DOI: https://www.doi.org/10.36719/2663-4619/77/309-316

Qismət Mehman oğlu Əliyev
Azərbaycan Dövlət Neft və Sənaye Universiteti
Magistrant
aliyev.gismet@gmail.com

KLASTER ƏSASLI SİMSİZ SENSOR ŞƏBƏKƏLƏRİ ÜÇÜN SƏMƏRƏLİ VƏ TƏHLÜKƏSİZ MƏLUMAT ÖTÜRÜLMƏSİ

Xülasə

Təhlükəsiz və səmərəli məlumat ötürülməsi klaster əsaslı simsiz sensor şəbəkələri (Wireless Sensor Networks-WSN) üçün əhəmiyyətlidir. Klaster əsaslı simsiz sensor şəbəkələrdə istifadəçilərin identifikasiyası çox mühüm məsələdir. Məlumatları göndərilən istifadəçinin və təyinat (məlumatları alan) istifadəçisinin identifikasiyası ilə klaster əsaslı simsiz sensor şəbəkələr üzərindən məlumatların təhlükəsizliyinə və səmərəliliyinə nail olmaq mümkündür. Məlumatların təhlükəsizliyini və istifadəçinin identifikasiyasını təmin etmək üçün bir metod daxilində bu əməliyyatları yerinə yetirən iki konsepsiya təklif edilir. Birincisi, təsdiqləyici tərəfindən yaradılan istifadəçinin yoxlanılması üçün şəxsiyyət əsaslı imzadır (Identity Base Signature - IBS). İkincisi isə məlumatla idarə olunan və şifrəni əldə edən və orijinal informasiyanın şifrələnməsi və deşifrə edilməsi üçün ikili səviyyəli bir açardır. Binar səviyyəli metod informasiyanı ikili formaya çevirir və sonra məlumatları bloklara bölür və ikili rəqəmlərin uzunluğundan asılı olan identifikasiya işarəsi (Identification Mark - IM) metoduna əsaslanaraq ona qiymətlər təyin edir. Sonra bu qiymətlər iki səviyyəyə bölünür, 1-ci. səviyyə 2 bit və 2-ci səviyyə isə 4 bitdir. Sonra qəbuledici istifadəçidə şifrəli mətni tərs metoddan (yəni deşifrələmə üçün istifadə edilən metod) istifadə etməklə deşifrə olunacaq və təyinat istifadəçisi orijinal informasiyanı alacaq. Bu metodları istifadə etməklə biz səmərəliliyi və təhlükəsizlik xərclərini optimallaşdırmaq mümkündür.

Açar sözlər: *şəxsiyyətə əsaslanan imza, açıq açarın yaradılması, istifadəçinin identifikasiyası, informasiyanın şifrələnməsi, şifrənin açılması*

Gismat Mehman Aliyev

Secure and effective data transfer for cluster-based wireless sensor networks

Abstract

Secure and efficient data transmission is important for cluster-based wireless sensor networks (WSN). In cluster-based wireless sensor networks, user identification is a very important issue. With the identification of the user to whom the data is sent and the user of the destination (data recipient), it is possible to achieve data security and efficiency over cluster-based wireless sensor networks. To ensure data security and user identification, two concepts are proposed that perform these operations within a single method. The first is the Identity Base Signature (IBS) to verify the user created by the authenticator. The second is a dual-level key that manages and decrypts the information and encrypts and decrypts the original information. The binary level method converts information into binary form and then divides the data into blocks and assigns values to it based on the Identification Mark (IM) method, which depends on the length of the binary digits. Then these prices are divided into two levels, 1st. level is 2 bits and level 2 is 4 bits. The receiving user will then decrypt the encrypted text using the reverse method (ie the method used for decryption) and the destination user will receive the original information. By using these methods, we are able to optimize efficiency and security costs.

Key words: *decryption, signature based on identity, user identification, encryption of information, creation of public key*

Giriş

Simsiz sensor şəbəkəsi fiziki və ya ətraf mühitin vəziyyətini izləmək və qeyd etmək üçün radio dalğadan istifadə edən, həmçinin hərbi məqsədlər, ətraf mühitin monitorinqi, fəlakətlərin idarə edilməsi və s. üçün istifadə edilir. Hər bir qovşaq məlumatı emal etmək və məlumatları simsiz sensor şəbəkələrində bir və ya bir neçə toplama nöqtəsinə göndərmək qabiliyyətinə malikdir. Məlumatların təhlükəsiz ötürülməsi simsiz sensor şəbəkələr üçün mühüm məsələlərdən biridir. Eyni zamanda, bir çox simsiz sensor şəbəkələr müəyyən tətbiqlər rəqib fiziki mühitlərdə yerləşdirilir. Məsələn, hərbi sahələr. Təhlükəsiz məlumat ötürülməsi xüsusilə zəruridir və bir çox praktik simsiz sensor şəbəkələrdə tələb olunur.

Sensor texnologiyası, gücü zəif olan elektronika və radio tezliyin (Radio Frequency - RF) dizaynı simsiz şəbəkə vasitəsilə qoşula bilən mikrosensorlar adlanan kiçik, nisbətən ucuz və gücü zəif olan sensorların inkişafına imkan verdi. Bu simsiz mikrosensor şəbəkələri ətraf mühitdən məlumatların çıxarılması və nəzarət, maşın nasazlığının diaqnostikası və kimyəvi/bioloji aşkarlama daxil olmaqla bir sıra tətbiqlər müxtəlif mühitlərin etibarlı monitorinqini təmin etmək üçün yeni paradiqmanı təmsil edir. Bu şəbəkələrin dizaynında mühüm problem ondan ibarətdir ki, iki əsas resurs-rabitə, genişlik və enerji – birləşdirilmiş şəbəkə mühitində əhəmiyyətli dərəcədə məhduddur. Bu məhdudiyyətlər mövcud genişlikdən və enerjidən səmərəli istifadə etmək üçün innovativ dizayn üsullarını tələb edir. Simsiz mikro sensor şəbəkələrində optimal protokollar tərtib etmək üçün sensor tətbiqlərinə müvafiq olan parametrləri başa düşmək vacibdir. Sensor şəbəkə protokolunun xüsusiyyətlərini qiymətləndirməyin bir çox yolu olsa da, əsasən aşağıdakı ölçülərdən istifadə edilir.

Yerləşdirmə asanlığı. Sensor şəbəkələri yüzlərlə və ya minlərlə qovşaqdan ibarət ola bilər və onların uzaq və ya təhlükəli mühitlərdə yerləşdirilməsinə ehtiyac ola bilər ki, bu da istifadəçilərə başqa cür mümkün olmayan üsullarla məlumat çatdırmağa imkan verir. Bu, qurulmuş şəbəkə infrastrukturu və əvvəlcədən təyin edilmiş qovşaq yerləri olmadıqda belə qovşaqların bir-biri ilə əlaqə qura bilməsini tələb edir.

Sistem ömrü. Bu şəbəkələr mümkün qədər uzun müddət fəaliyyət göstərməlidir. Düyün batareyalarını doldurmaq əlverişsiz və ya qeyri-mümkün ola bilər. Buna görə də, qovşağın bütün aspektləri, avadanlıqdan protokollara qədər, son dərəcə enerjiyə qənaət etmək üçün dizayn edilməlidir.

Ləngimə. Sensor şəbəkələrindən alınan məlumatlar adətən zamana həssasdır, ona görə də məlumatların vaxtında qəbul edilməsi vacibdir.

Keyfiyyət. Mikrosensor şəbəkəsində "keyfiyyət" anlayışı ənənəvi simsiz məlumat şəbəkələrindən çox fərqlidir. Sensor şəbəkələri üçün son istifadəçi şəbəkədəki bütün məlumatları tələb etmir, çünki 1) qonşu qovşaqlardan gələn məlumatlar yüksək korrelyasiyaya malikdir; 2) son istifadəçi monitorinq edilən mühitdə baş verən hadisələrin daha yüksək səviyyəli təsvirinə əhəmiyyət verir. Beləliklə, şəbəkənin keyfiyyəti məlumatların keyfiyyətinə əsaslanır, ona görə də protokollar sensor şəbəkəsinin unikal və tətbiqi xüsusiyyətini optimallaşdırmaq üçün tərtib edilməlidir. Bu yazı simsiz mikrosensor şəbəkələri üçün proqrama xas protokol arxitekturası olan aşağı enerjili adaptiv klasterləşmə iyerarxiyasının ətraflı təsviri və təhlili ilə təsvir edilən iş üzərində qurulur. Qeyd olunan dizayn məqsədlərinə nail olmaq üçün aşağıdakı üsullardan istifadə edir: 1) təsadüfi, adaptiv, özünü konfiqurasiya edən klaster formalaşması; 2) məlumat ötürülməsi üçün lokallaşdırılmış nəzarət; 3) aşağı enerjili informasiya girişinə nəzarət (Media Access Control - MAC); və 4) verilənlərin yığılması və ya sıxılması kimi tətbiqlərə xas məlumatların işlənməsi.

1. Simsiz sensor şəbəkələrində informasiya ötürülməsi üçün istifadə edilən üsullar

Mövcud üsul. Simsiz sensor şəbəkəsində məlumatların təhlükəsizliyini və səmərəliliyini təmin etmək əhəmiyyətli məsələdir. Simsiz sensor şəbəkələr üçün məlumat ötürmə protokolları bir sıra hücumlarına qarşı həssasdır. Xüsusilə, klasterli simsiz sensor şəbəkələrdə istifadəçilərə edilən hücumlar şəbəkəyə ciddi ziyan vura bilər, çünki məlumatların ötürülməsi və məlumatların toplanması əsas olaraq istifadəçilərdən asılıdır. Şəbəkəyə hücum edən şəxs özünü istifadəçi kimi göstərməyi bacararsa, o, müxtəlif növ hücumlara səbəb ola bilər, beləliklə də şəbəkənin işini poza bilər. Digər tərəfdən, şəbəkəyə

hücum edən şəxs simsiz sensor şəbəkəyə yanlış məlumat daxil etmək niyyətində ola bilər. Bu problemləri aradan qaldırmaq üçün təklif olunan sistem dizaynını tətbiq etmək olar.

Təklif edilən üsul. Simsiz sensor şəbəkəsində məlumatların səmərəli ötürülməsi simsiz sensor şəbəkələr üçün ən vacib məsələlərdən biridir. Burada imzalamanın 4 fərqli bloku mövcuddur, bunlar $01, 00, 10, 11$ kimidir. Açar yaratma texnikasına uyğun olaraq $01 = a, 00 = b, 10 = c, 11 = d$ təyin edilir ki, bu da 1-ci səviyyəli identifikasiya işarələridir. 2-ci səviyyəli identifikasiya işarələrinin yaradılması üçün a, b, c və d −nin iki bit təsviri $aa, ab, ac, ad, bb, bc, bd, cc, cd, dd, ba, ca, da, cb, db, dc$-dir. Bu iki bit təsvirləri müxtəlif dəyərlər ilə ifadə etdikdə alınır: $aa = e, ab = f, ac = g, ad = h, bb = i, bc = j, bd = k, cc = l, cd = m, dd = n, ba = o, ca = p, da = q, cb = r, db = s, dc = t$. Hər bir blok üçün identifikasiya nişanlarının yaranma səviyyəsi və bölünmüş blokun uzunluğu hesblama zamanı təsadüfi olaraq seçilir, çünki onun açarı hər bir şifrələmədən digərindən fərqlənir. Nəinki hər bir blok üçün identifikasiya işarələrini yaratmaq üçün görünən ardıcıllıqla parçalanmış blokları götürürük. b −dəki imza cütdür (X, y). İnformasiya verildikdə, təsdiqləyiciyə imza (X, y) göndərilir. Təsdiqləyici V y(y + a) və $L(b\ X)$ hesablayır və onların bərabər olduğunu yoxlayır. Sonra paketi götürür və həm v, həm də b bərabərdirsə onlar identifikasiya olunmuş istifadəçidir.

İstifadəçilərin identifikasiyası

Bu modul istifadəçinin identifikasiyasını etibarlı mərkəzdə həyata keçirmək üçün istifadə olunur. Etibarlı mərkəz istifadəçilərdən imzanı alır və hər bir istifadəçi imzasını müqayisə edir. Hər iki imza bərabərdirsə, onlar təsdiqlənmiş istifadəçidirlər. İmza bərabər deyilsə, onlar identifikasiya edilmiş istifadəçilər deyillər. Doğrulama prosesi aşağıdakı kimidir. b mesajını imzalamaq üçün S imzalayan təsadüfi X seçir və $L(b\ X)$ hesablanılır. Sonra imzalayan $y(y + a) = L\ (b\ X)\ \%\ n$ nəticəsini hesablayır. Həll yoxdursa, imzalayan yeni X təsadüfi seçimini edir və yenidən cəhd edir. Əgər L həqiqətən təsadüfidirsə, gözlənilən cəhdlərin sayı 4-ə bərabərdir. (X, y) b −dəki imza cütdür. İnformasiya verildikdə, təsdiqləyiciyə imza (X, y) göndərilir. Təsdiqləyici $V\ y(y + a)\ və\ L(b\ X)$ hesablayır və onların bərabər olduğunu yoxlayır. Sonra paketi yoxlayır. Əgər həm v, həm də b bərabərdirsə onlar identifikasiya olunmuş istifadəçidir.

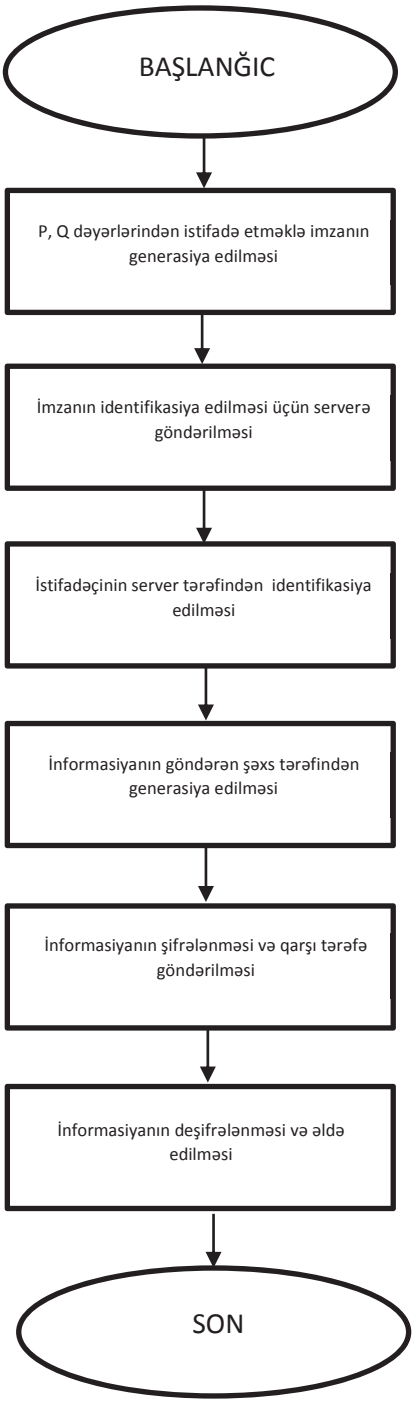
Şifrələmə

İstifadəçi tərəfindən göndərilən informasiya əməliyyatdan sonra bərabər uzunluğa malik bloklara bölünür. Sonra hər bir fərqli bloku götürülür və bütün fərqli bloklar görünüş ardıcıllığına görə şəxsi açarda saxlanılır. Əməliyyatdan sonra məzmun ikili formaya çevrilir, bu bit axınından fərqli deyil, eyni uzunluqda N sayda bloka parçalanır; Burada L tam ədəddir. Ola bilər ki, bitin ümumi axını bəzi L −bit bloklarına parçalandıqdan sonra, L bitdən az bloklar qalır. Şifrələmə zamanı ML dəyişməz saxlanılır ($ML < L$ uzunluğu deməkdir). Beləliklə, burada N $2L$ −dən az və ya bərabər olmalıdır ($N \leq 2L$). Şifrələmə üçün hər bir fərqli blok üçün identifikasiya işarələri kodu yaradılmalıdır. Hər bir bölünmüş blok yaradılmış müvafiq identifikasiya işarələri ilə göndərilir. Ardıcıl iki identifikasiya nişanını nəzərdən keçirilir. 2-ci səviyyəli regenerasiya prosesində yaranan identifikasiya nişanları ilə əvəz edilir və dəyişdirmə prosesi D səviyyəsinə qədər davam etdiriləcək. ML çıxışın əvvəlinə əlavə olunur, beləliklə şifrələnmiş mətn yaradılacaq.

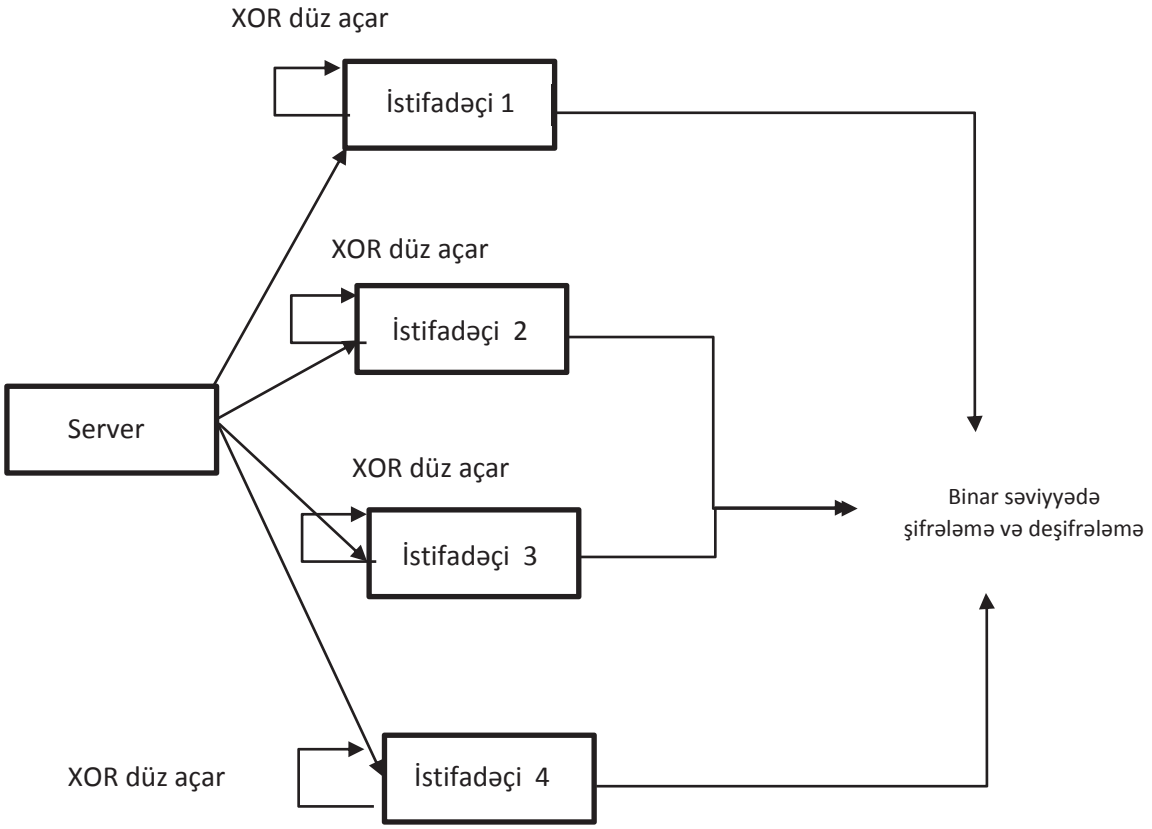
Şifrənin açılması

Bütün fərqli blokları toplayaraq, hər blok üçün identifikasiya işarələri təyin edilir. Bu identifikasiya nişanı identifikasiya nişanının birinci səviyyəsi ilə eynidir. Şifrələnmiş mətnin əvvəlindən uzunluğu açarla müəyyən edilən dəyişməz blok (ML) Əlavə edilir.

Sonra hər bir tanınma nişanı identifikasiya nişanları ilə əvəz olunur. Bu prosesdə hər bir fərqli bloka qarşı iki fərqli identifikasiya işarəsi tapılır. D səviyyəsinə qədər identifikasiya işarələrinin tapılmasını tərs qaydada təkrar edilir. İdentifikasiya işarələri üçün eyni proseduru təkrarlanılır. Açarın köməyi ilə bütün identifikasiya işarələrini onun binar formasına dəyişdirilir. Bütün bit axın blokları bir yerə toplanılır. Bu birləşmədən sonra UB axın sonunda yaradılan şifrəsi deşifrələnmiş bitə əlavə olunur.

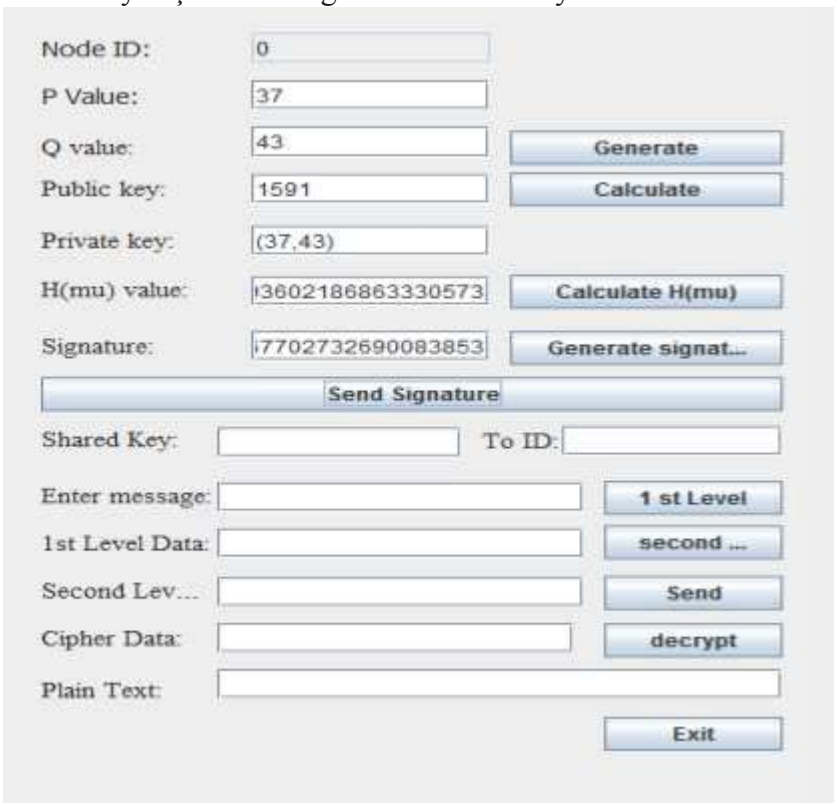


İmzanın identifikasiya edilməsi üçün serverə göndərilməsi

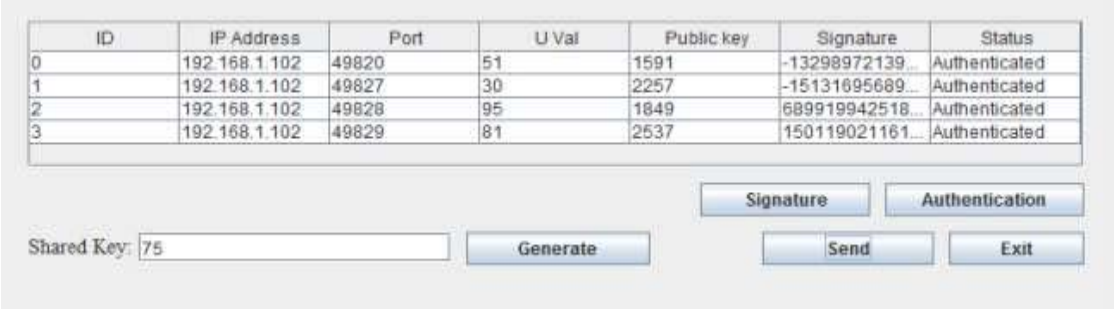


2. Təklif edilən üsulun simulyasiya edilməsi

Müştəri tərəfindən yaradılan imza. İlk göndərən istifadəçi tərəfindən verilən P, Q dəyərlərinə əsaslanaraq açıq açarı hesablayacaq. Bu dəyərlər yenidən hash funksiya XOR şəxsi açarı yaratmaq üçün istifadə edilir və identifikasiya üçün serverə göndəriləcək imza yaradır.



Server Doğrulaması. İmzanı aldıqdan sonra server istifadəçinin identifikasiyasını həyata keçirir və gələcək kommunikasiyanı davam etdirmək üçün ortaq açarı imzanı göndərmiş bütün müştərilərə təqdim edir.



İnformasiyanının ötürülməsi. Server tərəfindən göndərilən paylaşılan açarı aldıqdan sonra istifadəçi qəbul edən istifadəçinin id-sini daxil edəcək və sonra şifrələmə üsullarından istifadə edilməklə şifrələnəcək və konkret istifadəçiyə informasiya göndəriləcək informasiyanı daxil edəcək. Burada 2 səviyyəli şifrələmə metodundan istifadə edilir. Burada $01, 00, 10, 11$ sırasına görə 4 fərqli blok mövcuddur. Beləliklə, açar yaratma metoduna uyğun olaraq $01 = a, 00 = b, 10 = c$ və $11 = d$ təyin edilir. Bu 1-ci səviyyə identifikasiya nişanlarıdır. 2-ci səviyyəli identifikasiya işarələrinin yaradılması üçün a, b, c və d –nin iki bit təsviri $aa, ab, ac, ad,\ bb, bc, bd, cc, cd, dd, ba, ca, da, cb, db, dc -$ dir. İki bit təsvirlərin hər biri üçün simvol təyin edilir: $aa = e, ab = f, ac = g, ad = h, bb = i, bc = j, bd = k, cc = l, cd = m, dd = n, ba = o, ca = p, da = q, cb = r, db = s, dc = t.$ Hər bir blok üçün identifikasiya nişanlarının yaranma səviyyəsi və bölünmüş blokun uzunluğu hesablama zamanı təsadüfi olaraq seçilir, çünki onun açarı hər bir şifrələmədən digərinə fərqlənir. Hər bir blok identifikasiya işarələrini yaratmaq üçün görünən ardıcıllıqla bölünmüş blokları götürülür.

İnformasiyanın qəbulu. Qəbul edən informasiyanının şifrəsini açma üsulu ilə deşifrə edəcək və göndərən tərəfindən göndərilən faktiki informasiyanı alacaq.

Bütün fərqli blokları toplayaraq, hər blok üçün identifikasiya işarələri təyin edilir. Bu identifikasiya nişanı identifikasiya nişanının birinci səviyyəsi ilə eynidir. Şifrələnmiş mətnin əvvəlindən uzunluğu açara qədər müəyyən edilən dəyişməz blok (ML) əlavə edilir.

Sonra hər bir tanınma nişanı identifikasiya nişanları ilə əvəz olunur. Bu prosesdə hər bir fərqli bloka qarşı iki fərqli identifikasiya işarəsi təyin edilir. D səviyyəsinə qədər identifikasiya işarələrinin tapılmasını tərs qaydada təkrar edilir. İdentifikasiya işarələri üçün eyni proseduru təkrarlanılır və

məlumatlar geri alınır. Açarın köməyi ilə bütün identifikasiya işarələrini onun binar formasına dəyişdirilir. Bütün bit axın blokları bir yerə toplanılır. Bu birləşmədən sonra UB axın sonunda yaradılan şifrəsi açılmış bitə əlavə olunur.

Nəticə

Nəticədə, bu üsulları tətbiq etməklə məlumatların ötürülməsi üçün daha çox təhlükəsizlik və səmərəliliyi təmin edirik. Hacking və digər narahatlıqlar kimi əvvəlki problemlərin çatışmazlıqlarını aradan qaldıra bilər. Təyinat node təhlükəsiz və düzgün məlumatları alır. Bunlarda istifadəçi identifikasiyası, şəxsiyyət əsaslı imza, şifrələmə və şifrənin açılması konsepsiyaları təklif edilmişdir. Bu konsepsiyaların təklif edilməsi ilə verilən sistemə daha çox təhlükəsizlik və səmərəlilik əlavə olunacaq. Hal-hazırda məlumatların ötürülməsi gündəlik həyatda mühüm rol oynayır, lakin məlumatların ötürülməsi təhlükəsiz olmalıdır. Beləliklə, məlumatları təhlükəsiz şəkildə göndərmək üçün bəzi metodlar tətbiq edilməlidir. Tanınma ilə istifadəçinin identifikasiyası kimi və kommunikasiya üçün açar yaratma alqoritmi istifadə olunur. Burada başqa bir üsuldan istifadə edilik ki, açar məlumatlarla idarə olunur. Şifrəni alır və sonra ikili səviyyəli metod şifrələmə və deşifrələmə üçün istifadə olunur. Bu metodu tətbiq etməklə məlumatların ötürülməsi üçün daha çox təhlükəsizliyi və səmərəliliyi təmin edilir.

Ədəbiyyat

1. A.A. Abbasi and M. Younis, ―A Survey on Clustering Algorithms for Wireless Sensor Networks, Computer Comm.
2. K. Pradeepa, W.R. Anne, and S. Duraisamy, ―Design and Implementation Issues of Clustering in Wireless Sensor Networks, Int'l J. Computer Applications.
3. S. Andru, J. Tanenbaum, J. David, T. Wetherall, Computer Networks, 5th ed., Pearson, 2011.
4. T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless SensorNetwork Technologies for the Information Explosion Era, Studies inComputational Intelligence.
5. Y. Wang, G. Attebury, and B. Ramamurthy, ―A Survey of SecurityIssues in Wireless Sensor Networks, IEEE Comm. Surveys &Tutorials.
6. L.B. Oliveira et al., ―SecLEACH-On the Security of Clustered Sensor Networks, Signal Processing.

7. K. Zhang, C. Wang, and C. Wang, ―A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management,‖ Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM)
8. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, ―AnApplication-Specific Protocol Architecture for Wireless MicrosensorNetworks, IEEE Trans. Wireless Comm.
9. M. Grygiel, R. Żurkowski, Experimental system for measuring latency in ZigBee 802.15.4 standard, Wydział Elektrotechniki i Automatyki, Politechnika Gdańska, Gdańsk 2009.
10. Manjeshwar, Q.-A.Zeng, and D.P. Agrawal, ―An AnalyticalModel for Information Retrieval in Wireless Sensor NetworksUsing Enhanced APTEEN Protocol, IEEE Trans. Parallel &Distributed Systems.
11. S. Yi et al., ―PEACH: Power-Efficient and Adaptive ClusteringHierarchy Protocol for Wireless Sensor Networks, ComputerComm.
12. P. Banerjee, D. Jacobson, and S. Lahiri, ―Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks,‖Proc. IEEE Sixth Int'l Symp.Network Computing and Applications (NCA), pp. 145-152, 2007.

Rəyçi: tex. ü. f.d, dos. Sərdar Qasımov

Göndərilib: 18.02.2022 Qəbul edilib: 22.03.2022