



طراحی و پیاده‌سازی رمزکننده بلادرنگ مکالمات موبایل

عباس ریاضی^۱، سمیراسادات شفیعی^۲، هادی شهریار شاه حسینی^۳

^۱دانشگاه علم و صنعت ایران

a.riazi@misbah3com.com

^۲دانشگاه علم و صنعت ایران

shafiee@misbah3com.com

^۳دانشکده مهندسی برق، دانشگاه علم و صنعت ایران

hshsh@iust.ac.ir

چکیده

از آنجا که مکالمات در سیستم GSM توسط تجهیزات مدرن قابل ردگیری و شنود است و با توجه به اهمیت مکالمات صورت گرفته توسط مقامات نظامی یا دولتی، ضرورت ساخت تجهیزات سخت افزاری یا نرم‌افزاری جهت رمز کردن مکالمات موبایل آنهم بصورت بلادرنگ به وضوح دیده می‌شود. با توجه به پیشرفت سریع تکنولوژی و ساخت گوشیهای تجاری جدیدی که دارای پردازنده‌های تا ۴۰۰ مگاهرتز و گاهی اوقات بیشتر هستند، تلاش شده است که یک محصول نرم‌افزاری مبتنی بر ویندوز موبایل (Windows CE 4.x) طراحی گردد تا بدینوسیله امکان مکالمات بلادرنگ موبایل و همچنین دیگر امکانات مخابراتی نظیر ارسال پیام کوتاه رمز شده و غیره را فراهم آورد.

واژه‌های کلیدی

رمزکننده مکالمات موبایل، ارتباطات امن، Secure Mobile Communication

۱- مقدمه

در این مقاله به ارایه روشی پرداخته شده است که با رعایت استانداردهای موجود و با سازگاری کامل با تمامی تجهیزات و امکانات فعلی، بتوان یک ارتباط امن انتها به انتها ایجاد نمود. در ادامه در قسمت ۲ مروری بر فناوریهای تلفن همراه و در بخش ۳، رمزنگاری در GSM مورد بررسی قرار گرفته است. در بخشهای ۴ تا ۷ اجزای نرم‌افزاری و سخت افزاری مورد نیاز جهت پیاده‌سازی یک رمزکننده بلادرنگ مکالمات موبایل ارائه خواهد شد. بخش ۸ به نتیجه گیری و روشهای ادامه کار اختصاص یافته است.

۲- مروری بر فناوریهای تلفن همراه

GSM استاندارد است که توسط اتحادیه اروپا وضع شده و به شدت مورد استقبال عرضه کنندگان تجهیزات مخابراتی و همچنین عموم مشترکان این نوع خدمات قرار گرفته است. هم اکنون تعداد مشترکین شبکه‌های GSM در دنیا بالغ بر یک میلیارد نفر بوده (که ۷۵٪ از سهم بازار موبایل دنیا را در اختیار دارد) و بدلیل رشد بیسابقه این فناوری در تمامی دنیا، سعی شده

ارتباطات و مخابرات یکی از ارکان اصلی زندگی روزمره بشر است به نحوی که زندگی بدون آن یا بسیار سخت بوده و یا محال می‌باشد. تکنولوژیهای بسیار متنوع و پیشرفته‌ای که در تمامی شئون زندگی بشر فقط در عرصه ارتباطات پدیدار گشته است، موجد همین مطلب است. در بسیاری از ارتباطات صورت گرفته امکان شنود و یا مانیتورینگ آن بسیار ساده است بخصوص اگر فناوری بکار گرفته شده از نوع بی سیمی باشد. به همین دلیل الگوریتمها، سخت افزارها و نرم‌افزارهای مختلفی ایجاد شده که به نحوی نسبت به رمز کردن مکالمات صورت گرفته اقدام می‌کنند. از آنجا که مکالمه و ارتباط بصورت زنده صورت می‌گیرد، فناوری ساخته شده نیز بایستی قادر به رمز کردن اطلاعات، داده‌ها و صوت بصورت بلادرنگ باشد. موبایل یا تلفن همراه یکی از عمومی ترین وسایل جهت برقراری یک ارتباط دو یا چند نفره است که توسط میلیونها نفر در سراسر دنیا مورد استفاده قرار می‌گیرد.

مکانیزمی که در قسمتهای بعدی به آن اشاره خواهد شد، به راحتی قابل پیاده‌سازی در دیگر شبکه‌های سلولی نظیر CDMA نیز می‌باشد.

۴- اقدامات صورت گرفته

یکی از اقدامات صورت گرفته جهت رمزنگاری داده‌ها برای عبور از کانالهای مخابراتی، توسعه و ایجاد یک پروتکل سیگنالینگ به نام SCIP^۷ است. در واقع پروتکلی است که اجازه می‌دهد ادوات مختلف ساخته کارخانجات متفاوت، بتوانند با یکدیگر ارتباط امن نوع I^۸ برقرار کنند. بنابراین می‌توان چندین نوع دستگاه مختلف را در کانالهای مخابراتی گوناگون مورد استفاده قرارداد تا از این طریق نسبت به برقراری یک ارتباط End-to-End امن اقدام نمود [5].

کاربرانی که از ارتباط امن نوع I استفاده می‌کنند، بایستی بتوانند نسبت به ساخت یک کلید رمز^۹ یا کلید رمز عمومی خودکار^{۱۰} اقدام نمایند. در اینصورت ارتباط برقرار شده بر مبنای آن کلید خواهد بود.

۵- ملزومات

برای آنکه بتوان مکانیزمی امن جهت برقراری ارتباط داشت بایستی نکات زیر را در نظر گرفت: [1, 6, 7]

- کاربر بتواند در کنار مکالمات امن خود مکالمات عادی نیز داشته باشد.
- مکالمات امن از غیر امن براحتی قابل تشخیص باشد.
- مکانیزم ایجاد یک مکالمه امن ساده و راحت باشد.
- کیفیت مکالمه امن در حد کیفیت مکالمه عادی باشد.
- مکالمه امن بلادرنگ بوده و تاخیر چندانی نسبت به مکالمه عادی نداشته باشد.
- تجهیزات مورد نیاز (گوشی) برای کاربرانی که می‌خواهند مکالمه امن داشته باشند، براحتی قابل تهیه باشد.
- هزینه تجهیزات پایین باشد.

۶- طراحی نرم‌افزار / سخت افزار

با توجه به پیشرفت تکنولوژی و به خدمت گرفتن آن در گوشی‌های جدید، برای طراحی گوشی با قابلیت‌های انتقال مکالمه امن، گوشی مدل Qtek2020 که در واقع یک PocketPC با سیستم عامل ویندوز موبایل نسخه 4.2 بود، انتخاب گردید.

است دیگر فناوریهای مرتبط با GSM نظیر انتقال داده و سرویسهای ارزش افزوده کاملاً منطبق بر این استاندارد باشند.

این استاندارد اروپایی که توسط بیش از ۴۰۰ اپراتور در سراسر دنیا مورد استفاده قرار گرفته است در باندهای ۹۰۰، ۱۸۰۰ و ۱۹۰۰ مگاهرتزی تقسیم می‌شود و گوشیهایی که هر سه باند را پشتیبانی

می‌نمایند Tri-Band نامیده می‌شوند.

از آنجا که این استاندارد در کشور نیز مورد توجه قرار گرفته و هم اکنون تمامی اپراتورهای داخلی برای ارایه سرویس از آن استفاده می‌کنند، جهت ارایه راه حلی برای رمز کردن مکالمات این استاندارد مورد توجه قرار گرفته است.

۳- رمزنگاری در GSM

اگرچه در استاندارد GSM، رمز شدن داده‌ها و مکالمات وجود دارد، با اینحال مشکل اینجاست که رمز شدن اطلاعات تنها در هوا صورت گرفته و فقط قسمتهای هوایی لینک مخابراتی را شامل می‌شود. به عبارت دیگر داده‌ها توسط گوشی رمز شده و سپس بر روی هوا ارسال می‌گردد. [1, 2, 3]

ایستگاه پایه^۱ نیز آن را رمزگشایی کرده و اطلاعات در باقی کانالهای باقیمانده بصورت آزادانه منتشر می‌شود. این کانالها شامل قسمتی از تجهیزات شبکه موبایل نظیر BSC و MSC و همچنین شبکه سوئیچینگ تلفن عمومی^۲، سنترال آفیس^۳، PBX^۴، حلقه محلی^۵ و غیره می‌شود که فوق العاده مستعد شنود و بهره برداری غیر مجاز از داده‌هاست.

اشکال دوم در آن است که کاربر هیچگونه کنترلی بر روی داده‌های رمز شده در سیستم GSM ندارد. در ضمن سرویس دهنده^۶ نیز می‌تواند رمز شدن داده‌ها بر روی کانال هوایی را غیرفعال نماید. در بعضی از مناطق نیز جهت کنترل و نظارت، دولت مرکزی دستور توقف رمز شدن داده‌ها در لینک هوایی را می‌دهد. [1, 4]

همه اینها در واقع نشان دهنده ضعف در رمزنگاری داده‌ها در GSM می‌باشد. بنابراین بایستی مکانیزمی را اتخاذ نمود تا از این طریق بتوان داده‌ها را بصورت کاملاً مطمئن رمز نموده و سپس انتقال داد. به عبارت دیگر گیرنده نیز اطمینان داشته باشد که داده‌ها در نقطه انتهایی رمزگشایی شده و از دسترس دیگران بدور بوده است.

¹ Base Station

² Public Switched Telephone Network (PSTN)

³ Central Office

⁴ Private Branch Exchange

⁵ Local Loop

⁶ Service Provider

⁷ Secure Communication Interoperability Protocol (SCIP)

⁸ Type I

⁹ Encryption Key

¹⁰ Automatic Public Key



سیستم بطور خودکار اقدام به پرکردن بافر دوم کرده و در آن واحد نیز نسبت به رمزکردن بافر اول اقدام کرده و سپس بر روی کانال ارسال می‌کند.

لازم به ذکر است که صدا با فرمت PCM و با نرخ 8KHz و هر نمونه دو بیتی، نمونه برداری می‌شود.

۶-۲ اینکودر/دیکودر صوتی

بایستی توجه داشت که در بهترین حالت و در صورتیکه کانال دیتا بصورت Transparent مورد استفاده قرارگیرد، ماگزیمم ۹/۶ کیلوبیت برثانیه می‌توان داده‌ها را انتقال داد. با توجه به آنکه کیفیت ارتباطی عموماً بسیار پایین است، بنابراین نرخ انتقال دیتا به ۴/۸ و ۲/۴ کیلوبیت بر ثانیه نیز می‌رسد. بنابراین بایستی مکانیزمی اتخاذ نمود تا نسبت به فشرده کردن صوت ذخیره شده در بافر اقدام کرد. بنابراین با یک محاسبه سرانگشتی می‌توان داشت:

$$8,000 \times 2 \times 8 = 128,000 \text{ bit per sec} \quad (1)$$

از آنجا که حداکثر دیتای انتقالی ۹۶۰۰ بیت در ثانیه است اینکودر بایستی بتواند با ضریب حداقل ۱۳/۳ نسبت به فشرده سازی اقدام نماید.

علاوه بر نرخ فشرده سازی که جهت انتقال بلادرنگ داده‌ها بسیار حایز اهمیت است، میزان تاخیر نیز فاکتور قابل ملاحظه است. در واقع میزان زمانی که Vocoder جهت فشرده سازی هر بلوک صوتی نیاز دارد، توجه داشته باشید مدت زمانی که طول می‌کشد تا صدا از یک گوشی گرفته شده و به گوشی دیگر انتقال داده شود از رابطه زیر بدست می‌آید:

$$\text{تأخیر کل} = t_{\text{voice capturing}} + t_{\text{compress}} + t_{\text{encryption}} + t_{\text{channel}} + t_{\text{decryption}} + t_{\text{decompress}} + t_{\text{playback}} \quad (2)$$

رابطه (۲) را بصورت زیر نوشت:

$$t_{\text{Delay}} = t_{\text{channel}} + 2 \times (t_{\text{voice capturing}} + t_{\text{compress}} + t_{\text{encryption}}) \quad (3)$$

با توجه به حساس بودن گوش انسان به تاخیر، تاخیر کل بایستی مقداری کمتر از ۷۰۰ میلی ثانیه را داشته باشد. مقادیر بیشتر از ۷۰۰ میلی ثانیه در تاخیر، ایجاد ناراحتی برای شنونده خواهد کرد. از Vocoderهای موجود نظیر CELP^۵، MELP و Speex (که برگرفته از CELP می‌باشد)، پس از آزمایشات مختلف بر روی کارایی و آزمون کیفیت صوت خروجی، Vocoder نوع Speex انتخاب گردید.

از آنجا که Speex [8] مبتنی بر CELP است بنابراین از نقطه نظر نظامی و استانداردهای آن مشکل خاصی وجود ندارد. توجه

روش کار بدین صورت است که مکالمات امن از طریق لینک دیتای^۱ و مکالمات غیرامن به شیوه عادی و با استفاده از لینک صوت صورت می‌پذیرد.

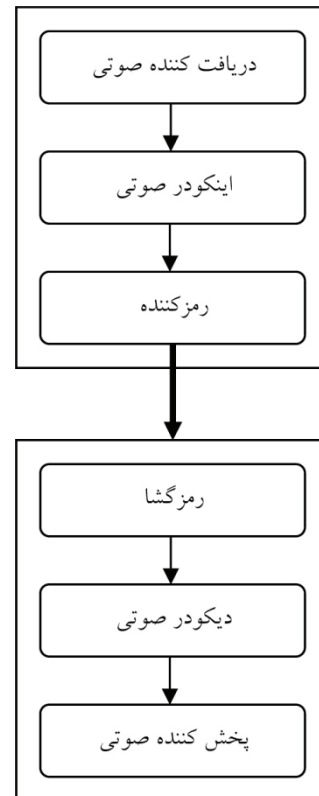
بنابراین برای پیاده‌سازی نرم‌افزاری که بتواند داده‌ها را بصورت رمز درآورد، نیاز به ماجولهای زیر است:

۱- دریافت کننده/پخش کننده صدا^۲

۲- فشرده ساز صوتی^۳

۳- رمز کننده/رمزگشا

ماجولهای مورد نیاز، در شکل ۱ دیده می‌شود.



شکل ۱: دیاگرام ماجولهای مورد نیاز

۶-۱ دریافت کننده و پخش کننده صوتی

از آنجا که سیستم عامل مورد استفاده ویندوز بود، جهت ضبط و پخش صدا از توابع Wave API ویندوز استفاده شد. برای آنکه بتوان مدیریت بهتری بر روی بافرها داشت (با توجه به محدود بودن حافظه RAM گوشی) و در نظر گرفتن آنکه به محض پرشدن یک بافر بایستی نسبت به فشرده کردن و سپس ارسال آن اقدام نمود، از یک مجموعه بافر چرخشی^۴ برای این منظور استفاده استفاده شد. بنابراین با داشتن ده بافر و به محض پرشدن یک بافر،

¹ Data Link

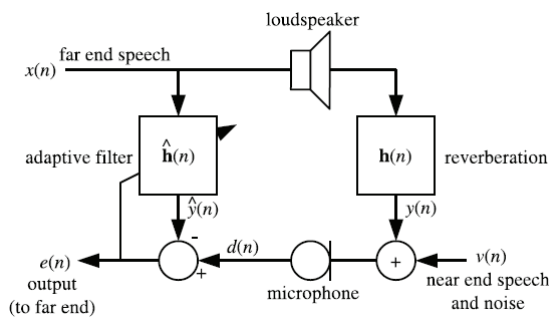
² Voice Recorder/Player

³ Voice Encoder/Decoder (Vocoder)

⁴ Circular Buffer

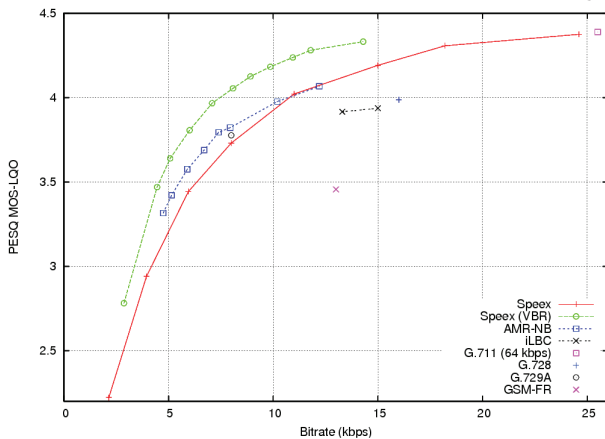
⁵ Code Exited Linear Prediction

مقداری بین ۳۹۵۰ تا ۵۹۵۰ بیت در ثانیه خواهد بود.



شکل ۲: مدل اکوی آکوستیکی

شکل ۳ و جدول ۲ مقایسه ای بین انکودرهای مختلف صوتی رایج در بازار را نشان می‌دهند. همانگونه که به وضوح دیده می‌شود برای کاربردهای صوتی (نه موسیقیایی) Speex یک گزینه بسیار خوب است.



شکل ۳: مقایسه ای بین Vocoderهای صوتی رایج [8]

جدول ۱: مقایسه کیفیت و نرخ بیت در مد باند باریک

Mode	Quality	Bit-rate (bps)	mflops
0	-	250	0
1	0	2,150	6
2	2	5,950	9
3	3-4	8,000	10
4	5-6	11,000	14
5	7-8	15,000	11
6	9	18,200	17.5
7	10	24,600	14.5
8	1	3,950	10.5

۶-۳ رمزکننده و رمزگشا

پس از آنکه دو ماجول ضبط صدا و فشرده ساز صدا کار خود را انجام دادند، نوبت به رمزکننده می‌رسد. بسیاری از برنامه‌های کاربردی که نیاز به عملیات رمز دارند، تقریباً از یک مکانیزم استفاده می‌کنند: کلید عمومی و کلید خصوصی. از این رو پس از برقراری ارتباط با استفاده از مکانیزم تبادل کلید دفی-هلمن،

داشته باشید که این Vocoder هم برای اصوات Wideband ۱۶ کیلوهرتزی و هم برای Narrowband ۸ کیلوهرتزی (یعنی کیفیت سیگنالهای تلفنی) و برای نرخ بیت‌های پایین نظیر G.728 @ 16 kbps و CELP @ 4.8 kbps و نرخ بیت‌های بالا نظیر G.728 @ 16 kbps بسیار مناسب است.

نکته دیگر آن است که Speex یک کدکننده Lossy است. این بدین معناست که فشرده سازی به قیمت حذف مقداری از اطلاعات صوتی است. کیفیت را در این انکودر می‌توان مقداری بین صفر تا ۱۰ گرفت که عدد ۱۰ نمایانگر بهترین کیفیت است. توجه داشته باشید که هر چه عدد کیفیت بزرگتر باشد، میزان فشرده سازی کمتر است.

یکی دیگر از مزایای این انکودر تشخیص حضور سیگنال صوتی یا VAD است. بنابراین در زمانهایی که سکوت وجود دارد (کاربر در حال گوش کردن مکالمات طرف مقابل است، می‌توان در پهنای باند و میزان مصرف باتری گوشی صرفه جویی کرد).

بطور خلاصه مزایای Speex به شرح زیر می‌باشند:

- کد متن باز و امکان ارایه رایگان
- ادغام باند وسیع و باند باریک صوتی با استفاده از جریان بییتی Embedded
- وجود تعداد بسیار زیادی از نرخ بیت‌های متفاوت از ۲/۱۵ تا ۴۴ کیلوبیت بر ثانیه
- تغییر نرخ بیت پویا (AMR) و عمل در نرخ بیت‌های متغیر (VBR)
- تشخیص فعالیت صوتی (VAD) به همراه VBR و امکان انتقال ناپیوسته (DTX^۲)
- پیاده‌سازی در مد Fixed Point
- و مد عملیاتی باند بسیار وسیع تا ۳۲ کیلوهرتز

یکی دیگر از مزایای این انکودر، قابلیت حذف اکو^۱ است.

شکل زیر مدل اکوی آکوستیکی را نشان می‌دهد. از طریق Speex و توابع فراهم آورده شده می‌توان نسبت به حذف اکو (که عموماً از طریق بلندگویی که مکالمات را پخش می‌کند و توسط میکروفون گرفته می‌شود) می‌توان اقدام نمود.

همانگونه که قبلاً بیان شد، یکی از مشخصه‌هایی که بایستی بدرستی انتخاب شود، کیفیت صوت خروجی است. هر چقدر کیفیت بهتر باشد، پهنای باند مورد نیاز نیز بیشتر خواهد بود. همانگونه که در جدول روبرو دیده می‌شود، برای آنکه بتوان با شرایط موجود در لینک داده GSM کار کرد، کیفیت باید مقداری بین ۱ و ۲ داشته باشد. در اینصورت پهنای باند اشغال شده

¹

² Voice Activity Detection

³ Discontinuous Transmission

⁴ Echo Cancellation



شکل ۴: نمایی از نرم افزار در حال کار

پارامترهای کلید عمومی از طریق کانال غیر امن به طرف مقابل ارسال می گردد. پس از آن تمامی پیامها با استفاده از این کلید عمومی رمز شده و هر طرف تنها با استفاده از کلید خصوصی که در دست دارد، نسبت به رمزگشایی اقدام می نماید.

برای آنکه بتوان بهترین ضریب اطمینان را از داده های رمز شده داشت، از دو شیوه رمز نگاری AES256 و Twofish برای این منظور استفاده شده است.

البته نرم افزار بگونه ای نوشته شده است که بتوان برحسب درخواست، براحتی کدهای موجود را تغییر داده و الگوریتم دیگری را بکار برد. توجه به این نکته نیز ضروری است که بایستی محدودیتهای گوشیهای PocketPC و میزان قدرت پردازش آنها را نیز در نظر گرفت. چرا که الگوریتمهای سنگین تر و کلیدهای طولی تر نیازمند قدرت پردازش و همچنین زمان تاخیر بیشتر هستند که باعث صدمه در پخش بلادرنگ مکالمه می شود.

جدول ۲: مقایسه ای بین Vocoderهای رایج در بازار [8]

Codec	Rate (KHz)	Bitrate (kbps)	Delay frame + lookahead (ms)	Multi-rate	Embedded	VBR	PLC	Bit-robust	license
Speex	8, 16, 32	2.15-24.6 (NB) 4-44.2 (WB)	20+10 (NB) 20+14 (WB)	Yes	Yes	Yes	Yes		Open source / free software
iLBC	8	15.2 or 13.3	20+5 or 30+10				Yes		No charge, but not open source
AMR-NB	8	4.75 – 12.2	20+5?	Yes			Yes	Yes	Proprietary
AMR-WB (G.722.2)	16	6.6-23.85	20+5?	Yes			Yes	Yes	Proprietary
G.729	8	8	10+5				Yes	Yes	Proprietary
GSM-FR	8	13	20+?				?	?	Patented?
GSM-EFR	8	12.2	20+?				Yes	Yes	Proprietary
G.723.1	8	5.3 6.3	37.5				Yes	?	Proprietary
G.728	8	16	0.625						Proprietary
G.722	16	48 56 64	?		Yes			?	?

۷- نتایج عملی طرح

اولین مشکلی که طرح با آن مواجه بود، عدم نصب تجهیزات دیتا در شبکه GSM کشوری بود. بنابراین امکان بهره برداری از نرم افزار در بسیاری از شهرستانهای کشور نبود. کیفیت بسیار پایین (که عمدتاً بدلیل کیفیت پایین سیگنال و مشکلات عمومی موبایل بوجود می آمد) باعث می شد که تاخیر داده ها گاهی اوقات خیلی بیشتر از مقدار ۰/۷ ثانیه شود و در نتیجه طرفین مکالمه را آزرده

۶-۴ مدیریت بافر

از آنجا که تعداد بافرها محدود است و در ضمن مکالمات به صورت پیوسته صورت می گیرد بایستی مکانیزمی در نظر گرفته شود تا بافرها همواره مورد استفاده قرار گیرند.

مکانیزم مورد استفاده در این پروژه در واقع ایجاد یک بافر چرخشی (Circular Buffer) است. بدین معنی که بافرها ابتدا در یک صف قرار می گیرند و پس از آن که مورد استفاده قرار گرفتند دوباره به انتهای صف متصل می شوند.

تابع CreateBuffer ابتدا بافرها را به صورت دینامیک ایجاد کرده و سپس آنها را در یک صف قرار می دهد.

هر بار که بافری پر شود، سیستم عامل برنامه را مطلع کرده و محتویات بافر از طریق تابع ابتدا فشرده شده و سپس از طریق لینک GSM ارسال می شود. پس از آن نیز بافر تخلیه شده و سپس به انتهای صف بافرها منتقل می شود.

۶-۵ نگاهی به نرم افزار

نرم افزار با استفاده از زبان برنامه نویسی Visual C++ 4.0 eMbedded و کیت توسعه نرم افزار (SDK¹) سیستم عامل ویندوز موبایل نسخه ۴/۲ نوشته شده است.

¹ Software Development Kit (SDK)

- [4] Sandro Grech, Pasi Eronen, "Implications of Unlicensed Mobile Access (UMA) for GSM security," Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), IEEE, 2005.
- [5] Elad Barkan, Eli Biham, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," Journal of Cryptology, Vol. 21, n 3, pp. 392-429, Springer, New York, 2008.
- [6] Daniel Guinier, "From eavesdropping to security on the cellular telephone system GSM," ACM SIGSAC Review archive, Volume 15, Issue 2, pp. 13-18, 1997.
- [7] Tero Ojanpera, Risto Mononen, "Security and Authentication in the Mobile World," Wireless Personal Communications, Volume 22, Issue 2, pp. 229-235, Kluwer, 2002.
- [8] Speex official website, <http://www.speex.org/>

خاطر می‌ساخت. کیفیت پایین به حدی بود که پهنای باند دیتا، در بیشتر مواقع بسیار کمتر از $9/6$ کیلوبیت بر ثانیه و بین $2/4$ تا $4/8$ کیلوبیت بر ثانیه می‌بود. نتیجه آنکه در عمل مجبور به بالابردن سطح فشرده سازی Speex و در نتیجه پایین آوردن کیفیت صدا می‌شدیم.

نتیجه‌گیری

با توجه به اهمیت ارتباطات در عصر حاضر و با توجه به فراگیر شدن استفاده از تلفن همراه و همچنین در نظر داشتن این نکته که در هر جایی که فرصتی فراهم می‌شود همواره تهدیدها نیز وجود دارند لذا در بحث انتقال صوت نیز این مساله مطرح است. بسترهای مخابراتی که این امکان را فراهم می‌کنند اغلب دارای دو فن آوری GSM و CDMA هستند. که GSM اگرچه رمزنگاری اطلاعات را انجام می‌دهد اما این رمزنگاری صرفاً در بخش هوایی (لینک هوایی) صورت می‌گیرد و بخش‌های مهم دیگری که مستعد شنود هستند در این فرایند لحاظ نمی‌شوند. این بخشها عبارتند از: شبکه سوئیچینگ تلفن عمومی، سنترال آفیس، PBX، حلقه محلی لذا استفاده از روشی که بتواند امنیت اطلاعات را در بخشهای دیگر نیز تضمین نماید امری مهم و ضروری است. با این رویکرد و نگاه این مقاله به پیاده‌سازی نرم‌افزاری که رمزنگاری مکالمات را با استفاده از سرویس دیتا در GSM انجام می‌دهد می‌پردازد. این نرم‌افزار روی یک گوشی PocketPC و به زبان برنامه نویسی Visual C++ 4.0 eMbedded نوشته و تست شده است.

در ادامه این تحقیق با توجه به ورود نسل $2/5$ و بالاتر به کشور و ارایه سرویسهایی نظیر GPRS، به نظر می‌رسد، شرایط برای تغییرات گسترده در نرم‌افزار و استفاده از بستر انتقال داده مبتنی بر GPRS فراهم شده باشد. با توجه به آنکه می‌توان در این تکنولوژی تا 56 کیلو بیت بر ثانیه داده‌ها را انتقال داد، شاید بتوان نتایج به مراتب بهتری از لحاظ کیفی جهت انتقال داده و صوت گرفت و همچنین بتوان کاربردهای ترکیبی از انتقال صوت و داده را نیز جامعه عمل پوشاند.

مراجع

- [1] Mohsen Toorani, Ali Asghar Beheshti Shirazi, "Solutions to the GSM Security Weaknesses," NGMAST, pp.576-581, The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, 2008.
- [2] S. Muhammad Siddique, Muhammad Amir, "GSM Security Issues and Challenges," Proceedings of the Seventh ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'06), pp. 413-418, 2006
- [3] David G. W. Birch, Ian J. Shaw, "Mobile Communications Security-Private or Public," IEE, pp. 5/1-5/6, June 1994.