LoRaWAN şəbəkəsində istifadəçi məlumatlarının təhlükəsizliyi problemləri və həlli yolları

Təbriz Ağaşov
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
tabriz@science.az

***Xülasə*— Məqalədə əşyaların internetində (IoT) istifadəçi məlumatlarının təhlükəsizliyi üçün mövcud olan kriptoqrafik açarların idarəetmə protokolu araşdırılmış və reputasiya sistemini tətbiq etməklə IoT-larda istifadə olunan LoRaWAN şəbəkə arxitekturasının təhlükəsizliyini artırmaq üçün həll təklif edilmişdir. Məqalədə kriptoqrafiyaya əsaslanan bəzi təhlükəsizlik məsələləri analiz edilmiş və həll yolları göstərilmişdir.**

Açar sözlər— IoT; LoRa; LoRaWAN; AES128; kriptoqrafik açar; heterogen; end nod; proksi-nod

I. GİRİŞ

Əşyaların interneti insanlara aid olan bir çox cihazları İnternet-ə bağlayaraq həyatımıza daxil olmuşdur. Bu həm insanlara daha ağıllı və daha rahat yaşamağa imkan verir, həm də onların fərdi və məxfi məlumatlarına, eləcə də onlara məxsus müxtəlif elektron cihazlara təcavüz edilməsinə zəmin yaradır. IoT-lar İnternetin mövcud infrastrukturunda unikal indentifikasiyaya malik fiziki qurğulardır. Bu qurğular ətraf mühitdən məlumatların toplanması və onların İnternet üzərindən intellektual şəbəkələr, ağıllı şəhərlər, ağıllı evlər və elektron səhiyyədə tətbiqi üçün istifadə edilir [1, 2].

Əşyaların İnternetinin məqsədi insanların gündəlik həyat şəraitinin yaxşılaşdırılması, yeni və daha əlverişli iş yerlərinin açılması, biznes üçün yeni imkanların yaranması, istehsalda səmərəliliyin, məhsuldarlığın və rəqabətədavamlılığın artırılmasıdır. Əşyaların internetində istifadə olunan qurğular arasındakı qarşlıqlı əlaqə onların şəbəkəsini əmələ gətirir. Əşyaların interneti hamı üçün əlyetərli olan adi İnternet qovşaqlarından, həmçinin qeyri-məhdud sayda xüsusi şəbəkədən ibarətdir [1].

İnternetin tənzimlənməsi ilə bağlı bütün problemlər əşyaların interneti üçün də aktuallıq kəsb edir. İnformasiya təhlükəsizliynin, istifadəçilərin fərdi məlumatlarının qorunması kimi məsələlər həll edilmədən bu şəbəkənin uğurlu fəaliyyəti mümkün deyil. Beləliklə, istifadəçilərin fərdi və məxfi məlumatlarını müxtəlif hücümlardan qorumaq üçün təhlükəsizlik məsələlərinin həllərindən istifadə etməklə əşyaların internetinin tam funksionallığına nail olmaq mümkündür. Bunun üçün, adətən, IoT-ların heterogenlik xassələrinə uyğunlaşdırılmış və kriptoqrafik əməliyyatları yerinə yetirə bilən protokollarla düzgün idarə edilməsi mümkün olan kriptoqrafik açarlardan istifadə edilir. Təklif olunan protokol iki əsas kateqoriyaya bölünür [3]:

- iki tərəf (“end nod” və şəbəkə serveri, “end-nod” və istifadəçi tətbiqi) arasında əlaqə açarının idarəetmə protokolu;
- qrupda (müvafiq olaraq üç və daha çox “end nod”dan təşkil edilmiş proksi-nodlar qrupu) əlaqəni təmin etmək üçün yaradılmış ümumi açarın idarəetmə protokolu.

IoT-lar üçün LoRaWANşəbəkəsinin çoxlu sayda ümumi təhlükəsizlik arxitekturası mövcuddur. Tədqiqatçıların apardığı analizlər əsasında LoRaWAN-nın təhlükəsizlik arxitekturası sənaye, kənd təsərrüfatı, şəhər infrastrukturu və digər sahələrdə tətbiq edilən IoT-ların tələbatına uyğun olan ən son layihələrdən biridir. Bu arxitektura ağıllı əşyalar arasında qarşlıqlı əlaqənin və təhlükəsiz mübadilənin təmin edilməsi üçün təklif edilmişdir. Bunu bir neçə səviyyəli şifrələmə tətbiq etməklə həyata keçirmək olar [4]:

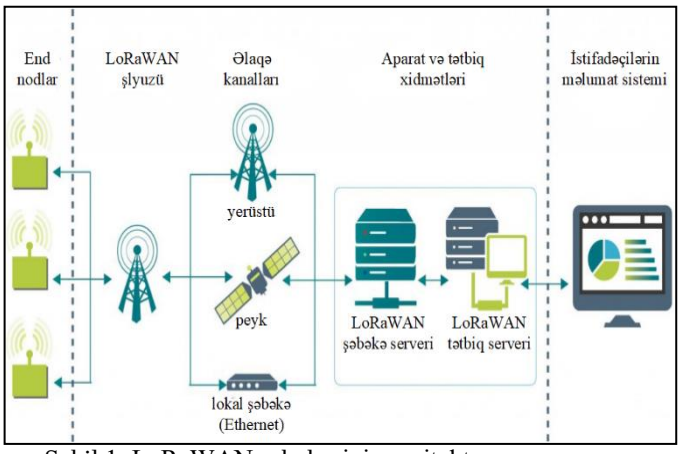
- şəbəkə səviyyəsi – “end nod”dakı məlumatların audentifikasiyasına təminat verir və “end nod”larla şəbəkə serveri arasında paylaşılan AES128 gizli açarı ilə təsdiqlənir;
- tətbiq səviyyəsi – “end nod” və istifadəçi tətbiqləri arasında paylaşılan AES128 gizli açarından istifadə edərək nodlardakı məlumatların məxfiliyi təmin edilir.

Bu işdə ikitərəfli paylanmış mövcud açarları idarəetmə protokoluna və reputasiya sisteminə əsaslanaraq LoRaWAN şəbəkə arxitekturasının təhlükəsizliyini artırmaqla istifadəçi məlumatların təhlükəsizlik həlli araşdırılmışdır.

II. LORAWAN-NIN ARXİTEKTURASI

LoRaWAN – aparat səviyyəli LoRa protokolu ilə dəstəklənən geniş əhatə radiuslu qlobal şəbəkədir və şlyuzlər (baza stansiyalar) vasitəsilə sondakı LoRa qurğuları (“end nod”lar, qovşaqlar) arasında kammunikasiya yaradır. LoRaWAN enerjiyə qənaət etmək üçün optimallaşdırılmış ağıllı cihazların bir-biri ilə əlaqə yaratmasını həyata keçirən, məlumatı uzaq məsafələrə ötürən və geniş əhatə radiuslu şəbəkə xüsusiyyətlərinə malikdir. Bu bölmədə LoRaWAN şəbəkəsinin arxitekturası şərh olunub.

DOI: 10.25045/NCInfoSec.2019.39



Şəkil 1. LoRaWAN şəbəkəsinin arxitekturası

Şəkil 1-dən göründüyü kimi bu şəbəkə “end nod”lar (LoRa qurğuları, IoT-lar), şlyuzlər, şəbəkə serveri və tətbiqi serverlərdən ibarətdir. Şlyuz “end nod”lardan qəbul edilmiş məlumat paketlərini müxtəlif rabitə (Wi-Fi, mobil əlaqə, Ethernet, yaxud peyk əlaqəsi) vasitələri ilə şəbəkə serverinə ötürür. Server şəbəkədəki bütün şlyuzlərin idarə edilməsinə cavab verir, “end nod”lara müraciəti təmin etmək üçün hansı şlyuzdən istifadə edilməsini müəyyən edir, məlumatların ötürülmə sürətini avtomatlaşdırır, qəbul edilmiş paketləri filtirləyir və məlumatların təhlükəsizliyinin təmin edilməsini yerinə yetirir. Məlumatların emal edilməsi tətbiq serverlərində yerinə yetirilir. Cədvəl 1-də bu arxitekturanın üstünlükləri təqdim edilmişdir.

CƏDVƏL 1. LORAWAN-IN ÜSTÜNLÜKLƏRİ

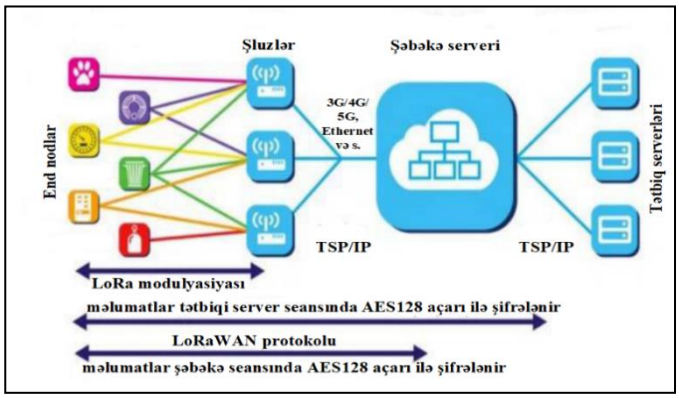
Üstünlüklər	Xüsusiyyətlər
Enerjiyə qənaət	nodlar qeyri-sinxrondur və sadəcə məlumatları ötürən anda qarşılıqlı əlaqədə olurlar
Yüksək buraxılış (ötürmə-qəbuletmə) qabiliyyəti	buna məlumatları ötürmək üçün adaptiv sürət rejimindən və xüsusi (çoxkannalla ötürmə xassəsinə malik multimodemli) şlyuzlərdən istifadə etməklə nail olmaq olur. Bu zaman paralel olaraq bir neçə kanaldan məlumat almaq olur.
Müxtəlif sinifli qurğular	üç sinif müəyyən edilmişdir: A, B və C.
Təhlükəsizlik	təhlükəsizliyin iki səviyyəsi müəyyən edilmişdir: şəbəkə və tətbiq. Hər iki səviyyə üçün AES (Advanced Encryption Standard) şifrələnməsindən istifadə edilir.

“End nod”lar – bu istifadəçilər tərəfdə quraşdırılmış sensorlar, ötürücülər, sayğaclar, aktuatorlar və IoT radiomodullarının ümumiləşdirilmiş adıdır. “End nod”lar üç sinfə bölünür:

- A sinfi - ikitərəfli mübadilə yaratmaq xassəsinə malik “end nod”lar. A sinfi əsas baza sinfi olaraq şəbəkədəki bütün qurğularda dəstəklənir. Qeyd edək ki, əlaqənin yaranmasını təşkil edən də elə bu “end nod”lardır. Nod hər bir ötürmədən sonra qəbul üçün qısa müddətli iki müvəqqəti pəncərə ayırır və bu qısa vaxt ərzində serverdən cavab gözləyir. Ötürmə intervalı “end nod”un ehtiyac meyarına əsaslanaraq planlaşdırılır. A sinfindən olan qurğular az güc sərf edərək serverə məlumatı ötürür və yalnız, bundan sonra tətbiqlərin vasitəsilə serverdən geriyə məlumat göndərilməsini tələb edir. Serverdən sondakı “end nod”a məlumatların ötürülməsi, həmin nodun serverlə əlaqəyə girdiyi anda mümkün olur;
- B sinfi - onlar da ikitərəfli mübadilə yaradır. B sinfində də A sinfində olan funksiyalar mövcuddur. Bundan başqa B sinfindən olan qurğular cədvəl üzrə qeyd edilmiş vaxtda qəbul üçün əlavə pəncərə açır. Qəbul üçün pəncərənin açılması, şlyuzlərin xüsusi siqnallarla (mayak, beacons) “end nod”ları sinxronlaşdırmasından sonra baş verir. Bu isə serverə nodun məlumatı qəbul etməsinə hazır olduğunu bildirir;
- C sinfi - Verilənləri qəbul etmək üçün maksimal sayda pəncərə ayırmaq imkanına malikdirlər. Qəbul pəncərəsi verilənləri ötürmə anında bağlanır. Bu tip qovşaqlar böyük həcmli verilənlərin mübadiləsi məsələləri üçün tətbiq edilir. Praktiki olaraq, C sinfindən olan qovşaqlar verilənləri ötürdükləri hallar istisna olmaqla, hər zaman qəbul rejimində olurlar. Belə qovşaqların enerji saxlama müddəti çox olur və bunun nəticəsində qəbuledicinin işləmə vaxtını məhdudlaşdırmağa ehtiyac olmur.

III. ŞƏBƏKƏ VƏ TƏTBİQİ SƏVİYYƏLƏRİNDƏ TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Məqalədə LoRaWAN şəbəkəsində OSI (Open Systems Interconnection) modelinin iki səviyyəsi üçün: şəbəkə və tətbiqi səviyyələrdə məlumatların mübadiləsi zamanı təhlükəsizliyin təmin edilməsi məsələsinə baxılmışdır (şək. 2).



Şəkil 2. LoRaWAN-nın təhlükəsizlik arxitekturası

Şəbəkə səviyyəsində “end nod”lardakı məlumatların autentifikasiyası, “end nod” və server arasında birgə istifadə olunan AES128 kriptoqrafik açarın köməyi ilə təsdiqlənərək müəyyən olunur. Tətbiqi səviyyədə isə “end nod” və istifadəçi tətbiqlərin birgə istifadə etdiyi AES128 kriptoqrafik açar vasitəsilə qurğulardakı məlumatların təhlükəsizliyini təmin etmək olur. LoRaWAN şəbəkəsində “end nod”lar və şəbəkə

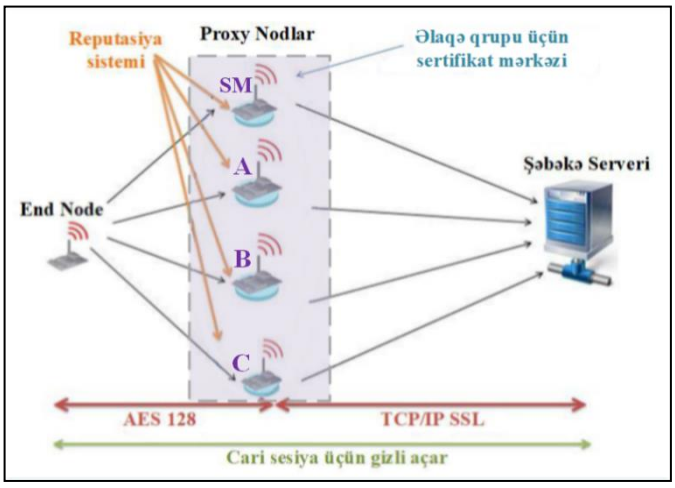
serveri arasında məlumatların mübadiləsinin təhlükəsizliyi üçün AES128 məxfi şifrələmə açarından istifadə edilir.

Əgər müdaxilə edən bu məxfi açarı əldə edərsə, onda o “end nod” və şəbəkə serveri arasında mübadilə olunan bütün məlumatları oxuya bilər və dəyişər.

Aşağıdakı bölmədə “end nod” və şəbəkə serveri arasında mübadilə zamanı belə müdaxilələrin qarşısını almaq üçün hər bir seansda açarların dəyişdirilməsi həlli təklif olunmuşdur. Əgər məlumatların mübadiləsinin hər bir seansında şifrə dəyişdirilərsə, onda bu daha təhlükəsiz və etibarlı əlaqənin yaranmasına imkan verəcək.

IV. TƏKLİF OLUNAN HƏLL

Bu bölmədə LoRaWAN şəbəkəsinin təhlükəsizlik protokollarını təkmilləşdirmək üçün həll təklif edilmişdir. Təklif olunan həlldə təhlükəsizlik açarlarının idarə edilməsi üçün reputasiya sistemindən istifadə edlir [5]. Şəkil 3-də LoRaWAN şəbəkəsinin təhlükəsizlik arxitekturası göstərilmişdir. Burada məhdud sayda nodlar bir qrup şəklində birləşdirilərək onlar arasındakı hesablamaları asanlaşdırmaq üçün proksilər (proksi-nodlar) yaradılmışdır. Təhlükəsizliyi gücləndirilən nodun AES128 şifrələnmiş açarı hər bir seansda yeni açarla əvəz edilir. Bu açar [5]-də göstərilən həll qaydasına uyğun olaraq “end nod” və şəbəkə serveri arasında quraşdırılır. Tətbiq edilmiş reputasiya sistemi proksi-nodların arasından daha etibarlı qovşağı seçir. Bu isə kriptoqrafik açarların qəbul edilməsi mərhələsində yalnız etibarlı qovşaqların iştirak etməsinə və hücuma məruz qalmış zərərli qovşaqlar tərəfindən baş verə biləcək təhlükənin qarşısının alınmasına imkan verəcək.



Şəkil 3. LoRaWAN-nın təhlükəsizlik arxitekturası

LoRaWAN şəbəkəsinin bu yeni arxitekturası enerji sərfiyyatı və hesablama gücü baxımından heterogen qovşağları özündə birləşdirir. Burada üç fərqli qovşaq nəzərdən keçirilmişdir:

- “end nod” (müxtəlif ötürücülər, sensorlar, LoRa qurğuları): mürəkkəb kriptoqrafik əməliyyatları dəstəkləmirlər və məhdud resurslara malikdirlər;
- şəbəkə şlyuzü: “end nod”larla qonşuluqda yerləşdirilmiş və mürəkkəb kriptoqrafik əməliyyatları yerinə yetirməyə malik olan qovşaqlar;
- şəbəkə serveri: yüksək həcmli yaddaş tutumuna, çevik hesablama imkanlarına və yüksək enerji istehlakına malik qovşaqlar.

Məqalədə növbəti fərziyyələr əsasında tədqiqat işi aparılmışdır.

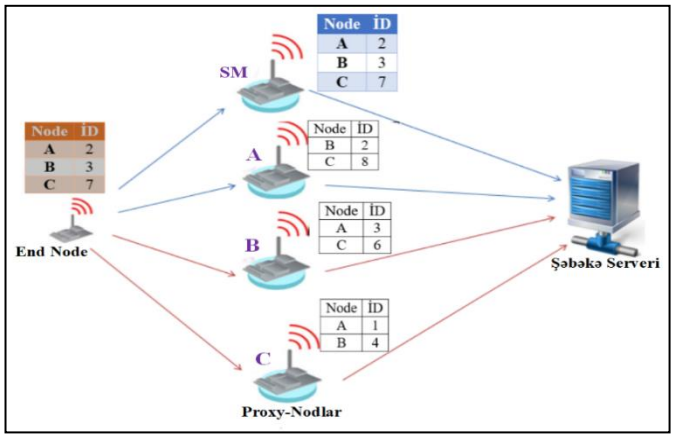
- “end nod” və proksi-nodlar arasındakı əlaqənin təhlükəsizliyi AES128 kriptoqrafik açarı vasitəsilə təmin edilir;
- AES128 kriptoqrafik açarı “end nod” və hər bir şlyuz arasında etibarlı şəkildə mübadilə olunur;
- ilk Sertifikat Mərkəzi və ona uyğun AES128 məxfi açarı (nodların quraşdırılmasından əvvəl) əvvəlcədən “end nod”ların dinamik siyahısına əlavə edilir.

Bu fərziyyələrə əsaslanaraq aşağıdakı bölmədə LoRaWAN şəbəkəsinin təkmilləşdirilmiş təhlükəsizlik protokolunun üstünlüyü və mərhələləri şərh edilmişdir.

V. PROTOKOL VƏ ONUN MƏRHƏLƏLƏRİ

[5]-də təsvir olunan protokol nodların heterogenlik xassəsindən istifadə edir. Yəni məhdud funksiyalı qovşaqlar sadə kriptoqrafik şifrələməni yerinə yetirdiyi halda, daha geniş funksiyalara malik qonşu qovşaqlar daha mürəkkəb kriptoqrafik əməliyyatları yerinə yetirir. Bu protokolun üstünlüyü ondan ibarətdir ki, proksi hər seansda məxfi şifrənin bir hissəsini hesablayır, lakin ötürücü və qəbuledici qovşaqlarda hesablanmış tam şifrəni əldə edə bilmir. Burada hər bir nod proksi-nodlarin siyahısını və onlara uyğun məxfi açarları yadda saxlayır. Nəticədə, qonşu nodlarin sayı artdıqca böyük həcmli yaddaş tələb olunur. Kriptoqrafik açarın etibarlığı onların generasiyası prosesində iştirak edən proksi-serverlərin sayından aslıdır. Bu zaman məlumatların itməsi, yaxud saxta məlumtla dəyişdirilməsi son məxfi açarın hesablanmasına təsir edəcək. Beləliklə, bu həll variantını inkişaf etdirmək üçün ötürücü nodun proksi-nodları aşkar etməsi və məxfi açarın qəbul edilməsində bu proksi-nodların arasından ən etibarlısını seçməsi təklif edilmişdir. Sonra isə bu nod hər seansda açarların hesablanmasında iştirak edən həmin proksi-nodların yenilənən dinamik siyahısını yadda saxlayacaqdır [6].

Mərhələlər. Bu həlldə hər proksi-nodun digər nodların reputasiyasını müəyyən etməsi üçün onlardan məlumat toplaması fərz edilir. Bu məlumatlar ya nodun özü tərəfindən birbaşa toplanmış məlumatlardır, ya da digər qovşaqlardan alınan tövsiyələrdir. Nod qonşu nodların siyahısını və onların etibarlılıq dərəcələrini müəyyən edən qiymətləri (inam dəyərini) cədvəl şəklində toplayaraq saxlayır (şək. 4). Inamın qiymətləndirilməsi, məlumat paketlərini maneəsiz ötürmək, məxfi açarları hissələrlə düzgün göndərmək, normal giriş-çıxış, istifadə etdiyi kanalın gücü və onun buraxılış imkanları da daxil olmaqla, nodların davranışını qiymətləndirməklə hesablanır. Deməli, özünü yaxşı apran nod ona inamın artdığını görəcək və digər nodlar bunu qəbul edəcək, əksinə pis nodlar bunun əksini görəcəklər [7].



Şəkil 4. Ən etibarlı nodun seçilməsi

Ən yüksək inam dəyəri olan proksi-nod Sertifikat Mərkəzi (SM) kimi seçilərək, digər proksi-nodlar üçün autentifikasiya, avtorizasiya və açarların idarə edilməsi funksiyalarını yerinə yetirəcək. Burada SM üç cədvəldən ibarətdir:

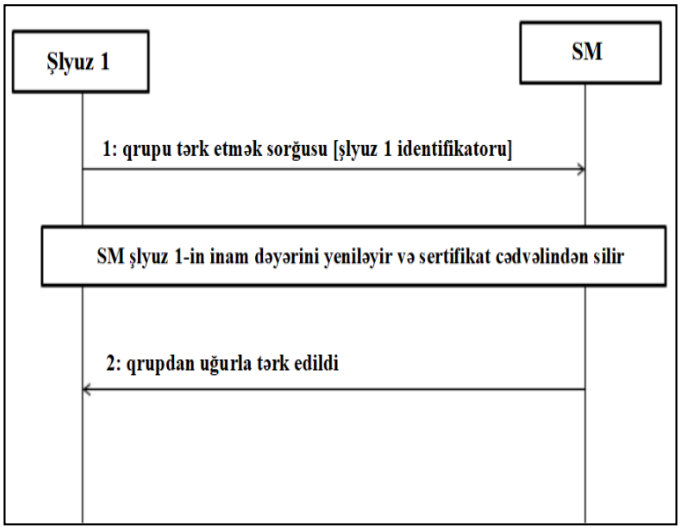
- proksi-nodların sertifikatlarının idarə edilməsi üçün istifadə olunan sertifikatlaşdırma cədvəli;
- hər bir proksi-nodun etibarlılıq dəyərini göstərən inam cədvəli;
- etibarlılıq dəyərləri sıfır olan bütün nodlar yerləşən qara siyahı.

Başlanğıcda ilk SM-in əvvəlcədən seçildiyi fərz edilir. Sonrakı hallarda o dinamik proksi-nodların inam dəyərlərinə uyğun olaraq yenilənir.

Hər bir proksi-nod özünün inam cədvəlini açıq açarla təmin edilmiş SM-ə göndərir. SM isə öz növbəsində bütün proksi-nodlardan alınan cədvəlləri bir araya gətirərək, AES128 məxfi açarla təmin edilmiş “end nod”a göndərmək üçün daha etibarlı bir qrupdan ibarət cədvəl yaradacaq. “End nod” yaradılan bu cədvələ əsaslanaraq açarın alınmasında iştirak edəcək ən etibarlı qonşuları seçəcək (şək. 4) və yeni SM-lər haqqında bütün proksi-nodları məlumatlandıracaqdır [8].

Protokolun ilkin mərhələsi. İlk mərhələdə, SM vasitəsilə şlyuzlər qrupu (proksi-nodlar) təşkil edilərək iki cədvəl, sertifikatlaşdırma və inam (əvvəlcə boş olan) cədvəlləri yaradılır. Sonra, SM multicast (çoxqütblü) prisipinə əsaslanaraq, hər bir şlyuzun açıq açarını qrupdakı digər üzvlərə ötürür. Beləliklə, hər bir proksi-nod qrupun digər üzvlərinin bütün açıq açarlarına malik olur. Bu açarlar qrupun üzvləri arasındakı informasiya mübadiləsinin təhlükəsizliyini təmin etməklə yanaşı, əsasında proksi-nodlar olan inam cədvəllərinin yaradılmasında da istifadə ediləcəkdir. Sonra hər bir iştirakçı üzv açıq açarla qorunan öz inam cədvəlini SM-ə göndərəcək. SM bütün inam cədvəllərini aldıqdan sonra onlardakı inam dəyərlərinin ortalama nisbətini hesablayacaq və “end nod”a göndərilməsi üçün yekun inam cədvəlini yaradacaq. Beləliklə, “end nod” məlumatları qrupdakı şlyuzlərlə bölüşmək istədikdə, o əldə etdiyi inam cədvəlindən istifadə edərək, bu cədvəldəki ən yüksək inam dəyərlərinə malik proksidən istifadə edəcək [9].

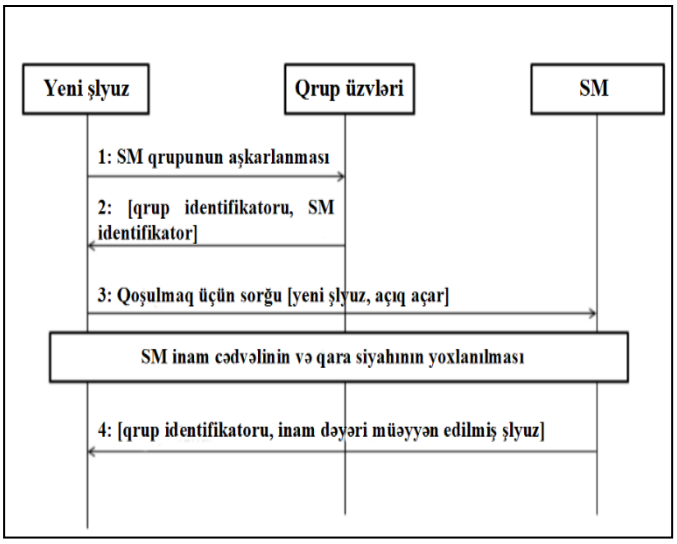
Nodun qrupa qoşulması. Proksi-nodlar qrupuna qoşulmaq istəyən yeni nod əvvəlcə SM-i aşkar etmək üçün qrupun bütün üzvülərinə mesaj göndərir (şək. 5). Mesajı alacaq ilk proksi-nod qrupun və Sertifikat Mərkəzinin identifikatorlarını özündə əks etdirən bir mesajla həmin noda cavab verir. Sonra nod, onun identifikatorunu və açıq açarını özündə saxlayan SM-ə qoşulmaq üçün sorğu göndərir. SM yeni nodun inam cədvəlində inam dəyərinə malik olub-olmadığını, yaxud onun qara siyahıya salındığını yoxlayır. Əks halda onun inam dəyəri 1-ə bərabər olmaqla inam cədvəlində saxlanılacaq. Daha sonra, SM məzmunu qrupun identifikatorundan və nodun inam dəyərindən ibarət olan bir mesajla cavab verəcək. Bu mesaj SM-ın məxfi açarı və nodun açıq açarı ilə şifrələnəcək. Sonda nod aldığı mesajı deşifrə etdikdən sonra aktivləşəcək [10].



Şəkil 5. Nodun qrupa qoşulması

Nodun qrupu tərk etməsi. Nod onun haqqında məlumatları saxlayan SM-ə qrupu tərk etmək üçün mesaj göndərir (şək. 6). SM mesajı qəbul etdikdən sonra sertifikat cədvəlindən bu noda

aid olan məlumatları silir və inam dəyərini yeniləyir (1-ə qədər azaldılır). SM cavab olaraq bu noda onun sertifikatının silindiyi və sistemdən (qrupdan) müvəffəqiyyətlə çıxarıldığı haqqında məlumat göndərir.



Şəkil 6. Nodun qrupu tərk etməsi

Yeni SM-in seçilməsi. SM öz inam cədvəlini yenilədiyi zaman və qrupdakı mövcud bir nodun daha yaxşı inam dəyərinə sahib olduğunu aşkar edərsə, həmin nodun yeni SM olduğunu bildirəcək. Müəyyən edilmiş yeni SM təhlükəsizlik baxımından qrup üzvlərinin hər birinin sertifikatını yeniləşdirməlidir. Beləliklə, o yeni sertifikat tələb etmək üçün hər bir qrup üzvünə mesaj göndərəcək. Proksi-nodlar identifikator və açıq açarlarını yeni formalaşan SM-ə göndərəcək, o isə öz növbəsində hər nodu yeni fərdi sertifikatla təmin edəcək. Bu zaman əvvəlki, yəni köhnə SM artıq adi proksi-nod funksiyasını yerinə yetirəcək.

VI. TƏKLIF OLUNAN HƏLLIN TƏHLÜKƏSIZLIYININ QIYMƏTLƏNDIRILMƏSI

Bu işdə təklif olunan həllin məqsədi bütün təhlükəsizlik məsələlərinin, xüsusən də məlumatın identifikasiya, məxfilik və tamlığının yoxlanılmasıdır. Məxfi məlumatlar onun məxfiliyinə zəmanət verən müvafiq açarlarla şifrələndiyi üçün təklif olunan protokolun əsas məqsədi AES128 məxfi açardan istifadə edərək, “end nod”larla şlyuzlər arasında o qədər də sürətli və böyük hesablamalar tələb edilməyən əlaqənin təhlükəsizliyini təmin etməkdir. Bu məqsədlə təklif edilən protokol, SSL (Secure Sockets Layer) sertifikatından istifadə edərək şluzlərlə şəbəkə serveri arasındakı əlaqənin daha da təhlükəsiz və etibarlı olmasına zəmin yaradacaq. Proksi-nodlar qrupunun üzvləri arasında mübadilə olunan məlumatlar nodların açıq açarları vasitəsilə qorunur. Mübadilənin sonrakı etaplarında məlumatlar və əlaqə “Man in the Middle” (ortada adam) hücümu ilə təhdid oluna bilər. Bu hücumdan müdafiə olunmaq üçün məlumatlar proksi-nodların xüsusi məxfi açarları ilə şifrələnir və bu şifrə proksi-nodlar arasından seçilmiş SM-də saxlanılır. Bu məlumatlar yalnız SM vasitəsilə deşifrə oluna bilir. Beləliklə, həm məlumatların həqiqiliyi, həm də əlaqənin təhlükəsizliyi ən təhlükəli hesab olunan “Man in the Middle” hücumundan müdafiə olunacaqdır. Qrupa daxil olan yeni noda göndərilən məlumat həmin nodun açıq açarı, həm də SM-in məxfi açarı ilə şifrələnir və bu açarın bir hissəsini alan proksi-nodlardan heç biri seans ərzində yekun açarı tam əldə edə bilmir. Bu işdə təklif olunan protokol “Man in the Middle” hücumana qarşı müdafiə üçün daha etibarlı hesab edlır [11].

NƏTİCƏ

Bu məqalədə əşyaların internetində istifadə olunan LoRaWAN şəbəkəsinin arxitekturasının təhlükəsizliyinin artırmaqla istifadəçi məlumatlarının təhlükəsizliyi üçün həll təklif edilmişdir. Təklif olunan bu həlldə açarların ikitərəfli idarə edilməsi üsulundan və mürəkkəb kriptoqrafik funksiyaları yerinə yetirən etibarlı qonşu qovşaqların seçilməsini təmin edən reputasiya sistemindən istifadə edilmişdir. Bütün mübadilələrdə eyni bir kriptoqrafik AES açarından istifadə edilərsə hücum edən şəxs bu açarı əldə də bilər. Belə təhlükələri aradan qaldırmaq üçün “end nod” və şəbəkə serveri arasında məlumat mübadiləsinin hər seansında yeni açardan istifadə edilməsi təklif edlmişdir.

İSTİNADLAR

[1] R.M. Əliquliyev, R.Ş. Mahmudov, Əşyalarin İnterneti: mahiyyəti, imkanlari və problemləri // İnformasiya cəmiyyəti problemləri, 2011, №2, s.29–40.

[2] A. Whitmore, A. Agarwal and Li Da Xu, The Internet of Things-Asurvey of topics and trends, Information Systems Frontiers, 2015, vol. 17, pp. 261–274.

[3] H. Ragab, A. Bouabdallah, H. Bettahar and Y. Challal, Key Management for Content Access Control in a Hierarchy, International Journal of Computer Networks, vol. 51, No. 11, 2007, pp. 3197-3219.

[4] LoRa Alliance Technical Marketing Workgroup, https://www.tuv.com /media/corporate/products_1/electronic_components_and_lasers/TUeV_ Rheinland_Overview_LoRa_and_LoRaWANtmp.pdf

[5] An. Braeken, P. Kumar, A. Gurtov, M. Ylianttila, Proksi-based end-to-end key establishment protocol for the Internet of Things, International Conference on Communication Workshop (ICCW), pp. 2677–2682.

[6] M. Riyadh Abdmeziem, T. Djamel and I. Romdhani, A Decentralized Batch-Based Group Key Management Protocol for Mobile Internet of Things (DBGK), International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015, pp. 1109–1117.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, Internet of Things: A survey on Enabling Technologies, Protocols and Apllications, IEEE Communications Survey and Tutorials, 2015, vol. 17, pp. 2347–2376.

[8] N. Renugadevi, G. Swaminathan, A.S Kumar, Key management schemes for secure group communication in wireless networks a survey, International Conference on Contemporary Computing and Informatics, 2014, pp. 446–450.

[9] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia and G. Bianchi, Key Management Protocol with Implicit Certificates for IoT systems, IoT-Sys’15 Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, 2015, pp. 37–42.

[10] Na S., Hwang D., Shin W., and Kim K.H., Scenario and countermeasure for replay attack using join request messages in LoRaWAN, International Conference on. IEEE, 2017, pp. 718–720.

[11] S. Tomasin, S. Zulian, L. Vangelista, Security analysis of LoRaWAN join procedure for Internet of Things networks, Wireless Communications and Networking Conference Workshops (WCNCW), 2017, pp. 1–6.

PERSONAL DATA SECURITY ISSUES AND THEIR SOLUTIONS IN LoRaWAN NETWORK

Tabriz Agashov
Institute of Information Technology of ANAS, Baku, Azerbaijan
depart4@iit.ab.az, tabriz@science.az

Abstract– The paper explores the existing cryptographic key management protocol for the user data security in the Internet of Things (IoT) and proposes a solution to improve the security of LoRaWAN network architecture used in IoTs. It also analyzes some security issues related to cryptography and provides solution ways. The study proposes a solution to facilitate the computation in end nodes through proxy nodes based on the cryptographic key management protocol.

Keywords– *IoT; LoRa; LoRaWAN; AES128; cryptographic key; heterogeneous; end node; proxy node*