# Securitatea în tehnologia WiMAX

Goia Călin Daniel
Grupa: 2231/1

## Cuprins

# 1. Abstract

Standardul IEEE 802.16, cunoscut și sub numele de WiMAX, este o tehnologie de bandă largă fără fir concepută pentru rețelele metropolitane (MAN). Așa cum se întâmplă în cazul oricărei tehnologii wireless, securitatea este o preocupare crucială, mai ales având în vedere potențialul de interceptare și acces neautorizat. Această lucrare examinează mecanismele de securitate utilizate în standardul IEEE 802.16, inclusiv autentificarea, autorizarea și criptarea. De asemenea, lucrarea analizează punctele forte și punctele slabe ale acestor mecanisme și vulnerabilitățile potențiale pe care atacatorii le-ar putea exploata, precum și unele măsuri care s-ar putea implementa pentru combaterea acestor probleme. Deși unele probleme de securitate au fost rezolvate prin adoptarea modificărilor recente și a soluțiilor de securitate din standardele IEEE 802.16 mai noi, lucrarea evidențiază necesitatea unei cercetări continue în acest domeniu. WiMAX este încă în proces de dezvoltare, iar pe măsură ce tehnologia avansează și devine mai stabilă, se deschide perspectiva pentru o utilizare extinsă și de succes în domeniul comunicațiilor wireless.

# 2. Introducere

WiMAX (Worldwide Interoperability for Microwave Access) este o tehnologie de comunicații wireless de bandă largă care funcționează pe baza standardului IEEE 802.16. WiMAX a fost proiectată să ofere acces fără fir în rețelele metropolitane, concepută pentru distanțe lungi, care se află în strânsă competiție cu alte tehnologii precum Wi-Fi, DSL sau cablul tradițional [1]. Securitatea în standardul IEEE 802.16 este un factor cheie pentru ca WiMAX să poată concura cu aceste tehnologii. Într-un mediu wireless, amenințările la adresa securității, cum ar fi interceptarea datelor și accesul neautorizat, reprezintă provocări semnificative. Implementarea unui nivel eficient de securitate în WiMAX poate contribui la creșterea încrederii utilizatorilor și la adoptarea pe scară largă a acestei tehnologii. Prin urmare, analiza și îmbunătățirea aspectelor de securitate în standardul WiMAX devin esențiale pentru dezvoltarea și evoluția acestei tehnologii.

Securitatea unei rețele wireless este o problemă care necesită tratată datorită naturii transmisiei. Rețelele fără fir folosesc unde radio pentru a transmite date, iar acestea pot fi interceptate foarte ușor, rețelele wireless fiind mai vulnerabile la amenințările de securitate decât rețelele de cablu. În orice tehnologie wireless, este esențial să avem o securitate care să asigure protejarea confidențialității și integrității datelor transmise precum și cea a utilizatorilor și dispozitivelor acestora. Cu toate acestea, rețelele WiMAX rămân vulnerabile la diferite amenințări de securitate, cum ar fi atacurile Denial of Service (DoS) sau atacurile man-in-the-middle, chiar și în contextul implementării măsurilor de securitate adecvate.

WiMAX încorporează o arhitectură de securitate solidă pentru a asigura confidențialitatea, integritatea și autenticitatea transmisiei de date. Mecanismele de securitate utilizate în WiMAX includ algoritmi avansați de criptare, protocoale de autentificare, controlul accesului și sisteme de detectare si prevenire a atacurilor.

Scopul acestei lucrări este de a examina și analiza securitatea în standardul IEEE 802.16 și de a aborda problemele de securitate specifice acestei tehnologii. Această lucrare este structurată în trei capitole importante după cum urmează. Capitolul 3 va oferi o imagine de ansamblu asupra arhitecturii fundamentale și componentele unei rețele WiMAX, având scopul unei mai bune înțelegeri a securității în această tehnologie. Capitolul 4 se va concentra asupra măsurilor de securitate implementate în tehnologia WiMAX, inclusiv criptarea datelor și procesul de autentificare și autorizare a utilizatorilor. Problemele de securitate specifice tehnologiei WiMAX, cum ar fi atacurile DoS (Denial of Service), atacurile man-in-the-middle și alte amenințări relevante vor fi abordate în profunzime în capitolul 5. Se va analiza impactul acestor probleme asupra securității și performanței rețelelor WiMAX.

# 3. Componentele arhitecturale fundamentale ale unei rețele WiMAX

Pentru o mai bună înțelegere a securității în standardul IEEE 802.16, este necesară introducerea unor concepte de bază referitoare la arhitectura unei rețele WiMAX. Arhitectura WiMAX este alcătuită din 5 componente de bază, acestea fiind: stația de bază (Base Station - BS), stația de abonat (Subscriber Station - SS), stația mobilă (Mobile Station - MS), stația de releu (Relay Station - RS) si rețeaua operatorului. În continuare, aceste componente fundamentale vor fi folosite mai departe în această lucrare sub forma abrevierilor lor în limba engleză (BS, SS, MS, RS).

Stația de bază (BS) servește ca nod care stabilește conexiunea logică între stația de abonat (SS) și rețeaua operatorului, reprezentând punctul central al unei rețele WiMAX. Aceasta gestionează comunicarea cu SS și controlează accesul la rețeaua operatorului. Prin intermediul stației de bază, SS obține acces la serviciile și resursele disponibile în cadrul rețelei. Stația de abonat (SS) este un dispozitiv endpoint în rețeaua WiMAX, care servește utilizatorii finali și permite conectarea lor la rețeaua operatorului. Stația mobilă (MS), care este un tip specific de SS, permite utilizatorilor să beneficieze de conexiune în timp ce se deplasează. Stația de releu (RS) este o componentă care ajută la extinderea acoperirii rețelei prin retransmiterea semnalului între BS și SS, aceasta fiind plasată la o distanța intermediară între BS și SS.

În Figura1 de mai jos este ilustrată una dintre topologiile principale implementate în rețelele WiMAX, cunoscută sub denumirea de „multi-hop relay". Această topologie oferă o soluție eficientă pentru a depăși limitările distanței de acoperire a unei singure BS, permițând extinderea și amplificarea semnalului prin intermediul RS [2]. Astfel, se asigură o acoperire mai mare a rețelei WiMAX în zonele extinse, care altfel ar fi dificil de atins cu o singură stație de bază.

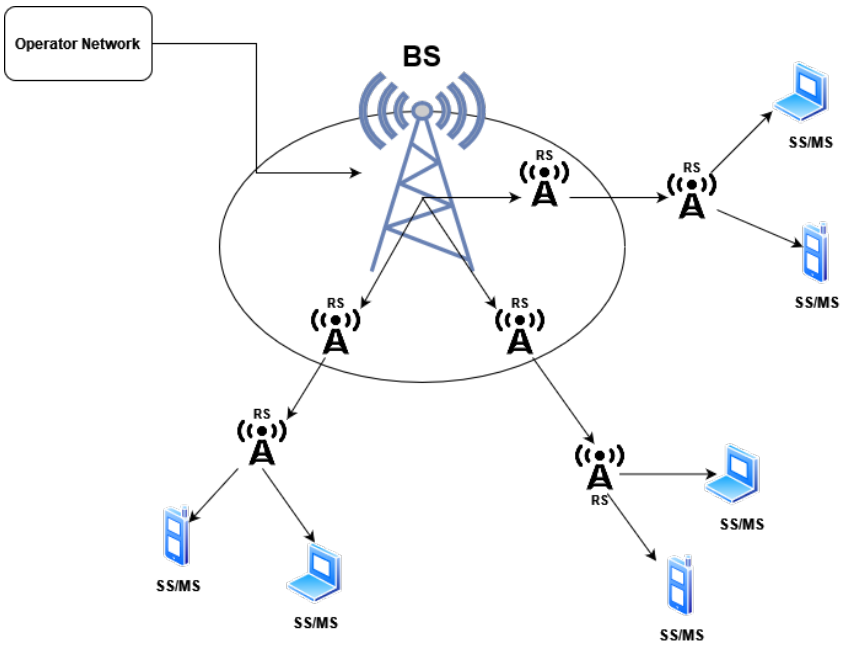


Figura 1. Topologia Multi-Hop Relay

# 4. Măsuri de securitate existente în tehnologia WiMAX

## 4.1 Elemente ale arhitecturii de securitate WiMAX

Standardul IEEE 802.16 utilizează un set de măsuri de securitate care implică trei pași esențiali: autentificarea, schimbul de chei și criptarea datelor [2]. După cum este ilustrat în Figura 1, acest framework oferă o imagine de ansamblu la nivel înalt a modului în care rețele WiMAX oferă comunicații securizate. Procedura de autentificare presupune furnizarea de informații critice de securitate între SS și BS, permițând astfel un schimb securizat de chei de criptare pentru datele transmise. Acest schimb asigură confidențialitatea comunicațiilor de date WiMAX, făcând dificil pentru atacatori interceptarea sau modificarea datelor.

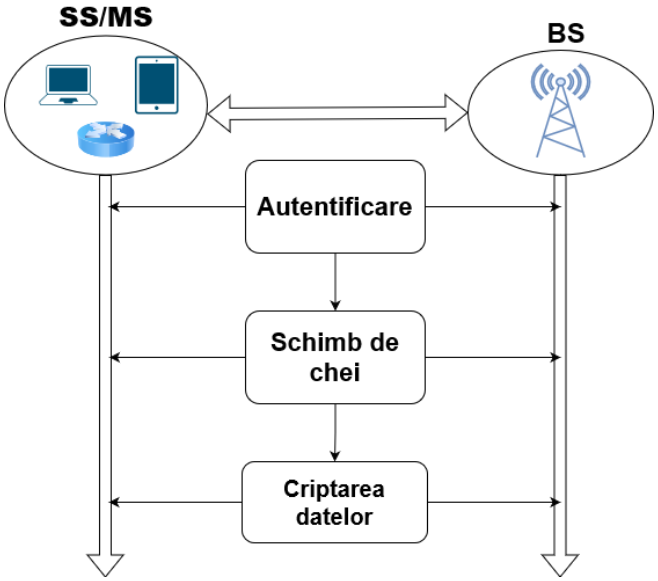


Figura 2. Framework-ul securității WiMAX

Cele două principale entități într-o rețea WiMAX, BS și SS, sunt protejate de următoarele caracteristici de securitate WiMAX:

1) Security Association (SA) joacă un rol critic în stabilirea și menținerea unei comunicații sigure într-o rețea. Un SA este o colecție de parametri de informații de securitate utilizate pentru a asigura comunicarea securizată între BS și unul sau mai mulți clienți SS [3]. Prin intermediul SA, unui SS i se acordă autorizația pentru accesarea unui serviciu WiMAX. În esență, SA servește ca mijloc de stabilire a încrederii între părțile care comunică, asigurându-se că datele sunt transmise în siguranță și împiedicând accesul neautorizat.

În standardul IEEE 802.16 sunt suportate două tipuri de SA, Authorization SA și Data SA. Authorization SA este utilizată pentru autorizarea SS și stabilirea Data SA între SS și BS, în timp ce Data SA protejează transportul conexiunilor [3]. Un Authorization SA conține următoarele atribute de securitate:

- Certificat X.509: un certificat digital folosit pentru identificarea SS.

- Cheie de Autorizare (Authorization Key - AK): înainte de a schimba cheia de criptare a traficului (Traffic Encryption Key - TEK), BS și SS/MS trebuie să se autentifice reciproc prin schimbul cheilor de autentificare (AK). Fiecare cheie de autentificare are identificator unic și o cheie care conține durata de viață a cheii de autorizare (AK).
- Cheie de Criptare a Cheilor (Key Encryption Key - KEK): derivată din AK, este utilizată de BS pentru a distribui TEK.

Un Data SA conține următoarele componente:

- Identificator SA (SAID): o valoare unică de 16 biți folosită pentru a deosebi SA între ele.
- Cheie de Criptare a Traficului (Traffic encryption key TEK): sunt generate aleatoriu de BS și sunt folosite pentru a cripta datele transmise prin rețelele WiMAX.

2) Protocolul PKM (Privacy Key Managment) este responsabil pentru distribuirea securizată a cheilor în WiMAX, oferind reguli de autentificare și autorizare. In plus, acest protocol este responsabil pentru autentificarea unei SS la BS. Protocolul PKM folosește un certificat digital X.509, algoritmul cu cheie publică RSA și un algoritm puternic de criptare, și anume Standardul de Criptare Avansată (Advanced Encryption Standard - AES).

## 4.2 Autentificarea și autorizarea

Într-o rețea wireless autentificarea este un mecanism care asigură că un anumit utilizator/dispozitiv este cel care pretinde a fi. În schimb, utilizatorul / dispozitivul ar trebui să poată verifica, de asemenea, autenticitatea rețelei la care se conectează. Acest proces se numește „mutual authentication” [4].

Autorizația este un mecanism care verifică faptul că un anumit utilizator are dreptul de a primi un anumit serviciu. În tehnologia WiMAX procesul de autorizație funcționează mână în mână cu mecanismul de autentificare. Pentru ca un utilizator să primească autorizația de a accesa rețeaua, protocoalele de autentificare trebuie îndeplinite [5].

Rețelele WiMAX utilizează protocolul PKM pentru autentificare. Procesul de autentificare și autorizare în WiMAX este ilustrat în Figura 3 și implică următorii pași pentru a stabili o conexiune sigură între o stație de abonat (SS) și o stație de bază (BS) [3]:

1. Pentru a se conecta cu stația de bază (BS), SS își trimite informațiile de autentificare printr-un mesaj de informare privind autentificarea. Acest mesaj conține certificatul digital X.509 al producătorului SS și este folosit de către BS pentru a verifica dacă SS-ul respectiv poate fi de încredere.

2. Imediat după ce SS trimite mesajul de informare privind autentificarea, SS trimite o cerere de autorizare către BS prin care solicită cheia de autorizare (AK). Această cerere conține certificatul X.509 unic al SS, o descriere a algoritmilor criptografici suportați de SS, precum și identificatorul unic SAID al SS.

3. După primirea cererii de autorizare, BS validează certificatul X.509 al SS, activează o cheie de autorizare (AK) pentru SS și ii trimite acesteia un mesaj de răspuns la cererea de autorizare.

Pentru a-și menține statutul de autorizare, SS trebuie să își reîmprospăteze periodic AK. Procesul de reautorizare este identic cu cel al procesului de autorizare inițială, cu excepția faptului că mesajul de informare privind autorizarea nu este trimis.

După ce autentificarea a fost realizată cu succes, începe a doua fază, care implică schimbul de chei de criptare a traficului (TEK), acestea fiind necesare pentru criptarea datelor [2].

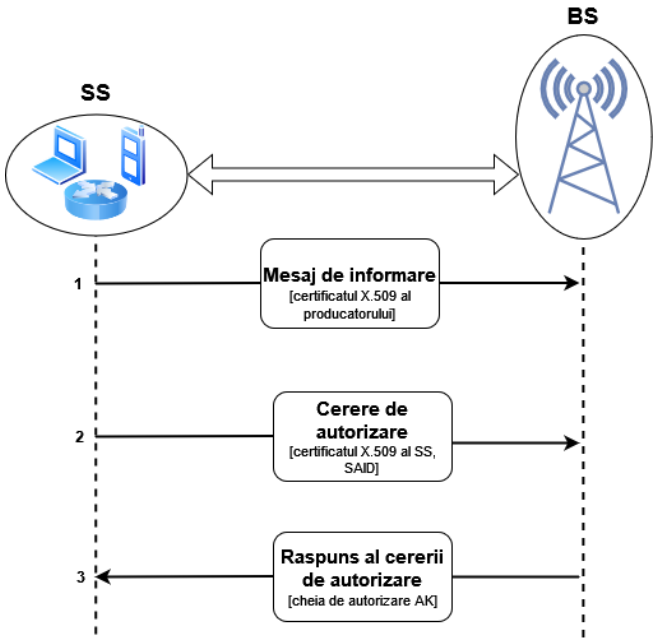


Figura 3. Procesul de autorizație PKM

## 4.3 Criptarea Datelor

Criptarea joacă un rol esențial în securitatea WiMAX prin asigurarea confidențialității și integrității datelor transmise prin rețea. WiMAX utilizează algoritmi de criptare puternici pentru a proteja datele utilizatorilor împotriva accesului neautorizat și a interceptării datelor.

Principalii algoritmi de criptare utilizați în tehnologia WiMAX sunt Standardul de Criptare a Datelor (Data Encryption Standard DES) si Standardul de Criptare avansata (Advanced Encryption Standard AES).

Standardul de Criptare a Datelor (DES) este un algoritm de criptare cu cheie simetrică care a fost implementat în standardele inițiale ale tehnologiei WiMAX. DES funcționează pe blocuri de date de 64 de biți și utilizează o cheie de 56 de biți pentru criptare. Principalul dezavantaj al algoritmului DES este dimensiunea relativ mică a cheii sale, ceea ce îl face susceptibil la atacuri de căutare exhaustivă [6]. Prin urmare, în standardele mai noi, DES a fost înlocuit de algoritmul AES, acesta fiind mai sigur.

AES este un algoritm de criptare cu cheie simetrică care operează pe blocuri de date și utilizează chei de 128, 192 și 256 de biți. AES funcționează prin aplicarea unei serii de transformări matematice asupra datelor în text simplu pentru a le converti în text cifrat, făcându-le indescifrabile fără cheia de decriptare corespunzătoare [7]. Adoptarea acestui algoritm pe scara larga în diverse industrii si arhitecturi de securitate, inclusiv WiMAX, este o dovada a robusteții și eficienței sale in protejarea datelor. Prin urmare, se recomandă utilizarea AES în locul DES pentru criptarea datelor in WiMAX cu scopul de a asigura o securitate mai puternică împotriva potențialelor vulnerabilități.

# 5. Probleme de securitate în tehnologia WiMAX

Ca orice altă tehnologie wireless, WiMAX este vulnerabilă la diferite amenințări de securitate care pot compromite confidențialitatea, integritatea și disponibilitatea datelor transmise prin rețea. Aceste amenințări de securitate pot fi clasificate în mai multe tipuri, inclusiv atacuri la nivel fizic, atacuri la nivelul legăturilor de date și atacuri la nivel de rețea. În aceasta parte a lucrării se vor discuta pe scurt câteva din amenințările de securitate, cum ar fi atacuri la nivelul stratului fizic, atacuri DoS sau atacuri man-in-the-middle, precum și contramăsuri împotriva acestor atacuri. Înțelegând amenințările la adresa securității WiMAX, se pot dezvolta strategii eficiente pentru a asigura funcționarea sigură și fiabilă a rețelelor WiMAX.

## 5.1 Atacuri DoS

Atacurile de tip Denial-of-Service (DoS) reprezintă o amenințare la adresa securității WiMAX, care poate perturba disponibilitatea resurselor rețelei și poate împiedica utilizatorii legitimi să acceseze rețeaua. Atacurile DoS sunt definite ca o încercare frauduloasă de a indisponibiliza sau bloca resursele unui calculator [8]. Aceste atacuri implică în mod obișnuit inundarea rețelei cu un număr mare de solicitări, ceea ce face ca rețeaua să devină supraîncărcată și să nu răspundă la solicitările legitime ale utilizatorilor. Un atac DoS folosește adresa IP pentru a ataca rețeaua utilizatorului și împiedică comunicarea între utilizatorul vizat si victima.

Conform ilustrației prezentate în Figura 4, dacă SS trimite o mulțime de cereri de autorizare false către BS, acesta își va folosi toate resursele pentru a calcula dacă acele informații sunt corecte. Acest lucru va cauza un atac DoS, deoarece BS nu va putea servi alte stații de abonat (SS) [9].

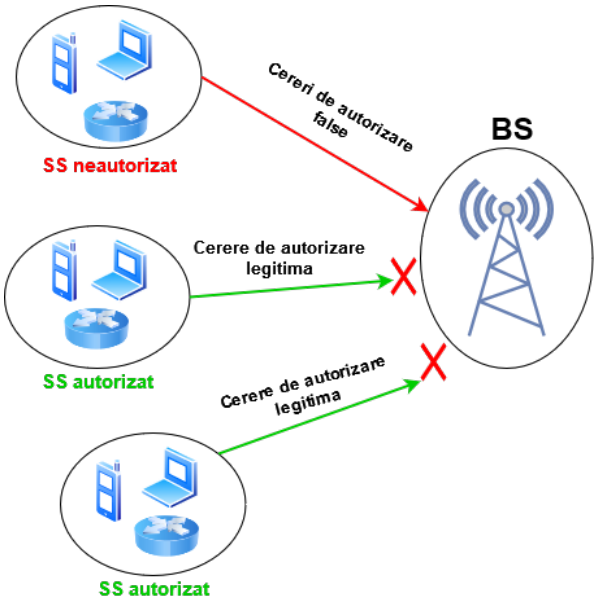


Figura 4. Atac de tip DoS în rețelele WiMAX

Acest tip de atac este foarte greu de prevenit, dar cu toate acestea se pot lua măsuri rapide pentru a rezolva problema. Anumite firewall-uri sunt echipate cu mecanisme de protecție încorporate împotriva atacurilor de tip Denial-of-Service (DoS). Aceste mecanisme monitorizează numărul de pachete primite și intervalul de timp în care au fost primite pentru a detecta și a limita eventualele atacuri DoS. De asemenea, un mecanism de apărare propus împotriva atacurilor de tip Denial-of-Service (DoS) implică utilizarea unui protocol SAI (Shared Authentication Information) [10]. În esență, protocolul SAI ar funcționa prin partajarea informațiilor de autentificare între stația de bază și clientul SS, ceea ce le-ar permite să detecteze și să prevină atacurile DoS mai eficient.

## 5.2 Atacuri de tip Man-in-the-Middle

Atacurile „man-in-the-middle" (MITM) reprezintă o amenințare des întâlnită la adresa securității WiMAX, care implică interceptarea și manipularea de către un atacator a comunicației dintre două părți legitime fără știrea lor [11]. Lipsa autentificării reciproce între stația de abonat (SS) și stația de bază (BS) în standardul IEEE 802.16d creează o vulnerabilitate semnificativă la atacurile Man-in-the-Middle (MITM), deoarece atacatorul poate acționa ca un BS. Astfel, după cum este ilustrat în Figura 5, o stație de bază (BS) falsă se poate plasa între SS și o stație de bază (BS) reală și poate forța SS să se autentifice prin transferul unei chei de autentificare AK, care poate fi falsificată de atacator. Atacatorul poate genera apoi propriul mesaj de autorizare, iar SS nu poate determina dacă acest mesaj provine de la o stație de bază de încredere, ceea ce permite atacatorului să câștige controlul asupra SS.

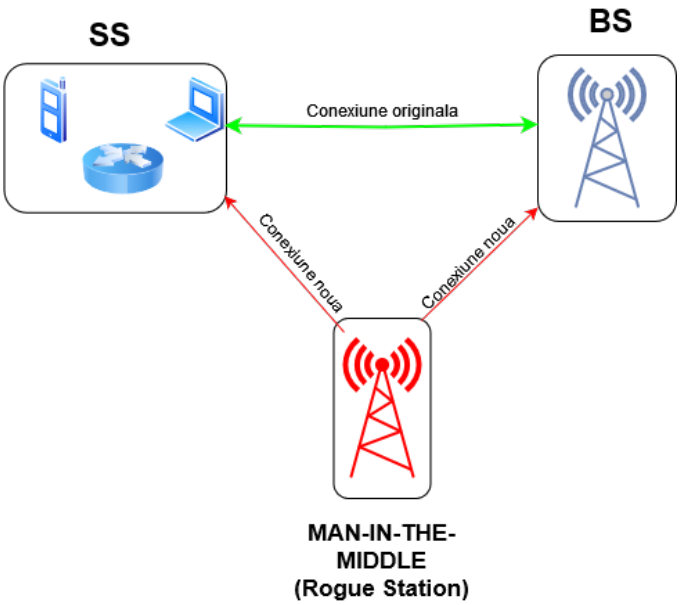


Figura 5. Atac de tip man-in-the-middle în rețelele WiMAX

O soluție eficientă pentru combaterea atacurilor de tip MITM este autentificarea reciprocă. Lipsa autentificării reciproce în tehnologia WiMAX a fost abordată în IEEE 802.16e prin introducerea PKMv2. Această versiune mai nouă a protocolului permite autentificarea reciprocă între cele două stații de comunicare, permițându-le să își verifice reciproc identitatea. În esență,

PKMv2 oferă un mecanism de securitate mai robust, asigurându-se că atât stația de bază, cât și clientul SS se pot autentifica reciproc, prevenind astfel accesul neautorizat sau manipularea datelor. Această îmbunătățire a protocolului de securitate asigură că sistemul WiMAX este mai sigur și mai puțin vulnerabil la atacuri în comparație cu versiunea anterioară a standardului.

## 5.3 Atacuri asupra stratului fizic

În cadrul standardul IEEE 802.16, mecanismele de securitate sunt definite la niveluri superioare față de stratul fizic, prin urmare stratul fizic poate fi vulnerabil la atacuri de tip „jamming", „scrambling" si „water torture".

Bruiajul (jamming) reprezintă un tip de atac care se încadrează în categoria atacurilor Denial-of-Service (DoS). Acest atac implică difuzarea de semnale radio pe canalul fizic în vederea blocării oricărei comunicații în raza sa de transmisie. Practic, scopul bruiajului este de a întrerupe comunicarea dintre emițător și receptor, făcându-le dificil sau imposibil să schimbe informații. Impactul bruiajului poate fi grav, deoarece poate cauza întreruperi semnificative în rețelele WiMAX, ducând la nefuncționarea rețelei și la pierderea datelor [12].

„Scrambling" este un tip de bruiaj realizat intenționat de către atactor care vizează anumite cadre sau părți ale cadrelor la stratul fizic, dar numai pentru intervale scurte de timp. Spre deosebire de alte tipuri de atacuri de bruiaj, „scrambling" este un proces selectiv, în care atacatorul poate alege să amestece informațiile de control pentru a perturba funcționarea normală a rețelei [13]. În esență, scopul atacului „scrambling" este de a provoca întreruperi direcționate în funcționarea rețelei, îngreunând accesul sau schimbul de date pentru utilizatorii legitimi. Deși impactul „scrambling" poate să nu fie la fel de sever ca alte tipuri de atacuri de bruiaj, poate duce totuși la întreruperi semnificative în operațiunile de rețea și poate compromite securitatea WiMAX.

„Water Torture" este un alt tip de atac asupra stratului fizic care implică trimiterea de cadre inutile cu intenția de a epuiza bateria SS sau de a-i epuiza resursele. Stația de abonat SS este de obicei un dispozitiv portabil cu resurse limitate, astfel acest tip de atac poate avea un impact mare asupra securității rețelei.

Pentru a combate atacurile asupra stratului fizic, o soluție ar fi utilizarea unui dispozitiv radio care poate detecta amenințarea, dar nu o poate preveni. În schimb, dispozitivul oferă o alertă administratorului, notificându-l cu privire la potențiala amenințare, astfel încât să poată fi luate măsuri imediate. De asemenea, o alta măsură posibilă ar fi implementarea tehnicii "frequency hopping". Tehnica Frequency-Hopping implică transmiterea de semnale radio prin schimbarea rapidă a frecvenței purtătoare pe o gamă largă de frecvențe care ocupă o bandă spectrală mare, pentru a împiedica atacatorii să blocheze sau să intercepteze semnalul [14].

# 6. Concluzii finale

În această lucrare, s-a analizat securitatea în rețelele WiMAX, punând accentul asupra măsurilor de securitate existente și a problemelor de securitate asociate acestei tehnologii.

S-a constatat că WiMAX dispune de o arhitectură de securitate bine definită, care include elemente cum ar fi autentificarea și autorizarea, precum și criptarea datelor pentru a proteja integritatea și confidențialitatea informațiilor. Cu toate acestea, există anumite vulnerabilități și amenințări, cum ar fi atacurile de tip DoS, atacurile de tip man-in-the-middle și diferite atacuri asupra stratului fizic, care pot compromite securitatea rețelei. Pentru a preveni și a contracara aceste amenințări, este important ca operatorii și utilizatorii rețelelor WiMAX să implementeze măsuri suplimentare de securitate, cum ar fi monitorizarea constantă a rețelei, utilizarea unor algoritmi criptografici robuști și implementarea unor politici stricte de autentificare și autorizare. Mai multe dintre aceste probleme de securitate au fost rezolvate odată cu adoptarea modificărilor recente și a soluțiilor de securitate din standardele IEEE 802.16 mai noi, dar unele dintre ele încă există și trebuie analizate cu atenție.

Tehnologia WiMAX este încă în proces de dezvoltare și necesită cercetare suplimentară în ceea ce privește vulnerabilitățile sale de securitate. În viitorul apropiat, pe măsură ce tehnologia WiMAX avansează și devine mai stabilă, există o perspectivă favorabilă ca această tehnologie de comunicare wireless să fie una de succes. Cu implementarea corespunzătoare a măsurilor de securitate și prin continuarea cercetării în acest domeniu, WiMAX poate oferi o opțiune viabilă și sigură pentru utilizatorii săi.

# 7. Referințe:

[1] https://ro.wikipedia.org/wiki/WiMAX

[2] K. Scarfone, C. Tibbs, M. Sexton, *Guide to Securing WiMax Wireless Communications*

[3] S. Y. Tang, P. Muller, H. R. Sharif *WiMAX Security and Quality of Service An End-to-End Perspective-Wiley (2010)*

[4] J. G. Andrews, A. Ghosh, R. Muhamed, *Fundamentals of WiMAX (2007)*

[5] S. P. Ahuja, N. Collier, *An Assessment of WiMax Security*

[6] *https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/*

[7] A. H. Raheem, *Performane study of WiMAX network security*

[8] M. McDowell, *Understanding Denial of Service Attacks (2007)*

[9] A. Sarik, B. Rahnama, *Adressing security challenges in WiMax environment*

[10] K. Youngwook, L. Hyoung-Kyu, B. Saewoong, *Shared Authentication Information for Preventing DdoS Attacks in Mobile WiMax Networks*, (2008)

[11] J. Kempf, *Wireless Internet Security Architecture and Protocols (2008)*

[12] A. T. Giang, H. T. Tran, H. T. Le, N. Q. Doan, M. H. Nguyen, *Jamming Attack in Vehicular Networks*

[13] R. Poisel, *Modern communications jamming principles and techinques (2003)*

[14] J. Jung, J. Jeung, J. Lim, *Control channel hopping for avoidance of scrambling attacks in IEEE 802.16 systems 2011.*