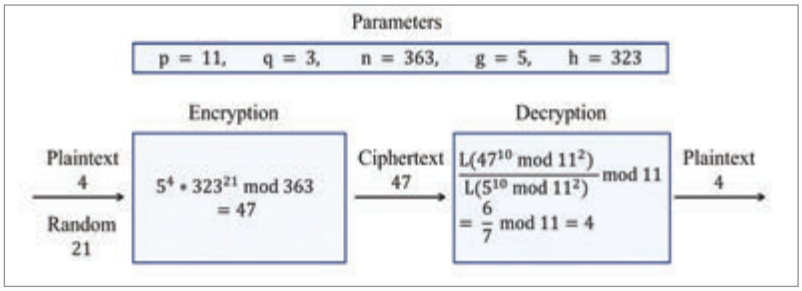
Okamoto و Uchiyama نیز یک سیستم افزایشی ایمن هم ریخت را پیشنهاد کردند. این سیستم رمزی تحت فرضیه زیرمجموعه p از نظر معنایی ایمن می باشد. ایمنی سیستم رمزی Okamoto–Uchiyama به تعامل پذیری فاکتورگیری n=p2q بستگی دارد. با این حال، سریعترین الگوریتم برای فاکتورگیری n تعداد الگوریتم های میدانی می باشد. مدت زمان اجرای الگوریتم نیز به اندازه n بستگی دارد. از این رو، پارامترهای سیستم رمزی Okamoto–Uchiyama باید به گونه ای انتخاب شوند که اندازه n=p2q همانند اندازه n=pq در سیستم رمزی RSA ۱۰۲٤ بیتی برابر باشد. همانطور که در تصویر ۹ نشان داده شده است، سیستم رمزی Okamoto–Uchiyama از عدد تصادفی r و متن عادی p برای ایجاد متن رمزی c استفاده می کند. رمزگذاری با استفاده از رمزهای عمومی g و h انجام می گیرد، این در حالی است که رمزگشایی با استفاده از رمز شخصی p انجام می شود. عملیات جداسازی در سیستم رمزی Okamoto–Uchiyama نیازمند ضرب معکوس مخرج می باشند.

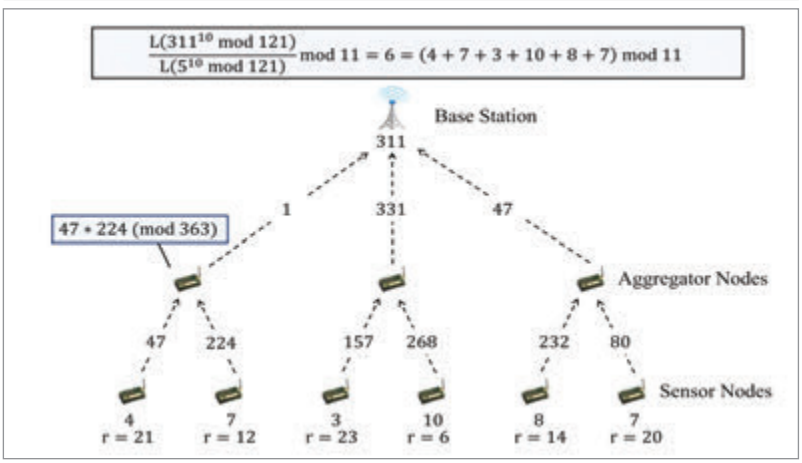
عملیات رمزگذاری، رمزگشایی و جمع آوری در یک توپولوژی جمع آوری داده مبتنی بر درخت در تصویر ۱۰ نشان داده شده اند. در سیستم رمزی Okamoto–Uchiyama، متنهای رمزی به منظور دستیابی به تاثیر افزایشی بر روی متن عادی مربوطه، ضرب می شوند. گره های جمع کننده از پارامتر همومی n برای جمع بندی متن های رمزی استفاده می کنند.



تصویر ۸- جمع آوری داده مبتنی بر درخت با استفاده از سیستم رمزی Goldwasser-Micali

تصویر ۹- رمزگشایی و رمزگذاری با استفاده از سیستم رمزی Goldwasser-Uchiyama



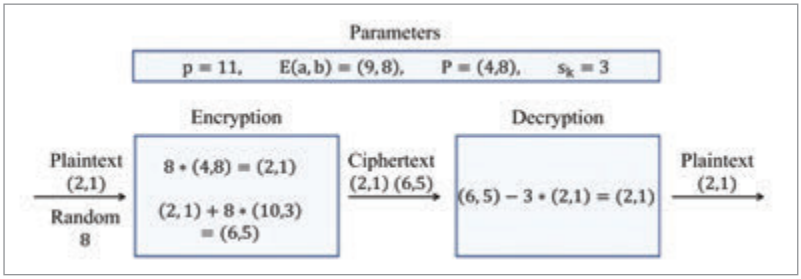


تصویر ۱۰- جمع آوری مبتنی بر درخت با استفاده از سیستم رمزی Okamoto–Uchiyama

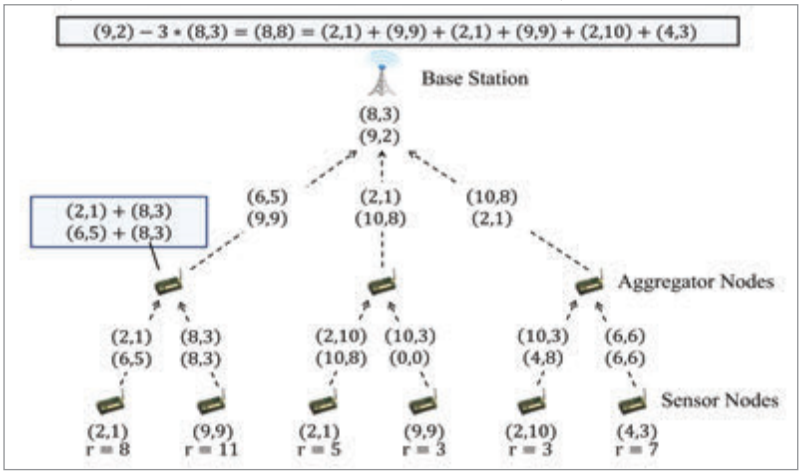
۵-۵- سیستم رمزی ElGamal مبتنی بر منحنی بیضوی

Koblitz اولین سیستم رمزی با رمز نامتقارن مبتنی بر منحنی بیضوی را با پشتیبانی از هم ریختی های افزایشی پیشنهاد نمود. سیستم رمزی ElGamal مبتنی بر منحنی بیضوی (EC-ElGamal) بر اساس تعامل پذیری حل مشکل لگاریتم مجزای منحنی بیضوی (ECDLP) ایجاد شده است. در سیستم رمزی EC-ElGamal، متن عادی قبل از انجام عملیات رمزگذاری، به عنوان یک نقطه منحنی بیضوی نشان داده می شود. همانطور که در تصویر ۱۱ نشان داده شده است، مثال از یک سیستم هماهنگی با مختصات x و y استفاده می کند. در این روش، مقدار متن عادی را می توان با استفاده از سایر سیستم های مختصات از جمله سیستم مختصات تصویری، سیستم مختصات Jacobian و ... نمایش داد. برای مثال، سیستم مختصات تصویری نیازمند سه مختصات x، y و z برای نمایش متن عادی به عنوان یک نقطه منحنی بیضوی می باشد. رمزگذاری در سیستم رمزی EC-ElGamal دو نقطه متن رمزی C۱ و C۲ بر روی منحنی بیضوی ارائه می دهد. رمزگشایی در سیستم رمزی EC-ElGamal یک نقطه را در منحنی بیضوی ایجاد می کند. نقطه ایجاد شده توسط عملیات رمزگشایی در منحنی بیضوی نیازمند نگاشت به مقدار متن عادی مربوطه می باشد.

تصویر ۱۲ مثالی از رمزگذاری، رمزگشایی و عملیات جمع بندی را در یک توپولوژی جمع آوری داده مبتنی بر درخت نشان می دهد. تابع نگاشت معکوس در سیستم رمزی EC-ElGamal بر پایه روش های brute-force ایجد شده اند. با این حال، بدلیل ایستگاه مرکزی غنی از منبع و فضای محدود پیام، سیستم رمزی EC-ElGamal رایج ترین سیستم رمزی با رمز نامتقارن برای ترافیک چندسویه معکوس WSN منبع محدود می باشد. در جدول ۶،۲، ما مقایسه سیستم های قابل



تصویر ۱۱- رمزگذاری و رمزگشایی با استفاده از سیستم رمزی مبتنی بر منحنی بیضوی ElGamal



تصویر ۱۲- جمع آوری داده مبتنی بر درخت با استفاده از سیستم رمزی منحنی بیضوی ElGamal

رمزی RSA از عملیات هم ریختی ضربی کار برده می شود. علاوه بر این، انسجام خوانش سیستم رمزی Goldwasser-Micali از عملیات هم ریختی X-OR و سیستم رمزی Okamoto-Uchiyama و سیستم رمزی EC-ElGamal از عملیات هم ریختی افزایشی برای داده های رمزگذاری شده پشتیبانی می کنند.

۶- نتیجه گیری

ویژگی تغییرپذیری سیستم های رمزی به دلیل تاثیر منفی آن بر روی انسجام داده های رمزگذاری شده، به عنوان یک ویژگی نامطلوب در نظر گرفته می شود. با این حال، ویژگی تغییرپذیری کاربردهای جالبی در حسگرهای شبکه بی سیم منبع محدود دارد. ویژگی تغییرپذیری در WSN ها به منظور اطمینان از حریم خصوصی خوانش های حسگر را می توان از طریق مکانیسم های دیگر در کنار حفظ حریم خصوصی خوانش های حسگر انجام داد. در این فصل، ما به بررسی الگوریتم های رمزگذاری مختلفی که در WSN ها به عنوان اطمینان از حریم خصوصی خوانش های حسگر در گره های واسط آسیب پذیر به کار برده می شوند، می پردازیم.

مباحث مربوط به الگوریتم های ارائه شده در این فصل به درک الگوریتم های پیچیده رمزنگاری کمک می کنند. سیستم های رمزی موردبحث در این فصل را می توان به سایر زمینه های تحقیقاتی نیز اعمال نمود که از جمله آنها می توان به اینترنت اشیاء، پردازش ابری و کدینگ شبکه اشاره کرد.

جدول ۲- مقایسه سیستم های رمزی قابل تغییر مبتنی بر رمز نامتقارن

سیستم رمزی	فرضیات امنیتی	عملیات هم ریختی	گسترش پیام
RSA	فاکتورگیری عدد صحیح و مشکل RSA	$\otimes$	1
Goldwasser-Micali	مشکل باقیمانده درجه دوم	X-OR	N
Okamoto-Uchiyama	فرضیه زیرمجموعه p	$\oplus$ $\ominus$ $\otimes_c$	$\frac{n}{2^{k-1}}$
EC-ElGamal	ECDLP	$\oplus$ $\ominus$ $\otimes_c$	2(+2-bit)

منابع و مراجع

1. Castelluccia, C., Chan, A. C. F., Mykletun, E., & Tsudik, G. (2009). Efficient and provablysecure aggregation of encrypted data in wireless sensor networks. ACM Transactions on Sensor Networks (TOSN), 5(3), 20:1–20:36. DOI 10.1145/1525856.1525858.

2. Castelluccia, C., Mykletun, E., & Tsudik, G. (2005). Efficient aggregation of encrypted datain wireless sensor networks. In Proceedings of the 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MOBIQUITOUS (pp. 109–117). Washington, D.C., USA: IEEE. DOI 10.1109/MOBIQUITOUS.2005.25.

3. Chan, A. C. F., & Castelluccia, C. (2008). On the (im)possibility of aggregate messageauthentication codes. In Proceedings of the International Symposium on Information Theory, ISIT (pp. 235–239). Toronto, Canada: IEEE. DOI 10.1109/ISIT.2008.4594983.

4. Dolev, D., Dwork, C., & Naor, M. (1991). Non-malleable cryptography. In Proceedings of the 23rd Annual Symposium on Theory of Computing, STOC (pp. 542–552). New Orleans, USA: ACM. DOI 10.1145/103418.103474.

5. Domingo-Ferrer, J. (2002). A provably secure additive and multiplicative privacy homomorphism. In Proceedings of the 5th International Conference on Information Security, ISC, Lecture Notes in Computer Science (Vol. 2433, pp. 471–483). Sao Paulo, Brazil: SpringerVerlag. DOI 10.1007/3-540-45811-5_37.

6. Fasolo, E., Rossi, M., Widmer, J., & Zorzi, M. (2007). In-network aggregation techniques for wireless sensor networks: a survey. Wireless Communications, 14(2), 70–87. DOI 10.1109/MWC.2007.358967.

7. Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. Journal of Computer and System Sciences, 28(2), 270–299. DOI 10.1016/0022-0000(84)90070-9.

8. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks andcountermeasures. Ad Hoc Networks, 1(2–3), 293–315. DOI 10.1016/S1570-8705(03)00008-8.

9. Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203–209. DOI 10.1090/S0025-5718-1987-0866109-5.

10. Krishnamachari, B., Estrin, D., & Wicker, S. (2002). The impact of data aggregation inwireless sensor networks. In Proceedings of the 22nd International Conference on Distributed Computing Systems, ICDCSW (pp. 575–578). Vienna, Austria: IEEE. DOI 10.1109/ICDCSW.2002.1030829.

11. Okamoto, T., & Uchiyama, S. (1998). A new public-key cryptosystem as secure as factoring. InProceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology, EUROCRYPT, Lecture Notes in Computer Science (Vol. 1403, pp. 303–318). Espoo, Finland: Springer-Verlag. DOI 10.1007/BFb0054135.

12. Ozdemir, S., & Xiao, Y. (2009). Secure data aggregation in wireless sensor networks: a comprehensive overview. Computer Networks, 53(12), 2022–2037.
DOI 10.1016/j.comnet.2009.02.023.

13. Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. InProceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques, EUROCRYPT, Lecture Notes in Computer Science (Vol. 1592, pp. 223–238). Prague, Czech Republic: Springer-Verlag. DOI 10.1007/3-540-48910-X_16.

14. Parmar, K., & Jinwala, D. C. (2016). Concealed data aggregation in wireless sensor networks: A comprehensive survey. Computer Networks, 103(7), 207–227.
DOI 10.1016/j.comnet.2016.04.013.

15. Parmar, K., & Jinwala, D. C. (2016). Malleability resilient concealed data aggregation in wireless sensor networks. Wireless Personal Communications, 87(3), 971–993. DOI 10.1007/s11277-015-2633-6.

16. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: security protocols for sensor networks. Wireless Networks, 8(5), 521–534. DOI 10.1023/A:1016598314198.

17. Peter, S., Westhoff, D., & Castelluccia, C. (2010). A survey on the encryption of convergecasttraffic with in-network processing. IEEE Transactions on Dependable and Secure Computing, 7(1), 20–34. DOI 10.1109/TDSC.2008.23.

18. Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks:
attacks and defenses. IEEE Pervasive Computing, 7(1), 74–81. DOI 10.1109/MPRV.2008.6.

19. Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. Foundations of Secure Computation, 4(11), 169–180.

20. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. DOI 10.1145/359340.359342.

21. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues inwireless sensor networks. IEEE Communications Surveys & Tutorials, 8(2), 2–23. DOI 10.1109/COMST.2006.315852