اولین همایش منطقه ای رویکردهای نوین در مهندسی کامپیوتر و فناوری اطلاعات
۵ خرداد ۱۳۹۰ - رودسر

افزایش ایمنی و قابلیت اطمینان در دستگاه‌های موبایل با استفاده از رمزنگاری مبتنی بر مکان

روح الله کریمی [1]، محمد کلانتری [2]

[1] دانشکده مهندسی برق ، رایانه و فناوری اطلاعات
دانشگاه آزاد قزوین
rukarimi@qiau.ac.ir
[2] دانشکده مهندسی برق ، رایانه و فناوری اطلاعات
دانشگاه آزاد قزوین
kalantari@qiau.ac.ir

چکیده

با تسریع رشد شبکه‌های موبایل و تکنولوژی‌های بی‌سیم، دستگاههای موبایل نیز جزء لاینفکی از زندگی ما شده اند. امروزه عموما اشخاص از این دستگاه‌ها برای ارسال و دریافت email، تجارت سیار، خریدهای اینترنتی و ... استفاده می کنند. این سرویس‌ها و برنامه‌ها به جهت ایمنی بیشتر باید از امضای دیجیتال پشتیبانی کنند. بدلیل اینکه دستگاه‌های موبایل توانایی محاسباتی اندک و باطری محدودی دارند، پروتکل های امضای دیجیتال قدیمی با محاسبات زیاد که مبتنی بر الگوریتم‌های رمزنگاری نامتقارن هستند برای استفاده در این دستگاه‌ها مناسب نیستند. بعلاوه این الگوریتم‌ها مستقل از مکان هستند و از مزایای تکنولوژی GPS نیز بهره نمی‌برند. در این مقاله ما یک تکنیک رمزنگاری مبتنی بر مکان برای داده‌ها با بهره‌گیری از ویژگی‌های تکنولوژی GPS ارائه می‌کنیم. در این روش گیرنده پیام، تنها هنگامی که در محدوده مکانی (و زمانی) مورد نظر فرستنده قرار داشته باشد می تواند پیام‌های رمز شده را رمزگشایی کند. همچنین بدلیل دقت پایین و وجود خطا در GPS خوانها، فاصله تحمل پویا نیز در کلید ما به منظور کاهش خطا و افزایش قابلیت اجرای طرحمان گنجانده شده است. آزمایشات صورت گرفته نشان می‌دهند که پیام رمزشده تنها می‌تواند در محدوده فاصله تحمل مورد نظر رمزگشایی شود. همچنین این روش زمان انجام محاسبات و ارتباطات بین فرستنده و گیرنده را بطور قابل توجهی کاهش می‌دهد. نتایج برنامه‌ها نشان می‌دهند که این طرح برای سیستمهای ارتباطی موبایل بسیار مفید هستند.

کلمات کلیدی

امنیت، دستگاه موبایل، رمزنگاری مبتنی بر مکان، GPS.

1- مقدمه

گرایش غالب در ارتباطات راه دور در سال ها یاخیر به سمت ارتباطات موبایل است. نسل آینده شبکه در کشور ما نیز، بیش از پیش از شبکه‌های موبایل فقط صوتی امروزی به شبکه هلی چند سرویسی که قادر به حمل داده ها و سرویس‌های ویدئویی، اینترنتی و ... در کنار سرویس صوتی سنتی هستند، گسترش خواهد یافت. همچنین با رشد صنعت موبایل و توجه به توسعه روزافزون تکنولوژی شبکه‌های بی‌سیم، ما می توانیم از دستگاه های موبایل در هر زمان و مکانی بمنظور دستیابی به اینترنت استفاده کنیم. اما باید توجه داشت که بسیاری از برنامه های کاربردی در دنیای وب از قبیل سیستمهای تجاری سیار، سیستم بلیط الکترونیکی، پول الکترونیکی و غیره، برای انجام صحیح وظایف خود نیازمند امنیت هستند.

امضای دیجیتال می‌تواند بعنوان مبنای ایمنی در یک چنین برنامه‌هایی ارائه شود زیرا تایید و تصدیق، جامعیت داده‌ها و سیستم‌های رمزنگاری غیر قابل انکار را فراهم می‌کند. طرحهای امضای دیجیتالی قدیمی که مبتنی بر تکنیک‌های رمزنگاری نامتقارن هستند باعث می‌شوند تا محاسبه امضا بسیار پرهزینه گردد. باید توجه داشت که علی رغم اینکه دستگاه‌های موبایل دارای انواع و اشکال مختلفی هستند و برای اهداف مختلفی استفاده می‌شوند، محدودیت‌هایی نیز دارند که از آن جمله می توان به توانایی انجام محاسبات محدود و توان باطری ضعیف اشاره کرد.

اگر محاسبات رمزنگاری نامتقارن قدیمی در دستگاه های موبایل بکار گرفته شوند، این دستگاه‌ها در زمان کوتاهی از کار خواهند افتاد و به سرعت باطری آنها تمام می شود. علاوه بر این امضاهای دیجیتال مرسوم برای تضمین اینکه تنها کاربران مجاز می‌توانند به محتوای امن اطلاعات دسترسی داشته باشند، مورد استفاده قرار می گیرند. اما با این حال، شرایطی وجود دارد که در آن امنیت ارائه شده توسط امضاهای دیجیتال سنتی کافی نیست. در بسیاری از موارد لازم است که یک لایه اضافی امنیتی داشته باشیم که تضمین دهد محتوای امن اطلاعات تنها می‌تواند در مکان و یا زمان‌های مجاز مورد استفاده قرار گیرد[1]. مفهوم رمزگذاری مبتنی بر مکان یا geoencryption برای برآورده نمودن چنین اهدافی بوجود آمده و درحال توسعه است. این قابلیت مزایای بالقوه فوق العاده ای برای برنامه‌های کاربردی دارد که از آن جمله می‌توان به مدیریت دسته بندی / امنیت داده ها، ارائه سرویسهای مبتنی بر مکان ایمن و یا توزیع فیلم‌های دیجیتال که در آن کنترل دسترسی نگرانی اصلی است اشاره نمود[2].

در این مقاله ما روش جدیدی از امنیت کلید را ارائه می کنیم که در آن کلید نهایی از ترکیب یک کلید تصادفی با مختصات بدست آمده از مکان گیرنده مورد نظر حاصل می شود. دریافت کننده تنها در صورتی قادر به رمزگشایی پیام خواهد بود که در مکان (و یا زمان) مورد نظر، قرار داشته باشد. طبیعتا برای گیرنده، رمزگشایی پیغام رمزشده دقیقا در همان محلی که با مختصات هدف مطابق می‌باشد، بسیار مشکل خواهد بود. در واقع استفاده از مختصات غیر دقیق GPS به عنوان یک کلید برای رمزنگاری داده‌ها غیر عملی است. در نتیجه برای حل این مشکل، ما فاصله تحمل پویا یا DTD را درکلید خود گنجانده‌ایم. گره موبایل فرستنده مقدار DTD را تعیین می‌کند و گیرنده می تواند پیغام رمزشده را در محدوده DTD رمزگشایی کند.

دنباله این مقاله این چنین طبقه بندی شده است : در بخش 2 به مرور ادبیات و کارهای مرتبطی که قبلا در این حوزه صورت گرفته و بیان نقاط ضعف آنها پرداخته و نیز ویژگیها و نوآوریهایی که در طرح خود برای غلبه بر این نقاط ضعف لحاظ کرده ایم را بیان می‌نماییم. در بخش 3 به تشریح پروتکل اصلاح شده و پیشنهادی رمزنگاری مبتنی بر مکان خود خواهیم پرداخت. در بخش 4 به بررسی نقاط ضعف کلی در پروتکل‌های رمزنگاری مبتنی بر مکان موجود و راهکارهای مقابله با آنها در پروتکل پیشنهادی خود می پردازیم. در بخش 5 نیز به پیاده‌سازی این پروتکل و ارزیابی کارایی و ایمنی آن می پردازیم و نهایتا در بخش 6 نتیجه گیری ارائه خواهد شد.

2- مرور ادبیات

تاکنون تحقیقات مختلفی در زمینه رمزنگاری مبتنی بر مکان اطلاعات در شبکه‌های بی سیم صورت گرفته است، که از آن جمله می‌توان به موارد زیر اشاره کرد :

در سال 2008 آقایان Hsien-Chou و Yun-Hsiang یک الگوریتم رمزگذاری داده‌های مبتنی بر مکان به نام LDEA را ارائه کردند. اما این پروتکل به اندازه کافی قوی نمی باشد زیرا در طرح آنها مکان گره موبایل ثابت و ایستا در نظر گرفته شده است[3].

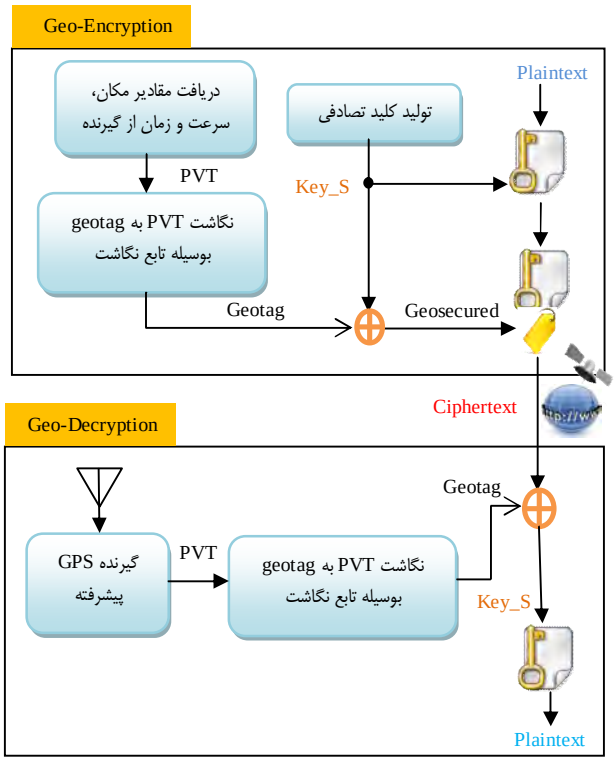
در سال 2007 نیز Ala و Omar یک پروتکل geoencryption را با محدود کردن رمزگشایی یک پیام به یک محل و زمان خاص، پیشنهاد کردند. رمزگذاری و رمزگشایی در این پروتکل نیز محدود به یک محل ثابت است و نمی تواند برای نودهای متحرک و پویا مورد استفاده قرار بگیرد [4].

همچنین فعالیتهایی نیز در زمینه امضاهای دیجیتال بر روی دستگاه های موبایل انجام شده است. برای مثال Asokan یک طرح server–supported signature را برای ارتباطات موبایل مطرح کرده است[5]. در طرح آنها سرورهای امضا مسئول تولید توکن امضا و گواهینامه های دیجیتال برای تایید این توکن‌ها بودند. بنابراین امنیت و قدرت امضاهای دیجیتال بستگی به اطمینان به این سرورها دارند. بر مبنای کار اقای Asokan آقای Ding یک طرح امضای دیجیتال اصلاح شده تحت عنوان server aided signature ارائه کرده است[6]. در این طرح کاربران درگیر تولید توکن امضا می باشند. این طرح متفاوت با امضاهای دیجیتالی قدیمی است که اغلب در آنها از جفت کلیدهای عمومی و خصوصی برای تولید توکن‌های امضای غیرقابل انکار استفاده می شد اما هر دو آنها از یک تابع هش یکطرفه جهت تولید کلید خصوصی فرستنده و بکارگیری این کلید برای تولید توکن امضای غیرقابل انکار استفاده می کنند.

در این طرح نیز هنوز محاسبات رمزنگاری نامتقارن برای کاربران پرهزینه است زیرا در مدت تایید امضای دیجیتال، دریافت کنندگان باید توکن‌های امضای رمزنگاری شده را به منظور تایید محتوای اضافه شده توسط سرور امضا رمزگشایی کنند. بنابراین به منظور افزایش ایمنی و قابلیت استفاده ما مدلی ارائه کرده‌ایم که در آن گره‌های موبایل گیرنده و فرستنده امکان تحرک و جابجایی را بصورت پویا خواهند داشت. همچنین ما بجای فاصله تحمل استاتیک ، فاصله تحمل پویا را بکار گرفته ایم که این امر پروتکل ما را در برابر حملات احتمالی بسیار قوی می کند.

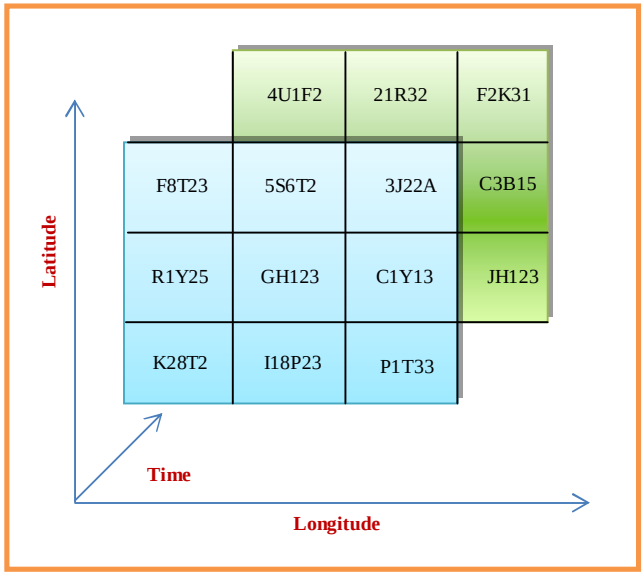
3- تشریح مدل پیشنهادی

با پیشرفت تکنولوژیهای دستگاه‌های موبایل و ترکیب آنها با GPS خوانها ، ما می‌توانیم از این مزیت برای رمزنگاری مبتنی بر مکان که اصطلاحا Geo-Encryption نیز نامیده می شود، استفاده کنیم. رمزنگاری مبتنی بر مکان یک تکنیک رمزنگاری است که موقعیت و زمان را در داخل فرایند رمزنگاری و رمزگشایی ترکیب می کند بطوریکه لایه های امنیتی بیشتری- فراتر از آنچه در رمزنگاری‌های مرسوم تولید می‌شود- ایجاد می‌نماید.



شکل (1): پروتکل geoencryption پیشنهادی

شکل 1 نمایی کلی از نحوه کار الگوریتم Geo-Encryption را نشان می‌دهد. یک الگوریتم نگاشت در طول فرایند رمزنگاری جهت نگاشت مختصات جغرافیایی، زمان و سرعت حرکت گیرنده (PVT) به مقدار منحصر بفرد geotag به منظور ترکیب با یک کلید متقارن تصادفی، برای تولید کلید نهایی geosecured جهت انتقال با پیام استفاده می‌شود.



شکل (2): تابع نگاشت برای تولید مقادیر مختلف geotag

همانگونه که در شکل 2 ملاحظه می‌شود مقدار geotag از ارسال مقادیر مکان، سرعت و زمان به این الگوریتم، حاصل می‌شود.

مقدار geotag در واقع برای تولید کلید geosecured از کلید متقارن و همچنین بازیابی کلید متقارن از کلید geosecured مورد استفاده قرار می‌گیرد. در ادامه و در بخش 4 بطور کامل در مورد الگوریتم نگاشت PVT به geotag صحبت خواهیم کرد.

رمزنگاری GEO هنگامی قابل اجرا خواهد بود که فرستنده موقعیت و مکان فعلی یا آتی دریافت کننده را بداند. بسادگی قابل درک است که در صورتیکه گیرنده ثابت و فاقد تحرک باشد، انجام عمل geoencryption بسیار ساده تر از زمانی خواهد بود که گیرنده متحرک و در حال حرکت می‌باشد. در حالت اول و برای گیرنده‌های ثابت و فاقد تحرک، تنها کافی است که موقعیت فعلی گیرنده از قبل به فرستنده اعلام شود. اما در حالت دوم و برای گیرنده‌های متحرک فرستنده باید قادر به تعیین معادله مسیر حرکت گیرنده و تعیین مکان آتی وی در زمان مورد نظر باشد.

ما قبلا در مقاله ای با عنوان "افزایش ایمنی سرویسهای مبتنی بر موقعیت کاربران در شبکه های موبایل"[7] به تفصیل در مورد مسیریابی و نحوه محاسبه معادلات مسیر گره متحرک صحبت کرده‌ایم. ما قصد داریم در بخش بعدی و در ادامه این مقاله به بررسی نقاط ضعف پروتکل‌های رمزنگاری مبتنی بر مکان موجود و راهکارهایی که سبب افزایش ایمنی در پروتکل پیشنهادی ما می گردد بپردازیم و در نهایت با شبیه سازی این پروتکل تلاش می کنیم تا نشان دهیم توانسته‌ایم سطح ایمنی و قابلیت اطمینان و کارایی آنرا تا حدودی ارتقا دهیم.

4- راهکارهای افزایش ایمنی در مدل پیشنهادی

تجزیه و تحلیل ایمنی یک پروتکل دشوار و پیچیده است زیرا هیچ معیار استانداردی برای اندازه گیری دقیق موضوع امنیت وجود ندارد[8,14]. امنیت یک سیستم رمزنگاری نه تنها بستگی به طراحی پروتکل دارد بلکه به پیاده سازی آن نیز وابسته است. بطور کلی ، برای پیاده سازی geoencryption دستگاهی که رمزگشایی را انجام می‌دهد باید شامل یک حسگر مکانی و الگوریتمهای رمزنگاری مبتنی بر مکان مربوطه باشد. اما نگرانی اصلی در ساخت و پیاده سازی چنین دستگاهی این است که آیا می‌توان آن را در برابر حملات و دسترسی‌های غیر مجاز مقاوم ساخت یا خیر. منظور ما از حملات، هم شامل حملات فیزیکی به سخت افزار و هم حملات به پیاده سازی مانند جعل هویت است. اگر دستگاه در معرض دسترسی‌های غیر مجاز باشد ممکن است برای دشمن مقدور باشد که اطلاعات مکانی را تغییر دهد و عمل چک کردن مکان را دور بزند[9,10]

4-1- بررسی انواع حملات ممکن

افزودن امنیت به یک سیستم ارتباطی موبایل بدلیل وجود کاربران متعدد نامعتبر و غیر مجاز و محیط های ارتباطی غیر قابل اطمینان موضوع پیچیده و دشواری است. در این قسمت قصد داریم تا

به بررسی نقاط ضعف پروتکل‌های مشابه موجود بپردازیم. منظور ما از نقاط ضعف هر نوع حمله احتمالی است که ممکن است این پروتکل را تضعیف یا تهدید کند. بنابراین لازم است که از قبل به همه انواع حملات احتمالی و راه های مقابله با آن فکر کنیم. در یک دسته‌بندی کلی این حملات را می توان به سه دسته زیر تقسیم کرد :

- حمله مبتنی بر جعل هویت

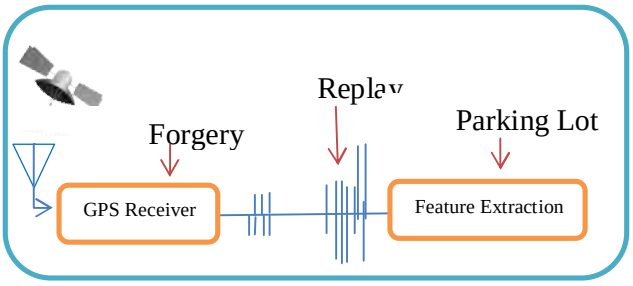
مهاجم سیگنال مسیریابی RF را به منظور جعل هویت و به اشتباه انداختن گیرنده شبیه سازی می کند.

- حمله تکرار :

مهاجم به منظور کلاه گذاشتن بر سر گیرنده، اطلاعات مکانی تغییر یافته و جعلی را برای وی ارسال می کند.

- حمله موسوم به پارکینگ :

مهاجم با یک نگاشت احتمالی از مکان کاربر به گیرنده پاسخ می‌دهد.



شکل (3): انواع حملات ممکن به سیستم GEO

شکل 3 نحوه وقوع این حملات را نشان می‌دهد. به دلیل اینکه هدف از بکارگیری این شیوه رمزنگاری، افزایش ایمنی در انتقال اطلاعات است، برای ما بسیار مهم خواهد بود که هر یک از حلقه‌های زنجیره سیستم geoencryption امن باشد. این امر نه تنها شامل خود پروتکل geoencryption می‌شود، بلکه پخش و انتشار سیگنالهای RF را نیز در بر می‌گیرد. امنیت سیگنال ناوبری RF بوسیله پیام احراز هویت تامین می‌شود. احراز هویت مربوط به تایید و بررسی منبع داده‌ها و پیامها است. یکی از اهداف احراز هویت جلوگیری از این باور اشتباه کاربر مبنی بر آمدن پیامها از یک منبع خاص است در هنگامی که واقعا این چنین نیست. هدف دیگر آن این است که به گیرنده اجازه دهد تا مطمئن شود که آیا پیام ها در زمان انتقال، تغییر داده شده‌اند یا خیر[11,12].

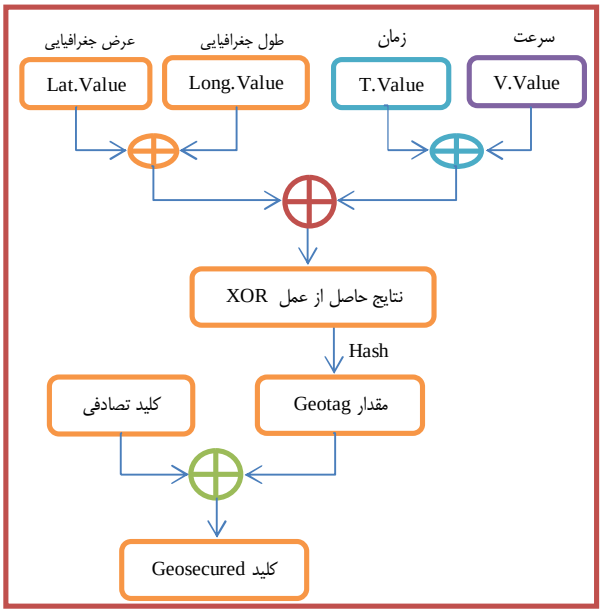
4-2- راهکارهای پیشنهادی

تصدیق یا احراز هویت منبع به گیرنده کمک می کند تا تأیید نماید که آیا داده‌های دریافتی واقعا از منبع مورد نظر می آیند و یا اینکه در راه انتقال تغییر یافته‌اند. به منظور احراز هویت منبع سیگنال‌های رادیویی ناوبری RF و محافظت در برابر جعل هویت، قبلا مطالعاتی صورت گرفته و در جهت حل مشکلات موجود در این زمینه یک پروتکل تصدیق سیگنال به نام TESLA ارائه شده است [10].

TESLA از مکانیزم احراز هویت متقارن برای رسیدن به ویژگی عدم تقارن که برای یک احراز هویت پخشی امن مورد نیاز است، استفاده می‌کند. اما این شیوه بدلیل پیچیدگی محاسباتی بالا، سرباز زیادی را به سیستم تحمیل می کند[13].

بجای استفاده از این پروتکل پرهزینه، ما می توانیم علاوه بر اینکه هر پیام را بطور مجزا بوسیله تکنیک geoencryption رمز می‌کنیم، از یک تابع MAC نیز در انتهای هر پیام استفاده کنیم. بدین طریق مهاجمین نمی‌توانند سیگنال ها را شبیه سازی کنند یا از هر وسیله دیگری برای فریب دادن GPS خوانها استفاده کنند، زیرا آنها کلید مورد استفاده در تابع MAC را در اختیار ندارند. بنابراین اگر یک دسترسی غیر مجاز رخ دهد یا مهاجم یک پیام جعلی ارسال نماید، سیستم متوجه آن می‌شود و آن پیام را نادیده می‌گیرد و کل فرایند با شکست مواجه خواهد شد. بنابراین پیامهایی که واقعا از سوی فرستنده ارسال شده باشند، از پیامهای جعلی تمیز داده شده و مجزا خواهند شد و در نهایت تنها از این پیامها رمزگشایی خواهد شد.

اگر پروتکل رمزنگاری خوب طراحی شده باشد و هیچ حمله تحلیلی یا ضعف ساختاری در آن وجود نداشته باشد، سطح ایمنی سیستم بستگی به قدرت کلید geotag خواهد داشت. بنابراین یک معیار مهم امنیت در پروتکل geoencryption استفاده از یک مکانیزم ایمن برای تولید کلید geotag است. شکل 4 مکانیزم پیشنهادی ما برای تولید یک geotag قوی و ایمن را نمایش می دهد.



شکل (4) : مکانیزم پیشنهادی ما برای تولید یک geotag قوی

5- شبیه سازی و نتایج آن

در این بخش یک نمونه اولیه از پروتکل ارائه شده برای نشان دادن نحوه کار و ارزیابی و تجزیه تحلیل ایمنی آن شبیه سازی سازی شده

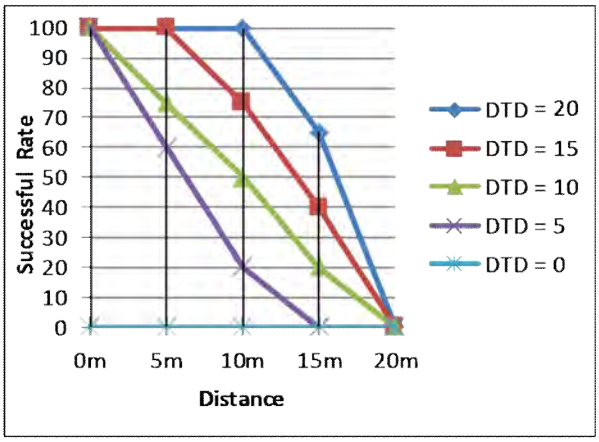
است. مراحل مختلف شبیه سازی به همراه تصاویری از فرمهای مربوطه در انتهای مقاله و در شکل 5 نشان داده شده است. شکل الف، شبیه ساز دستگاه موبایل را قبل از اجرای برنامه نشان می دهد. شکل ب، صفحه ورودی کاربر را نمایش می دهد که بیانگر نحوه عمل رمزنگاری برای فرستنده و رمزگشایی برای گیرنده می‌باشد. در شکل پ، کاربر فایل plaintext خود را جهت انجام عمل رمزنگاری انتخاب کرده و همینطور مکان و نامی برای ذخیره فایل ciphertext حاصل از رمزنگاری متقارن اولیه تعیین کرده و با کلید مخفی که در اختیار دارد اقدام به رمزنگاری می‌کند.

در شکل ت، کاربر مختصات گیرنده را در قالب پیام‌های بروز رسانی دریافت کرده و طول و عرض جغرافیایی، سرعت و زاویه حرکت وی را بدست می‌آورد و اقدام به تخمین مکان وی برای t ثانیه بعد می‌کند. سپس همانطور که در شکل ث مشاهده می‌کنید مختصات گیرنده در زمان مورد نظر محاسبه شده و فرستنده فاصله تحمل مورد نظر را انتخاب کرده و کلید Geotag را تولید می نماید. فایل رمزشده نهایی به روش Geoencryption در شکل ج نمایش داده شده است. پس از تهیه ciphertext و ارسال آن به گیرنده باید بتوانیم آن را رمزگشایی کنیم. همانطور که در شکل چ ملاحظه می کنید ابتدا موقعیت دریافت کننده چک می شود و تنها در صورتیکه مختصات به دست آمده محدودیت مختصات هدف و فاصله تحمل مورد نظر را رعایت کند و گیرنده در موقعیت صحیح و پیش بینی شده قرار داشته باشد، به مرحله بعد خواهد رفت و قادر به رمزگشایی فایل خواهد بود. در مرحله آخر و بعد از تایید شدن مکان کاربر همانطور که در شکل ح دیده می شود وی قادر به رمزگشایی فایل ciphertext با کلید مخفی خود خواهد بود.

5-1- تجزیه و تحلیل نتایج

قدرت کلید بستگی به مکان فعلی گیرنده موبایل و اندازه DTD دارد. بنابراین، احتمال شکستن کلید ما صفر و غیر ممکن است زیرا هیچ کسی مختصات برآورد شده را تا زمانی که در این موقعیت قرار نگرفته نمی داند کلید تصادفی با کلید مخفی ترکیب می‌شود که این باعث می‌شود تا کلید نهایی بسیار قوی شود. پروتکل ما مبتنی بر الگوریتم DES و MD5 hash می‌باشد. هرچند، این روش انعطاف پذیر است و می تواند با الگوریتم های دیگر مانند AES، triple-DES و غیره نیز ترکیب شود اما بدلیل کارایی بالاتر الگوریتم DES نسبت به سایر الگوریتمهای رمزنگاری متقارن از این الگوریتم استفاده کرده ایم. اثبات این مطلب به همراه مقایسه کارایی الگوریتمهای رمزنگاری نامتقارن قبلا در مقاله ای از اینجانب با عنوان "تحلیل و ارزیابی الگوریتمهای رمزنگاری نامتقارن" مورد بحث و بررسی قرار گرفته است[15].

ما این پروتکل را با انتخاب DTD های مختلف بررسی و نتایج را با هم مقایسه کرده ایم. مطالعه تحلیلی بر روی میزان موفقیت در رمزگشایی پیغامهای دریافتی را در نمودار 6 مشاهده کنید.



شکل(6) : نرخ موفقیت به ازای DTD های مختلف

اکنون ما روش پیشنهادی مان را از نظر تامین چهار فاکتور مهم موضوع امنیت از جمله قابلیت اطمینان، احراز هویت، سادگی و قابلیت اجرا، مورد بحث قرار می دهیم.

1) قابلیت اطمینان

تنها فرستنده و گیرنده مورد نظر دارای کلید تصادفی هستند و باید از یک کلید تصادفی متقارن یکسان برای رمزگشایی موفقیت آمیز پیام استفاده کنند. این کلید برای هر session مجزا تغییر می کند. این کار باعث جلوگیری از حمله ciphertext-only می شود.

2) احراز هویت

گیرنده باید کلید تصادفی متقارن و تابع MAC صحیح را به منظور ارائه درخواست خود به فرستنده بداند. اگر حمله کننده از حمله تکرار استفاده کند، عمل رمزگشایی شکست خواهد خورد زیرا کلید تصادفی صحیح را نمی‌توان مشخص نمود و نهایتا فرستنده از درخواست مهاجم چشم پوشی می کند.

3) سادگی

ما در روش خود تنها از یک الگوریتم رمزنگاری متقارن ساده و عمل XOR استفاده کرده ایم. این کار سبب می‌شود تا اجرای پروتکل پیشنهادی ما بر روی دستگاه موبایل که منابع و توانایی محاسباتی محدودی دارند کارا و ساده باشد.

4) قابلیت اجرا

سیستم اطلاعاتی موبایل یک نیاز مبرم در آینده است. قدرت ایمنی در روش ما هنوز هم می تواند با توجه به سطح ایمنی مورد نیاز و با جایگزین کردن الگوریتم های رمزنگاری دیگر بهبود یابد. به عنوان مثال، حداکثر طول کلید Triple-DES و AES به ترتیب برابر با 168 و 256 بیت است که قدرت آن قوی تر از DES با طول کلید 16 بیت است که ما در اینجا از آن استفاده نمودیم. اما این افزایش ایمنی متناظر با تحمیل سربارهای محاسباتی و اتلاف انرژی بیشتر خواهد بود.

شکل (5) : تصاویری از شبیه سازی فرایند رمزنگاری (الف تا ج) و رمزگشایی (چ و ح) پیام.

6- نتیجه گیری

تکنولوژی های رمزگذاری مرسوم قادر به محدود کردن مکان گیرنده متحرک برای رمزگشایی داده ها نیستند. به منظور برآورده کردن نیازهای امنیتی سیستم‌های اطلاعاتی موبایل در آینده نزدیک، در این مقاله، ما یک پروتکل رمزنگاری مبتنی بر مکان ارائه کردیم و در آن تا حدودی نقاط ضعف پروتکل‌های موجود دیگر را از نقطه نظر کارایی و ایمنی بهبود بخشیدیم. همچنین به منظور کاهش خطای تخمین مختصات احتمالی، ما از فاصله تحمل پویا استفاده می‌کنیم.

پروتکل پیشنهادی ما می تواند چهار فاکتور مهم موضوع امنیت یعنی قابلیت اطمینان، احراز هویت، سادگی، و قابلیت اجرا را برآورده سازد. در نتیجه، این روش برای انتقال داده ها بین سیستمهای اطلاعاتی و دریافت کنندگان موبایل خدمات آنها، موثر و عملی است.

همچنین این پروتکل می تواند در بسیاری از برنامه ها در حوزه نرم‌افزار بکار گرفته شود، به عنوان مثال در مجوز استفاده از یک نرم افزار موبایل. اگر استفاده از یک نرم افزار موبایل تنها در داخل یک منطقه از پیش تعریف شده، مانند یک شهر، مجاز باشد، اجرای نرم‌افزار نیاز به چک کردن مکان بر اساس پروتکل پیشنهادی ما خواهد داشت. نرم‌افزار تنها زمانی که کاربر در داخل منطقه مجاز باشد قابل اجرا خواهد بود. علاوه بر این، پروتکل پیشنهادی ما ممکن است در توزیع محتوای چند رسانه ای به منظور انجام کنترل دسترسی پیشرفته، به غیر از کنترل نام کاربری و رمز عبور، نیز مورد استفاده قرار بگیرد.

کارهای آینده شامل مطالعه و بررسی بیشتر پارامترهای مبتنی بر مکان قابل استفاده برای تولید geotag مستحکم تر و بسط و توسعه دادن الگوریتم تولید کلید geotag به منظور بهبود کارایی سیستم می‌باشد.

مراجع

[1] L. Scott, D. Denning, "*A Location Based Encryption Technique and Some of Its Applications*", Proceedings of ION NTM 2003.

[2] L. Scott, D. Denning, "*Location Based Encryption & Its Role In DigitalCinema Distribution*", Proceedings of ION GPS/GNSS 2003, pp288-297.

[3] L.Hsien-Chou, C.Yun-Hsiang, "*A New Data Encryption Algorithm Based on the Location of Mobile Users*", Info. Tech. J. , 2008.

[4] Al.Omar, Al.Ala, D.Dyk, N.Akerman, "*Mobility Support for Geo-Encryption*", IEEE ICC International Conference, 2007.

[5] N.Asokan, G.Tsudik, M.Waidner, "*Server-supported signatures*", Journal of Computer Security, Volume 5, Issue 1, pages 91–108, January 1997.

[6] Xuhua Ding, Daniele Mazzocchi, Gene Tsudik, "*Experimenting with Server-Aided Signatures*", In Proceedings of Network and Distributed System Security Symposium (NDSS'2002), San Diego, 2002.

[7] R.Karimi, "*Providing safe location-based services in mobile networks by Location-based Data Encryption Algorithm*", In the First National Conference on new Approaches in computer engineering, 2011.

[8] H.Liao, P.Lee, Y.Chao, C.Chen, "*A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security*", In The 9th International Conference on Advanced Communicate Technology, pp. 625-626, Feb. 2007.

[9] G.Yan, "*Providing Location Security in Vehicular ad hoc Networks*", Ph.D. Thesis, Old Dominion University, May 2010.

[10] D. Qiu, "*Geoencryption Using Loran*", Proceeding of ION NTM 2007.

[11] P.Reddy, K.R.Sudha, S.Krishna Rao, "*Data Encryption technique using Location based key dependent Permutation and circular rotation*", International Journal of Computer and Network Security, March 2010.

[12] H.Hamad, S.Elkourd, "*Data encryption using the dynamic location and speed of mobile node*", Journal Media and Communication Studies Vol. 2, pp.67-75, March 2010.

[13] P Sanyasi Naidu, P.Reddy, K.R.Sudha, "*A Modified Location-Dependent Data Encryption for Mobile nformation System with Interlacing, key dependent Permutation and rotation*", International Journal of Computer and Network Security, Vol.2, No.5, May 2010.

[14] G.Yan, S.Olariu, "*A probabilistic analysis of link stability in vehicular ad hoc networks*", IEEE Transactions on Intelligent Transportation Systems, 2010.

[15] R.Karimi, "*Performance Evaluation of Symmetric Encryption Algorithms*", In the First National Conference on Software Engineering, 2008.