ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

طرح جدید تعیین هویت امن دو طرفه کاربر بر اساس سیستم رمزنگاری مبتنی بر شناسه

سید حسین سجادی جهرمی[۱]، محمود گردشی[۲]

[۱]دانشگاه امام حسین(ع)
Sajjadi_hossein@yahoo.com
[۲]دانشگاه امام حسین (ع)- مرکز تحقیقات فتح
Mgardeshi2000@yahoo.com

چکیده

با توجه به اینکه اکثر طرح‌های تعیین هویت مبتنی بر شناسه که تا به حال مطرح شده‌اند یک طرفه بوده و فقط کاربر قادر بود هویت خود را به طرف مقابل اثبات کند و کاربر از قانونی بودن طرف مقابل اطمینان پیدا نمی‌کرد، لذا یکی از اهداف ما از ارائه این مقاله پیشنهاد یک طرح تعیین هویت امن دو طرفه مبتنی بر شناسه، به نحوی که در آن طرفین ارتباطی هویت خود را برای یکدیگر به اثبات می‌رسانند می‌باشد.

هدف دیگری که در طرح پیشنهادی آن را دنبال می‌کنیم، طراحی این طرح به گونه‌ای که در شبکه‌های بی‌سیم که در مقدار ظرفیت باتری محدودیت داریم قابل استفاده باشد، لذا در قسمت ارزیابی عملکرد از طرح پیشنهادی مقایسه‌ای به لحاظ پیچیدگی محاسبات و هزینه ارتباطات با دو طرحی که اخیرا پیشنهاد شده است مطرح خواهیم کرد و نشان می‌دهیم که طرح پیشنهادی علاوه بر دستیابی به یک طرح تعیین هویت دوطرفه به یک طرح کارامد دست پیدا کرده‌ایم به نحوی که در شبکه‌های بی‌سیم نیز قابل استفاده می‌باشد.

واژه‌های کلیدی

تعیین هویت دو طرفه، مهرزمانی، شخص مورد اعتماد، ایستگاه مبنا، وسیله سیار، حمله جعل هویت

۱- مقدمه

در سال ۱۹۸۴ شامیر[۱] ایده سیستم‌های رمزنگاری کلید عمومی مبتنی بر شناسه را مطرح کرد[1] . در این طرح، شناسه کاربر همان کلید عمومی کاربر بوده و کلید خصوصی هر کاربر توسط یک شخص مورد اعتماد[۲] (TA) با توجه به پارامترهایی که خود انتخاب کرده و شناسه کاربر، ساخته می‌شود. تاکنون طرح‌های مختلفی با استفاده از طرح ارائه شده توسط شامیر ارائه شده است[7-2].

در سال ۱۹۹۸ تسنگ[۳] و جان[۴] یک طرح تعیین هویت یک‌طرفه مبتنی بر شناسه را پیشنهاد دادند[8] . در این طرح، پس از سه بار تبادل[۵] اطلاعات بین طرفین، تعیین هویت صورت می‌گرفت. به منظور کاهش تعداد دفعات تبادل اطلاعات، وانگ و همکارانش در سال ۲۰۰۴ یک طرح بهبود یافته ارائه دادند که در آن برای اینکه ایستگاه مبنا[۶](BS) از شناسه کاربر اطمینان پیدا کند فقط نیاز به یک بار تبادل اطلاعات داشت[9]. اما در سال ۲۰۰۶ چو و همکارانش به ارئه حمله جعل هویت به طرح وانگ و همکاران پرداختند و یک طرح تعیین هویت یک‌طرفه جدید برای مرتفع ساختن آن خلل امنیتی پیشنهاد کردند[10].

ما در این مقاله به بیان یک طرح تعیین هویت دو طرفه خواهیم پرداخت که در آن وسیله سیار و ایستگاه مبنا از قانونی بودن یکدیگر اطمینان پیدا خواهند کرد.

[1] Shamir
[2] Trusted authority
[3] Tseng
[4] Jan
[5] Tree passes
[6] Base station

در بخش دوم مروری بر طرح وانگ و همکارانش را بیان می‌کنیم و در بخش سوم به بیان حمله جعل هویت به طرح وانگ و همکاران پرداخته می‌شود. در بخش چهارم نیز به طور خلاصه به بیان طرح تعیین هویت یک طرفه چو و همکاران خواهیم پرداخت و در بخش پنجم نیز به بیان طرح پیشنهادی خود پرداخته می‌شود و در بخش ششم نیز به بیان تحلیل امنیتی طرح پیشنهادی و در بخش هفتم به مقایسه ارزیابی عملکرد و در نهایت در بخش هشتم نتیجه حاصل شده از طرح پیشنهادی خود را مطرح می‌کنیم.

۲- مروری بر طرح وانگ و همکاران[9]

این طرح از سه مرحله مقداردهی اولیه، ثبت کاربر و تعیین هویت کاربر تشکیل شده است در اینجا به طور خلاصه به بیان این سه مرحله اشاره می‌کنیم.

۲-۱ مقداردهی اولیه

در این مرحله شخص مورد اعتماد (TA) می‌بایست مراحل زیر را طی کند:

- انتخاب چهار عدد اول P_j , $(1 \le j \le 4)$ به طوری‌که این اعداد بین ۶۰ تا ۷۰ رقم‌دهدهی[1] باشند، با این شرط که $\frac{p_j - 1}{2}$ فرد بوده و دو به دو نیز نسبت به هم اول باشند.
- محاسبه $N = p_1.p_2.p_3.p_4$
- انتخاب عدد صحیح $e \in Z^*_{\varphi(N)}$ و سپس محاسبه پارامتر مخفی d به طوری‌که $ed \equiv 1 \bmod \varphi(N)$، وقتی‌که $\varphi(N)$ نشان دهنده تابع فی اویلر[2] باشد.
- انتخاب عدد مخفی تصادفی t از $Z^*_{\varphi(N)}$.
- انتخاب عضو اولیه g در $GF(p_j)$.
- انتخاب تابع یک طرفه امن $h(.)$.
- محاسبه $v \equiv t^{-1} \bmod \varphi(N)$

۲-۲ ثبت کاربر

زمانی که وسیله سیار M قصد دارد به شبکه متصل شود، او می‌بایست در ابتدا کلید خصوصی خود را از TA دریافت کند. برای دریافت کلید خصوصی، وسیله سیار M می‌بایست ابتدا شناسه خود (ID_m) را برای TA ارسال کند. پس از دیافت شناسه، TA کلید خصوصی وسیله سیار (S_m) را به صورت زیر محاسبه کرده و برای او ارسال می‌کند:

$$S_m = e.t.\log_g(ID_m^2) \bmod \varphi(N) \qquad (۱)$$

حال TA، پارامترهای $\{N, g, e, h(.)\}$ را به صورت عمومی انتشار[3] داده و $\{p_1, p_2, p_3, p_4, t, v, d\}$ را به صورت مخفی برای تمامی کاربران نزد خود نگه می‌دارد.

۲-۳ تعیین هویت کاربر

فرض کنید وسیله سیار M قصد دارد هویت خود را به ایستگاه مبنا ثابت کند.

مراحلی را که وسیله سیار می‌بایست طی کند به شرح زیر است:

- وسیله سیار M عدد صحیح و تصادفی $k \in_R Z^*_N$ را انتخاب کرده و Y و Z را به صورت زیر محاسبه و $L = ((ID_m \| Y \| Z), T)$ را برای BS ارسال می‌کند:

$$Y = (ID_m^2)^k \bmod N \qquad (۲)$$

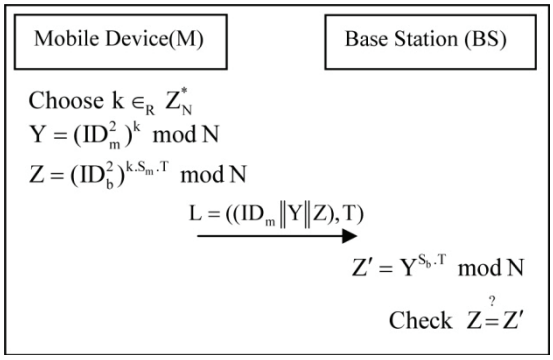
$$Z = (ID_b^2)^{k.S_m.T} \bmod N \qquad (۳)$$

در اینجا T بیان کننده مهر زمانی[4] می‌باشد.

- پس از دریافت پیام L، BS نیز Z' را به صورت زیر محاسبه و صحت رابطه $Z \stackrel{?}{=} Z'$ را مورد بازبینی قرار می‌دهد:

$$Z' = Y^{S_b.T} \bmod N \qquad (۴)$$

در رابطه فوق نیز S_b معرف کلید خصوصی BS می‌باشد. حال اگر در بازبینی رابطه $Z \stackrel{?}{=} Z'$ به موفقیت رسید، ایستگاه مبنا هویت وسیله سیار M را تایید و در غیر این‌صورت آن را انکار می‌کند. مرحله تعیین هویت طرح وانگ و همکاران در شکل(۱) نشان داده شده است[10].



شکل ۱: مرحله تعیین هویت طرح وانگ و همکاران

۳- حمله جعل هویت به طرح وانگ و همکاران[10]

این حمله در سال ۲۰۰۶ توسط چو و همکاران به طرح وانگ و همکاران مطرح شده است. فرض کنید شخص بداندیش[5] (کاربر H) قصد جعل کردن هویت یک کاربر قانونی[6] (وسیله سیار M) را داشته باشد، می‌توان به راحتی نشان داد که چگونه از طریق

[1] Decimal digits
[2] Euler,s totient function
[3] Publishes
[4] Time stamp
[5] Malicious user
[6] Legal user

حمله جعل هویت، کاربر H می‌تواند به صورت زیر به موفقیت برسد:

- کاربر H پیام مخابره شده $L=((ID_m \| Y \| Z),T)$ را قطع کرده و یک مهرزمانی دیگر به نام T' را انتخاب می‌کند.
- کاربر H در پیام قطع شده، Y' را با Y و Z' را با Z که به صورت زیر تعریف می‌شوند جا به جا می‌کند:

$$Y' = (Y^{s_h.T}) \bmod N \quad (۵)$$

$$Z' = (Z^{s_h.T'}) \bmod N \quad (۶)$$

در اینجا S_h بیانگر کلید خصوصی شخص بداندیش H می‌باشد.

- کاربر H پیام جعل شده $L'=((ID_m \| Y' \| Z'),T')$ را به BS ارسال می‌کند.
- پس از دریافت پیام L' از طرف کاربر H، BS رابطه(۷) را می‌بایست محاسبه کند.

$$Z'' = (Y')^{s_b.T'} \bmod N \quad (۷)$$

- حال BS بررسی می‌کند که آیا رابطه $Z' \stackrel{?}{=} Z''$ برقرار است یا خیر، اگر رابطه برقرار باشد، BS اطمینان پیدا می‌کند که H یک کاربر مجاز است.

مطابق با پروتکل پیشنهادی وانگ و همکاران، دشمن به راحتی به عنوان یک کاربر مجاز، بدون آشکار شدن توسط BS به موفقیت می‌رسد. معادله بازبینی $Z' = Z''$ به صورت زیر اثبات می‌شود:

$$\begin{cases} Z' = Z^{S_h.T'} \bmod N = [(ID_b^2)^{k.S_m.T}]^{S_h.T'} \bmod N \\ Z'' = (Y')^{S_b.T'} \bmod N = (Y^{S_h.T})^{S_j.T'} \bmod N \Rightarrow \end{cases} \quad (۸)$$

$$Z'' = \{[(ID_m^2)^k]^{S_h.T}\}^{S_b.T'} \bmod N \quad (۹)$$

و از طرفی داریم:

$$S_m = et.\log_g (ID_m^2) \bmod \varphi(N) \Rightarrow ID_m^2 = g^{S_m.v.d} \quad (۱۰)$$

بنابراین می‌توان از معادلات (۱۰و۹) نتیجه گرفت که:

$$\begin{aligned} Z'' &= (g^{S_m.v.d})^{k.S_h.T.S_b.T'} \bmod N \\ &= [(ID_b^2)^{k.S_m.T}]^{S_b.T'} \bmod N = Z' \end{aligned} \quad (۱۱)$$

بنابراین اهمیتی ندارد مقدار T چقدر باشد، دشمن همیشه می‌تواند در حمله جعل هویت به موفقیت برسد.

۴- مروری بر طرح چو و همکاران[10]

بزرگترین مشکل طرح وانگ و همکارنش این بود که مهر زمانی بدون هیچ گونه محافظتی مخابره می‌گردید؛ بنابراین دشمن به راحتی می‌توانست اقدام به حمله کند. برای حفاظت در برابر این حمله، چو و همکارانش برای برطرف کردن این مشکل مهر زمانی T را با مقدار a (مانده درجه دوم) برای بهبود آن جابه‌جا کردند، که این مقدار از کلید ارتباط مخفی[1] c نتیجه شده و مقدار c بین وسیله سیار M و BS به اشتراک گذاشته[2] شده است. در واقع، این طرح به جز در مقدار c به طرح وانگ و همکارن شباهت زیادی دارد و از سه مرحله مقداردهی اولیه، ثبت کاربر و تعیین هویت کاربر تشکیل شده است. مرحله مقداردهی اولیه و ثبت کاربر مشابه طرح وانگ و همکارانش می‌باشد البته با کمی تغییرات که در ادامه به طور مفصل شرح داده خواهد شد.

زمانی که وسیله سیار M به شبکه متصل می‌شود، TA می‌بایست دو عدد اول بزرگ p و q را طوری انتخاب کند (به غیر از پارامترهایی که TA در مرحله مقدار دهی اولیه انتخاب کرده بود) که به ترتیب در $4|(p+1)$ و $4|(q+1)$ صدق کند. سپس $n=p.q$ را محاسبه می‌کند. فرض کنید نماد QR_n نشان دهندهٔ مجموعه مانده‌های درجه دوم[3] درفاصله $[1,n-1]$ باشد. همچنین TA تمام QR_p و QR_q را محاسبه می‌کند. در نهایت TA، پارامترهای (n,p,q,QR_p,QR_q) را به M از طریق یک روش امن ارسال می‌کند.

هر زمانی که وسیله سیار M بخواهد هویت خودش (ID_m) را به BS ثابت کند، او می‌بایست کلید ارتباط مخفی متمایز $c \in (QR_p \cap QR_q)$ را انتخاب کرده و سپس a را از طریق معادله(۱۲) محاسبه کند:

$$a = c^2 \bmod n \quad (۱۲)$$

ارتباط بین c و a یک ارتباط یک به یک می‌باشد [11]، یعنی اینکه وسیله سیار M فقط زمانی می‌تواند c را تعیین کند که مقدار ثابت a داده شده باشد.

۴-۱ تعیین هویت کاربر

مراحل طی شده در این قسمت می‌بایست به صورت زیر انجام پذیرد:

- وسیله سیار M عدد تصادفی $k \in_R Z_N^*$ را انتخاب کرده و Y و Z را به صورت زیر محاسبه و در نهایت مقادیر $L=\{(ID_m \| Y \| Z),a\}$ را برای BS ارسال می‌کند:

$$Y = (ID_m^2)^k \bmod N \quad (۱۳)$$

$$Z = (ID^2{}_b)^{k..S_m.c} \bmod N \quad (۱۴)$$

- به مجرد دریافت پیام L از طرف وسیله سیار M، BS مقدار c را از a محاسبه کرده و Z' را از طریق معادله (۱۵) بدست می‌آورد.

$$Z' = Y^{s_b.c} \bmod N \quad (۱۵)$$

در نهایت بررسی می‌کند که آیا رابطه $Z \stackrel{?}{=} Z'$ برقرار است یا خیر. اگر برقرار بود هویت وسیله سیار M را تایید و در غیر این صورت آن را انکار می‌کند.

معادله بازبینی $Z \stackrel{?}{=} Z'$ به صورت زیر قابل اثبات است:

$$\begin{aligned} Z' &= Y^{s_b.c} \bmod N = (ID_m^2)^{k.S_b.c} \bmod N \\ &= (g^{S_m.v.d})^{k.S_b.c} \bmod N = (ID_b^2)^{k.S_m.c} \bmod N = Z \end{aligned} \quad (۱۶)$$

[1] Secret communication key

[2] Shared

[3] Quadratic residue numbers

۵- طرح پیشنهادی

هدف از پیشنهاد این طرح ارائه یک طرح تعیین هویت دو طرفه مبتنی بر شناسه می‌باشد که در آن وسیله سیار M و BS قادر به بازبینی هویت یکدیگر باشند. این طرح نیز مشابه دو طرحی که اخیرا بیان شد، از سه مرحله مقدار دهی اولیه، ثبت کاربر و تعیین هویت کاربر تشکیل شده است. مرحله مقداردهی اولیه و ثبت کاربر مشابه طرح وانگ و همکاران می‌باشد. بنابراین در این مقاله ما فقط به بیان مرحله تعیین هویت کاربر اکتفا می‌کنیم.

۵-۱ تعیین هویت کاربر

برای انجام این مرحله طرفین ارتباطی می‌بایست گام‌های زیر را طی کنند:

- وسیله سیار M، عدد صحیح و تصادفی $k \in_R Z_N^*$ را انتخاب و Y، Z و W_1 را به صورت زیر محاسبه کرده و پیام $L_1 = (ID_m \| Y \| W_1), T)$ را به BS ارسال می‌کند(T بیان کننده مهر زمانی فعلی است).

$$Y = (ID_m^2)^k \bmod N \quad (۱۷)$$

$$Z = (ID_b^2)^{k.S_m.T} \bmod N \quad (۱۸)$$

$$W_1 = h(Z \| Y \| T) \quad (۱۹)$$

- به مجرد دریافت پیام L_1 ، BS نیز Z' و W_1' را به صورت زیر محاسبه می‌کند:

$$Z' = Y^{S_b.T} \bmod N \quad (۲۰)$$

$$W_1' = h(Z' \| Y \| T) \quad (۲۱)$$

حال BS صحت رابطه $W_1 \stackrel{?}{=} W_1'$ را مورد بازبینی قرار می‌دهد، اگر صحیح بود هویت وسیله سیار M را تایید و در غیر این صورت آن را انکار کرده و پروتکل را نیمه کاره رها می‌کند.

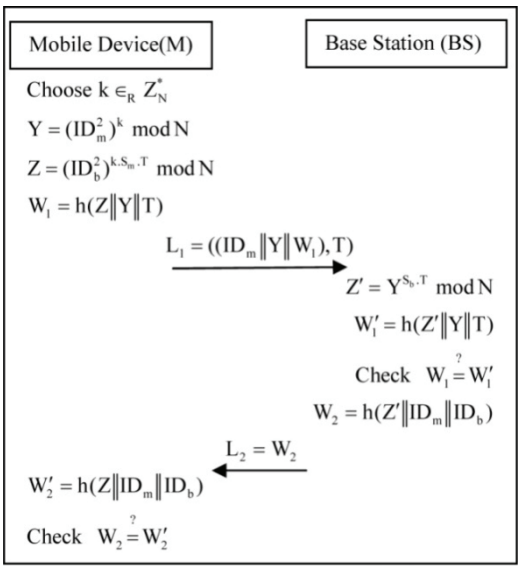
- اگر BS در بازبینی به موفقیت رسید، W_2 را از طریق معادله (۲۲) محاسبه کرده و آن را برای وسیله سیار M ارسال می‌کند.

$$W_2 = h(Z' \| ID_m \| ID_b) \quad (۲۲)$$

- به مجرد دریافت W_2 ، وسیله سیار M نیز W_2' را به صورت زیر محاسبه می‌کند:

$$W_2' = h(Z \| ID_m \| ID_b) \quad (۲۳)$$

- حال وسیله سیار M نیز صحت رابطه $W_2 \stackrel{?}{=} W_2'$ مورد بازبینی قرار می‌دهد، اگر صحیح بود وسیله سیارM اطمینان پیدا می‌کند که BS معتبر است و در غیر این‌صورت آن را انکار می‌کند. مرحله تعیین هویت این طرح در شکل(۲) به تصویر کشیده شده است.



شکل۲: مرحله تعیین هویت طرح پیشنهادی

۶- تحلیل امنیتی

در این قسمت نشان خواهیم داد که در طرح پیشنهادی ضمن اینکه به یک تصدیق دوطرفه دست پیدا کرده ایم در برابر حملات مجدد، جعل هویت و بدست آوردن کلید خصوصی امن است.

از آنجایی که در طرح پیشنهادی به صورت آشکار از مهر زمانی استفاده کرده ایم طرح پیشنهادی در برابر حمله مجدد امن خواهد بود.

دشمن در بدست آوردن عامل های N ناکام می‌ماند چرا که با توجه به بزرگ بودن عدد مرکب N دستیابی به عامل های اول آن کاری دشوار است.

دشمن در بدست آوردن کلید خصوصی S_m با توجه به پارامترهای مخفی t و $\varphi(N)$ با مشکل مواجه است.

اگر دشمن بخواهد با استراق سمع کردن از پیام اطلاعاتی L_1 به مقدار صحیح Z دست پیدا کند تا بتواند خود را به جای ایستگاه مبنا جا بزند با مشکل مواجه است، چرا که با توجه به امن بودن تابع درهم‌ساز به کار گرفته شده، بدست آوردن مقدار صحیح Z کاری بس دشوار است.

مهاجم در جعل وسیله سیار M که همان حمله ارائه شده به طرح وانگ و همکاران می‌باشد ناکام خواهد ماند. برای بهتر روشن شدن این مطلب فرض کنید مهاجم قصد دارد پیام $L_1' = ((ID_m \| Y' \| W_1'), T')$ را به $L_1 = ((ID_m \| Y \| W_1), T)$ تغییر دهد، وقتی‌که T' بیانگر مهر زمانی فعلی مهاجم باشد. اما تغییر ایجاد شده با شکست مواجه می‌شود ، چرا که مهاجم روشی برای بدست آوردن مقدار صحیح $Z = (ID_b^2)^{k.S_m.T} \bmod N$ ندارد تا بتواند به صورت دقیق پارامتر W_1 را محاسبه کند. از این گذشته بدست آوردن Z از روی W_1 نیز با توجه به امنیت تابع درهم‌ساز کاری دشوار است.

۷- ارزیابی عملکرد

در این قسمت به بیان مقایسه‌ای بین طرح وانگ و همکاران، چو و همکاران و طرح پیشنهادی بر حسب پیچیدگی محاسبات و هزینه ارتباطات را مطرح می‌کنیم.

نمادهای زیر برای سادگی، در بیان ارزیابی عملکرد به کار گرفته شده اند.

T_h : زمان لازم برای اجرای تابع درهم‌ساز h

T_{mul} : زمان لازم برای اجرای محاسبه ضرب پیمانه ای

T_{exp} : زمان لازم برای اجرای توان رسانی در پیمانه

$|x|$: طول بیت x

باید توجه داشت که پیچیدگی زمانی برای انجام توان رسانی پیمانه‌ای و ضرب پیمانه‌ای به ترتیب برابر با $o(\log^3(N))$ و $o(\log^2(N))$ می‌باشد.

مقایسه این سه طرح در جدول (۱) نشان داده شده است.

جدول۱: مقایسه ارزیابی عملکرد طرح پیشنهادی با طرح های پیشین

نام طرح	هزینه ارتباطات بر حسب بیت	پیچیدگی محاسباتی		گردش های اطلاعاتی	تصدیق دو طرفه
		وسیله سیار m	ایستگاه مبنا(BS)		
وانگ و همکاران	$2\|N\|+\|ID\|+\|T\|$	$4T_{exp}$	$2T_{exp}$	۱	☒
چو و همکاران	$3\|N\|+\|ID\|$	$5T_{exp}$	$6T_{exp}$	۱	☒
طرح پیشنهادی	$\|N\|+2\|H\|+\|T\|+\|ID\|$	$6T_{exp}+T_h$	$2T_h+T_{exp}$	۲	☑

ذکر این نکته در جدول(۱) الزامی است که اندازه تابع درهم‌ساز معمولا کوچک بوده و تاثیر چندانی در هزینه ارتباطات ندارد و از طرف دیگر، طول بیت N نسبت به دیگر پارامترها بزرگتر می‌باشد، بنابراین ما در طرح پیشنهادی با کاستن $|N|$ به یک بار توانسته‌ایم به یک طرح کارامد دست پیدا کنیم.

و از طرف دیگر به لحاظ پیچیدگی محاسباتی نیز طرح پیشنهادی یک طرح بهبود یافته می‌باشد، چرا که با توجه به پیچیدگی محاسباتی که تعریف کردیم بیشترین پیچیدگی مربوط به زمان محاسبه عمل توان‌رسانی می‌باشد، که ما در طرح پیشنهادی توانسته ایم آن را تا حد ممکن تقلیل دهیم، در حالی که ما توانسته ایم به یک طرح تعیین هویت دو طرفه دست پیدا کنیم.

۸- نتیجه گیری

در این مقاله ما به بیان یک طرح تعیین هویت دو طرفه که در آن وسیله سیار و ایستگاه مبنا هر دو از قانونی بودن یکدیگر اطمینان پیدا می‌کنند دست پیدا کرده‌ایم، این در حالی است که در طرح‌های تعیین هویت یک طرفه مبتنی بر شناسه که تا به حال مطرح شده‌اند تنها وسیله سیار می‌توانست خود را به ایستگاه مبنا اثبات کند.

از این گذشته همانطور که در بخش ارزیابی عملکرد طرح پیشنهادی دیده می‌شود ما توانسته‌ایم به یک طرح کارامد دست پیدا کنیم به نحوی که در محیط های بی‌سیم که در مقدار ظرفیت باتری محدودیت داریم قابل استفاده باشد.

۹- سپاسگذاری

با تشکر از مرکز تحقیقات مخابرات ایران که این مقاله را مورد حمایت مالی و معنوی خود قرار دادند کمال تشکر و قدردانی دارم.

مراجع

[1] A. Shamir, "Identity Based Cryptosystem & Signature Scheme," Advances in Cryptology CRYPTO'84. Lecture Note-Computer Science, pp.47-53, 1984.

[2] H. Tanaka, "A Realization Scheme for the Identity-Based Cryptosystem," proc Crypto'87, pp.340-349, 1987.

[3] Y.W. Tsai, T. Hwang, "ID based public key cryptosystems based on Okamoto and Tanaka's ID based one way communication scheme," Electronic Letters, vol. 26, No. 10, pp. 666-668, 1987.

[4] S. Tsujii, T. Itoh, and K. Kurosawa, "ID-based cryptosystem using discrete logarithm problem," Electron Letters, vol. 23, pp. 1318-1320, 1987.

[5] C.G. Gunther, "An identity-based key-exchange protocol," Cryptology-Eurocrypt'86.New York: Springer, pp. 29-37, 1987.

[6] E. Okamoto, k. Tanaka, "Identity-based information security management system for personal computer networks," IEEE J Sel Area Commun, vol. 7, No. 2, pp. 290-294, Feb 1989.

[7] W.B. Lee, K.C. Liao, "Constructing identity-based cryptosystems for discrete logarithm based cryptosystems, " Journal of Network and Computer Applications, vol. 27, No. 4, pp. 191-194, 2004.

[8] Y.M. Tseng, J.K. "Jan, ID-based Cryptographic Schemes Using a Non-interactive Public-key Distribution System," Proceeding of the 14th Annual Computer Security Applications Conference,Phoenix, Arizona, pp.237-243, 1998.

[9] M.S. Hwang, J.W. Lo, and S.C. Lin, "An Efficient User Identification Scheme Based on ID-based Cryptosystem, " Computer Standard and InterIFPes, vol. 26, No. 6, pp. 565-569, 2004.

[10] J.S. Chou, Y. Chen, and C.H. Lin, "An improvement of an efficient user identification scheme based on ID-based cryptosystem," Proc of the IEEE International Conference on Sensor Networks, vol. 1, No. 5, pp.558-561, 2006.

[11] J.S. Chou, C.H. Lin, and T.Y. Lee, "A Novel Hierarchical Key Management Scheme Based on Quadratic Residues," ISPA2004, LNCS 3358, pp. 858-865, 2004.