Journal of New Results in Engineering and Natural Science, No:8 (2018) 63-74
http://jrens.gop.edu.tr

Received: November 16, 2017
Accepted:January 09, 2018

Akıllı Şebekelerde Güvenli Haberleşme Tabanlı Güç Akışı Analizi

Metin VARAN[1*], Sajia Haidary[2], İsmail ÖYLEK[3] ve Özkan CANAY[4]

[1]Elektrik-Elektronik Mühendisliği Bölümü / Teknoloji Fakültesi, Sakarya Üniversitesi, Türkiye
[2]Bilgisayar ve Bilişim Mühendisliği Bölümü / Fen Bilimleri Enstitüsü, Sakarya Üniversitesi, Türkiye
[3]Bilgisayar Teknolojileri Bölümü / Sakarya Meslek Yüksekokulu, Sakarya Üniversitesi, Türkiye
[4]Bilgisayar Teknolojileri Bölümü / Adapazarı Meslek Yüksekokulu, Sakarya Üniversitesi, Türkiye

Abstract

The coordination of the power system management with the phasor measurement devices (PMUs) in real time on the load side and the production side is carried out within the context of smartgrid studies. Smartgrid evolves power systems into equipped with information systems at the same time opens grid to external threats. The fact that the network is resistant to these threats, which are described as cyber attacks, has a strategic precaution. Within the smartgrid studies, the cyber attack openness concept has a very important working area. In this study, a secure communication based power flow management system has been developed. The instantaneous parameter shares of the electrical units connected to the PMU bus are made securely by using RSA encryption method in accordiance with topological priorities of IEEE model. It has been shown that the power flow analyzes for the power systems studied show that the bus voltage and power values are within the stability limits. It has been demonstrated that RSA data encryption method has been applied successfully.

Keywords: *Smart grid, secure communication, power flow analysis, Java.*

Özet

Güç sistemi yönetiminin fazör ölçüm cihazları (PMU) ile gerçek zamanlı olarak yük ve üretim tarafında koordineli ve güvenilir olarak yapılması günümüzde akıllı şebeke çalışmaları kapsamında incelenmektedir. Akıllı şebeke çalışmaları kapsamında, bilgi sistemleri ile modernize edilen güç sistemleri dış tehditlere açık hale gelmektedir. Şebekenin siber saldırı olarak nitelenen bu tehditlere karşı dirençli olması stratejik öneme sahiptir. Akıllı şebeke çalışmaları içerisinde siber saldırılara açıklık konusu oldukça önemli bir çalışma alanına sahiptir. Bu çalışmada akıllı şebeke mimarisine uygun ve güvenli haberleşme tabanlı bir güç akışı yönetim sistemi geliştirilmiştir. Baraya bağlı olan elektriksel birimlerin anlık parametre paylaşımları PMU cihazları üzerinden seçilen ağ topolojisine ve IEEE modeli parametre değerlerine uygun olarak RSA şifreli olarak yapılmıştır. İncelenen güç sistemleri için yapılan güç akışı analizlerinin bara gerilimi ve güç değerlerinin kararlılık sınırlarının içinde kaldığı gösterilmiştir. Aynı şekilde belirlenen ağ topolojisine uygun, RSA veri şifrelemeli paket alışverişlerinin tüm modeller için başarılı olarak uygulandığı ortaya koyulmuştur.

Anahtar Kelimeler: *Akıllı şebekeler, güvenli haberleşme, güç akışı analizi, Java.*

1. Giriş

Günümüzde güç sistemleri çalışma limitleri sınırlarında çalıştırılmaktadır. Şebekelere bağlanan, değişken karakteristik gösteren, lineer olmayan yükler ve bunu karşılamaya çalışan değişken karakteristik gösteren üretim santralleri arasında kararlılık limitleri dâhilinde üretim ve tüketim dengesi gözetilerek bir işletme yapılması oldukça zor bir mühendislik problemidir. Bu durum elektrik güç sistemlerinin analizini her geçen gün daha da zorlaştırmaktadır. Elektrik güç sistem planlaması yapılırken sürekli yük akışı analizlerinin yapılması sistemin kararlı, güvenilir ve

[*] *Corresponding Author,* e- mail: mvaran@sakarya.edu.tr

ekonomik olarak işletilmesinde önemli bir fonksiyona sahiptir. Güç sistemi yönetiminin gerçek zamanlı olarak yük ve üretim tarafında koordineli ve güvenilir olarak yapılması günümüzde akıllı şebeke çalışmaları kapsamında incelenmektedir. Akıllı şebeke çalışmaları kapsamında, bilgi sistemleri ile modernize edilen güç sistemleri dış tehditlere açık hale gelmektedir. Şebekenin siber saldırı olarak nitelenen bu tehditlere karşı dirençli olması stratejik öneme sahiptir. Akıllı şebeke çalışmaları içerisinde siber saldırılara açıklık konusu oldukça önemli bir çalışma alanına sahiptir. Bu çalışmada akıllı şebeke mimarisine uygun ve güvenli haberleşme tabanlı bir güç akışı yönetim sistemi geliştirilmiştir.

Tasarlanan güç akışı yönetim sistemi Java tabanlı olarak geliştirilmiş olup güç akışları Newton-Raphson, Gauss-Seidel ve Fast Decoupled gibi farklı sayısal yöntemler kullanılarak gerçekleştirilmiştir. Tasarlanan güç akışı yönetim sisteminin çalışma başarımı, IEEE-9 Bara, IEEE-14 Bara ve IEEE-30 bara modelleri üzerinden RSA şifreleme yöntemi uygulanarak ortaya koyulmuştur. Bu çalışmada baraya bağlı olan elektriksel birimlerin anlık parametre paylaşımları, seçilen ağ topolojisine ve IEEE modeli parametre değerlerine uygun olarak RSA şifreli olarak yapılmıştır.

Güvenli haberleşme güç akışı yönetim sisteminde analizleri yapılan IEEE güç sistemleri modelleri için sistemin çalışma başarımı, kararlılık limitleri dâhilinde yapılan güç akışı sonuçları ve RSA haberleşme paket alışverişinin oluşturulan haberleşme paketlerini eksiksiz bir şekilde gerçekleştirilmiş olması ile ölçeklenmiştir. İncelenen güç sistemleri için yapılan güç akışı analizlerinin bara gerilimi ve güç değeri kararlılık marjinlerinde olduğu gösterilmiştir. Aynı şekilde belirlenen ağ topolojisine uygun, RSA veri şifrelemeli paket alışverişlerinin tüm modeller için başarılı olarak uygulandığı ortaya koyulmuştur.

2. Materyal ve Metot

Elektrik güç sisteminin güç ve yük akışlarının analiz edilmesinde birbirine bağlı çok sayıda baraya bağlı lineer ve lineer olmayan çok sayıda yük ve üretim elemanı olduğu için bilgisayar yazılımları sıklıkla kullanılır. Güç sistemlerinin bilgisayar destekli analizleri sayısal yöntemlerin kullanılmasını elzem kılmakta olup bu yük akışı yöntemleri arasında Newton-Raphson, Gauss-Seidel ve Fast Decoupled yöntemleri sıklıkla kullanılmaktadır[1]. Güç akışının hesaplanarak baralardaki gerilim ve açıların güç akışları ile ilişkilendirmeleri yapılması güç sisteminin maksimum yüklenme noktalarının tespit edilmesini kolaylaştırır. PV eğrileri de oluşturularak güç sistemleri planlama ve analizlerini daha kolay yapılmasını sağlanır [2, 3].

2.1. Güç Akışı Denklemlerinin Oluşturulması

Bir baraya giren net kompleks gücü $S_k=S_{gk}-S_{dk}$ olarak tanımlayabiliriz. Burada şebeke gerilimi, admitansı gibi tüm büyüklük değerleri per-unit cinsinden olup tüm hesaplamalarda tek faz güç ilişkisi kuruludur [4,5,6]. Bilinen ilişkileri kompleks güç için yazacak olursak S_k ifadesi:

$$S_k=V_kI_k^* \tag{1}$$

$$\begin{bmatrix} I_1 \\ . \\ . \\ I_n \end{bmatrix} = \begin{bmatrix} Y_{11} & Y_{12} & Y_{13} & Y_{14} \\ . & . & . & . \\ . & . & . & . \\ Y_{n1} & Y_{n2} & Y_{n3} & Y_{n4} \end{bmatrix} \begin{bmatrix} V_1 \\ . \\ . \\ V_n \end{bmatrix} \tag{2}$$

N baralı bir sistemi ifade eden (2) nolu matriste herhangi bir baraya giren akımın ifadesi

$$I_k = \sum_{j=1}^{N} Y_{kj} V_j \tag{3}$$

şeklinde ifade edilir burada Y_{kj} terimi admitans matrisinin elemanlarını temsil etmekte olup (3) denklemi (1) de yerine yazılırsa:

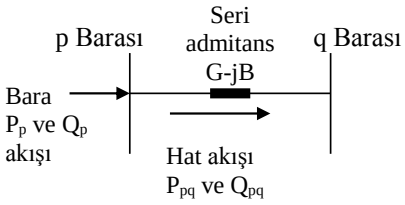
$$S_k = V_k \left(\sum_{j=1}^{N} Y_{kj} V_j \right)^* = V_k \sum_{j=1}^{N} Y_{kj}^* V_j^* \tag{4}$$

V_k'nın genlik ve açı değerine sahip bir büyüklük olduğunu hatırlayarak $V_k=|V_k|\angle\theta_k$. Ayrıca Y_{kj}, bir admitans foksiyonu olup kompleks bir değerdedir. G_{kj} ve B_{kj} elemanları bu admitans fonksiyonunun reel ve kompleks kısımları $Y_{kj}=G_{kj}+jB_{kj}$ şeklinde yazılabilir. Dolayısıyla (4) olan denklem tekrar düzenlenerek ve Euler formu hatırlanacak olursa bir fazör büyüklük $V=|V|\angle\theta=|V|\{\cos\theta+j\sin\theta\}$ gibi sinusoidlerin kompleks fonksiyonu olarak tanımlanarak denklem şu şekilde yazılabilir;

$$S_k = \sum_{j=1}^{N} \left(|V_k||V_j|\angle(\theta_k - \theta_j) \right)(G_{kj} - jB_{kj}) = \sum_{j=1}^{N} |V_k||V_j| \left(\cos(\theta_k - \theta_j) + j\sin(\theta_k - \theta_j) \right)(G_{kj} - jB_{kj}) \tag{5}$$

Bu denklemde parantez içindeki iki terimin cebirsel çarpımı yapılarak reel ve imajiner kısımlar ve $S_k=P_k+jQ_k$, ifadesi hatırlanırsa (5) denklemini aşağıdaki gibi P_k ve Q_k olarak ifade edebiliriz;

$$\begin{aligned} P_k &= \sum_{j=1}^{N} |V_k||V_j| \left(G_{kj}\cos(\theta_k - \theta_j) + B_{kj}\sin(\theta_k - \theta_j) \right) \\ Q_k &= \sum_{j=1}^{N} |V_k||V_j| \left(G_{kj}\sin(\theta_k - \theta_j) - B_{kj}\cos(\theta_k - \theta_j) \right) \end{aligned} \tag{6}$$



Şekil 1. p Barasının sadece q barasına bağlı olduğu durum

(6) denkleminde *k* barası *p* barası olarak isimlendirilirse ve bu baranın sadece bir *q* barasına bağlı olduğu düşünülürse, *p* barası güç akışı *pq* hattı boyunca yapılan akış gibi olup bu durum Şekil 1'de gösterilmiştir. Şekil 1'de gösterilen durum dolayısıyla (6) denklemi şu şekilde yazılabilir:

$$\begin{aligned} P_p &= |V_p|^2 G_{pp} + |V_p||V_q|G_{pq}\cos(\theta_p - \theta_q) + |V_p||V_q|B_{pq}\sin(\theta_p - \theta_q) \\ Q_p &= -|V_p|^2 B_{pp} + |V_p||V_q|G_{pq}\sin(\theta_p - \theta_q) - |V_p||V_q|B_{pq}\cos(\theta_p - \theta_q) \end{aligned} \tag{7}$$

Eğer hattın *pq* admitans değeri Şekil 1'de gösterildiği gibi $y=G-jB$ olursa bu durumda $G_{pq}=-G$ ve $B_{pq}=B$ yazılabilir. Burada p barasına hattı şarj eden şönt bir reaktans olmadığından $G_{pp}=G$ *ve* $B_{pp}=B$ yazılabilir. Bu şartlar (7) denklemi şu şekilde yazılabilir:

$$\begin{aligned} P_p &= |V_p|^2 G - |V_p||V_q|G\cos(\theta_p-\theta_q) + |V_p||V_q|B\sin(\theta_p-\theta_q) \\ Q_p &= |V_p|^2 B - |V_p||V_q|B\cos(\theta_p-\theta_q) - |V_p||V_q|G\sin(\theta_p-\theta_q) \end{aligned} \tag{8}$$

ifadesi yazılabilir.

2.2. Güç Akışı Probleminin Sayısal Yöntemlerle Çözümü

N baralı bir şebekenin olduğu baz alınarak, N_G üretim barası sayısını ifade etmekte olup sistemde bir adet salınım barası da seçilmek üzere N_G*-1* adet *PV* barası (üretim) ve ve N-N_G adet *PQ* barası (tüketim) vardır [7]. Salınım barasının 1 nolu bara olduğu kabul edilerek *PV* baraları 2, 3, şeklinde *NG* ye kadar *PQ* baralarının da N_G*+1* den başlamak üzere *N*'e kadar olduğu sistem aşağıdaki adımlar gözetilerek tanımlanır:

1. Tüm seri ve şönt elemanların admitans değerleri *Y-bara* matrisi olmak üzere,
2. Tüm üretim barası gerilim büyüklüklerinin *Vk, k=1,...,NG*, olmak üzere,
3. Salınım barası dışındaki tüm baralara olan aktif güç akışı *Pk, k=2,...,N* olmak üzere,
4. Tüm *PQ* baraları için reaktif güç akışı *Qk, k=NG+1, ...,N* olmak üzere,

3 ve 4 adımları doğrudan (6) nolu güç akışı denklemlerinin sol tarafındaki güç değerlerini temsil etmektedir. Denklem sayısı denklemde yer alan bilinmeyen sayısından bir tane az olduğu sol tarafın varlığı oldukça önemlidir. Bu denklemlerin sol tarafına eşitlenecek olan denklemlerin sayısı adım 3'de yer alan aktif güç akışının olduğu baralara adım 4'de yer alan reaktif güç akışının olduğu baraların eklenmesiyle *(N-1)* + *(N-*N_G*)* = *2N-*N_G*-1* şeklinde elde edilir. Güç akışı denklemlerini burada uygun rakamları sağdan vererek tekrar oluşturursak;

$$\begin{aligned} P_k &= \sum_{j=1}^{N} |V_k||V_j|\left(G_{kj}\cos(\theta_k-\theta_j) + B_{kj}\sin(\theta_k-\theta_j)\right), \\ k &= 2,...,N \\ Q_k &= \sum_{j=1}^{N} |V_k||V_j|\left(G_{kj}\sin(\theta_k-\theta_j) - B_{kj}\cos(\theta_k-\theta_j)\right), \\ k &= N_G+1,...,N \end{aligned} \tag{9}$$

Şebeke ile ilgili şu bilgileri bulmaya çalışırsak;

a. Salınım barası hariç tüm baralardaki gerilim fazör açıları (salınım barası açısı *0°*) θ_k, *k=2,...,N* olmak üzere,
b. Tüm *PQ* baraları için gerilim fazörlerinin genlik değerleri $|V_k|$, $k=N_G+1, ..., N$ olmak üzere,

olmak üzere toplamda *(N-1)* + *(N-NG)* = *2N-NG-1* adetlik bir bilinmeyeni temsil eder [8]. Dolayısıyla sol taraftaki *2N-NG-1* adet bilinen denklem sayısı, bilinmeyen *2N-NG-1* adet gerilim ve açı sayısı ile eşit olup denklem çözülebilir durumdadır. Ancak (9) nolu denklemden de görüleceği üzere çarpan halde bulunan bilinmeyen elemanların varlığından dolayı bu denklemler lineer değildir. Bu lineer olmama durumundan dolayı bu denklemleri "*Ax=b*" formunda matris

formunda yazamayıp denklemleri diğer çözüm yöntemlerinin formuna uygun hale getirmek gerekmektedir.

Bilinmeyen değerler vektörü iki adımda tanımlanır. Bilinmeyen açılar vektörü $\underline{\theta}$ (alt çizgi değişkenin bir vektör veya matris olduğunun temsil eder) ve bilinmeyen gerilim genlikleri $|\underline{V}|$olmak üzere,

$$\underline{\theta} = \begin{bmatrix} \theta_2 \\ \theta_3 \\ \text{M} \\ \theta_N \end{bmatrix}, \qquad |\underline{V}| = \begin{bmatrix} |V_{N_G+1}| \\ |V_{N_G+2}| \\ \text{M} \\ |V_N| \end{bmatrix} \tag{10}$$

ikinci olarak bilinmeyen açıları ve gerilim genlikleri vektörleri birleştirilerek;

$$\underline{\text{x}} = \begin{bmatrix} \underline{\theta} \\ |\underline{V}| \end{bmatrix} = \begin{bmatrix} \theta_2 \\ \theta_3 \\ \text{M} \\ \theta_N \\ |V_{N_G+1}| \\ |V_{N_G+2}| \\ \text{M} \\ |V_N| \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ \text{M} \\ x_{N-1} \\ x_N \\ x_{N+1} \\ \text{M} \\ x_{2N-N_G-1} \end{bmatrix} \tag{11}$$

şeklinde yazılabilir. (9) denklemi tekrar düzenlenirse

$$\begin{aligned} P_k &= P_k(\underline{x}), \qquad k = 2,...,N \\ Q_k &= Q_k(\underline{x}), \qquad k = N_G + 1,...,N \end{aligned} \tag{12}$$

Burada P_k ve Q_k incelenen akışlar olup (bilinen sabitler), sağ taraf elemanlar bilinmeyen $\underline{x}$ vektörünün içindeki fonksiyonlardır. Sol taraf sağ tarafa atılırsa

$$\begin{aligned} P_k(\underline{x}) - P_k &= 0, \qquad k = 2,...,N \\ Q_k(\underline{x}) - Q_k &= 0, \qquad k = N_G + 1,...,N \end{aligned} \tag{13}$$

Nihai olarak $\underline{f(x)}$ değer fonksiyonu vektörü aşağıdaki gibi tanımlanmış olur:

$$\underline{f}(\underline{x}) = \begin{bmatrix} f_1(\underline{x}) \\ \text{M} \\ f_{N-1}(\underline{x}) \\ \text{--------} \\ f_N(\underline{x}) \\ \text{M} \\ f_{2N-N_G-1}(\underline{x}) \end{bmatrix} = \begin{bmatrix} P_2(\underline{x}) - P_2 \\ \text{M} \\ P_N(\underline{x}) - P_N \\ \text{-------} \\ Q_{N_G+1}(\underline{x}) - Q_{N_G+1} \\ \text{M} \\ Q_N(\underline{x}) - Q_N \end{bmatrix} = \begin{bmatrix} \Delta P_2 \\ \text{M} \\ \Delta P_N \\ \text{-------} \\ \Delta Q_{N_G+1} \\ \text{M} \\ \Delta Q_N \end{bmatrix} = \begin{bmatrix} 0 \\ \text{M} \\ 0 \\ \text{-------} \\ 0 \\ \text{M} \\ 0 \end{bmatrix} = \underline{0} \tag{14}$$

(14) nolu denklem *f(x)=0* formunda olup, burada *f(x)* is a değer fonksiyon vektörü ve 0 sıfırlar vektörüdür. Her iki vektörün de boyutu *(2N-NG-1)×1* bilinmeyenler *x* vektörü boyutuna eşittir. *ΔPk* ve *ΔQk* vektörleri denklemde uyumsuzluk vektörü olarak tanımlanmıştır. Bu vektörler çözüm algoritması boyunca tüm iterasyonlar için en uygun çözümün elde edilmesinde kullanılacaktır [14].

2.3. Fazör Ölçüm Birimi (PMU) ve Yapısı

Fazör ölçüm birimi güç sistemlerinde ani gerilim akım fazörlerini gerçek zamanlı ve zaman etiketli olarak yüksek hassasiyette ölçmek için geliştirilmiş cihazlardır[15]. GPS tarafından zaman senkronizasyonu yapılmış yüksek örnekleme hızına sahip fazör ölçümü ile oldukça karmaşık, değişken ve lineer olmayan güç sistem dinamiklerinin ortaya çıkarılması ve sistem kararlılığının en zor koşullarda bile sürdürülmesi ve kesintisiz güç dağıtımını mümkün hale gelebilecektir. Günümüzde GPS sinyali ile dünyanın herhangi bir yerinden 1 mikro saniye hassasiyetle zaman damgası alınabilmektedir.

Güç sisteminde güvenilirliği ve kararlılığı arttırmanın en önemli koşulunun sistemin sürekli ve doğru bir şekilde ölçülmesi olduğu ifade edilebilir. Kirchhoff akım ve gerilim yasası eşliğinde, elektriksel büyüklüklerin fazör olduğu ve elektrik sinyalinin ışık hızında ilerlediği kabul edilerek sistemin anlık gerilim ve akım değerinin doğru zamanlanmış bir zamanlayıcı ile alınmış tüm gerilim ve akım değerleri fazör ölçümlerinin birleştirilmesi ile mümkün olduğu söylenebilir. Güç sisteminin her noktasından fazör ölçümü almak yerine özellikle yüksek dinamiklerin görüldüğü, anlık değişimin en yoğun olduğu baralardan ölçüm alınması fazör ölçüm sistemin ekonomik, sürdürülebilir ve kullanılabilir olmasına katkı sunacaktır. Şekil 2'de PMU birimine ait veri paketinin yapısı gösterilmiştir.

SYNC	FRAME SIZE	ID	SOC	FRACSEC	CMD	PHASORS	DATARATE	CRC
2 BYTE	2 BYTE	2 BYTE	4 BYTE	4 BYTE	2 BYTE	[0-65518] BYTE	2 BYTE	2 BYTE
SYNC : Paket türü ve versiyon numarası içerir.								
FRAMESIZE : Pakette bulunan byte sayısını tutar.								
ID : PMU/DC ID numarasını tutar.								
SOC : Zaman Damgası bilgisini tutar.								
FRACSEC: Saniye küsürat bilgisini tutar								
CMD: PMU ların haberleşmesi için tanımlı olan kod kümesini tutar.								
PHASORS: Genişletilmiş veri paketi yapılan Gerilim, Akım, Faz Açısı, Frekans bilgisini içerir.								
DATARATE: Fazör ölçüm frekans bilgisini tutar.								
CRC: 16 bit CRC kontrol paketidir.								

Şekil 2. PMU veri paketi tanımlanması

Veri paketi yapısı bir PMU tarafından toplanması gereken f (frekans), m_V (gerilim genliği), δ_V (gerilim faz_açısı), m_I (akım genliği) ve δ_I (akım_faz_açısı) başta olmak üzere, cihazın kimlik bilgisi, içerdiği verinin boyutu, IEEE C37.118 PMU birimi haberleşme protokol standartları içerinde yer alan GPS zaman damgası ,saniye küsuratı, veri paket türü ve paketin gönderileceği komutlar başta olmak üzere veri bütünlüğün kontrolcüsü 16 bit CRC'den oluşmaktadır.

2.4. RSA Şifreleme Yöntemi

RSA şifreleme algoritması, 1987 yılında Ronald Rivist, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir. Bu sistem hem gizlilik hem de dijital imza sağlamak amaçlı kullanılmaktadır. RSA sistemin güvenliği tamsayılarda çarpanlara ayırma probleminin kolaylıkla olmaması temeline dayanır[9]. RSA sisteminde şifreli mesaj gönderebilmesi için kişilerin açık anahtarlarına ihtiyaç vardır. Mesajı alan kişide mesajı okuması için gizli bir anahtar olması gerekir.

Anahtar oluşturma algoritması:

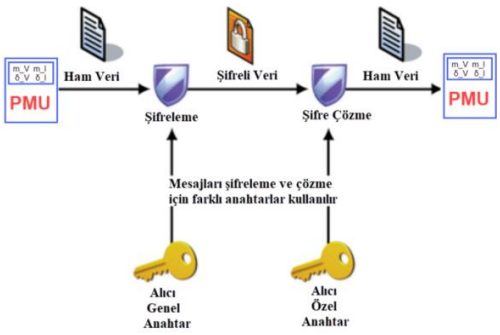
- İki adet farklı, rastgele ve yaklaşık aynı uzunlukta olan p ve q asal sayıları seçilir.
- *n = pq* ve *(phi) φ = (p-1)(q-1)* değerleri hesaplanır.
- e, *1 < e < phi* ve *gcd(e, phi) = 1* olacak şeklinde bir tamsayı seçilir.
- *d* sayısı öklid algoritmasını kullanarak *1 < d < phi ed ≡ 1 (mod phi)* koşulu sağlanarak hesaplanır.
- A'nın açık anahtarı *(n,e)*, gizli anahtarı ise *d* olur.

Şifre Oluşturma Algoritması:

- A'nın açık anahtarını *(n,e)* alır
- *m* mesajını *1 < m < n* aralığında yazar.
- $c = m^e \bmod n$'i hesaplar.
- Oluşan *c* şifresini *A*'ya gönderir.

Şifre Çözme Algoritması:

- *(n, d)* gizli anahtarını kullanarak ve $m = c^d \bmod n$ hesaplar.
- *m* açık metni ulaşır.



Şekil 3. PMU verilerinin RSA veri şifreleme mekanizması

Şekil 3'de PMU verilerinin RSA veri şifreleme mekanizması verilmiştir. RSA, şifreleme ve şifre çözme amacı için iki farklı anahtar kullandığı için asimetrik anahtar güvenlik protokolüdür. En popüler ve kanıtlanmış asimetrik anahtar şifreleme algoritması olan RSA şifrelemede iki anahtarlı özel anahtar ve genel anahtar üretilir[10]. Asimetrik anahtarlar, simetrik şifrelemede anahtar dağılım problemini çözmektedir. Ayrıca, yalnızca anahtarı olan göndericinin mesaj göndermiş olabileceğini ortaya çıkarmak amaçlı *"reddedilemezlik"* durumlarının ortaya çıkarılmasında kullanılır[11]. Özel anahtar kullanıcıya kapalı olup sadece genel anahtar kullanıcıyla iletişim kurmak isteyen taraf tarafından bilinir. Bu nedenle, açık anahtar şifrelemesi olarak da bilinir. Hem imzalama hem şifreleme için birlikte kullanılabilen ilk algoritma olup RSA açık anahtar şifrelemesindeki ilk algoritmalardan biridir. Günümüzde daha hızlı bir RSA şifrelemesi oluşturmak için iç bağlantı ağı kavramı temelli yeni algoritmalar geliştirilmektedir.

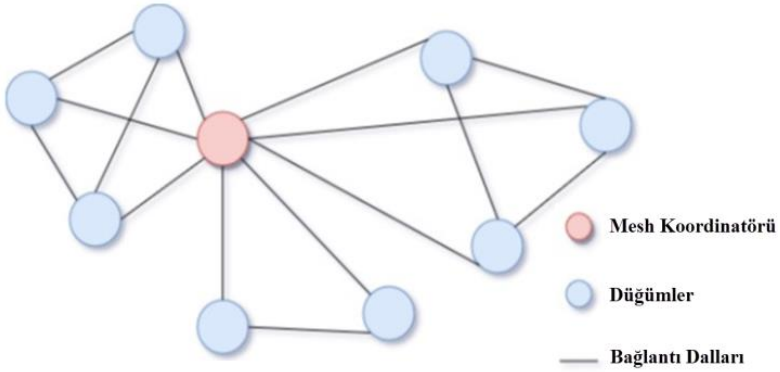
2.5. Mesh Ağ Topolojisi

Mesh ağ topolojisinde, tüm düğümler birbirine bağlıdır. Mesh ağı kendisini inşa etme ve yapılandırma kabiliyetine sahip bir ağ topolojisi olarak bilinir. Herhangi bir uç düğüme güç verildiğinde komşu düğümleri dinler ve bulur ve ağlara katılmak için bir istek gönderir ve ardından ağ güvenlik gereksinimlerini yerine getirdikten sonra düğümler topolojiye kabul edilir.

Otomatik olarak yol veya güzergâhlar son düğüm tarafından oluşturulur, çünkü gönderilen bilgi merkezi düğüme erişene kadar komşu düğümler tarafından yönlendirilir[12].
Mesh topolojisi, esnek yönlendirme, esnek trafik mühendisliği yönetimi, ağ operasyonlarının basitleştirilmesi gibi avantajlar sağlayabilen birçok uygulama alanlarına sahiptir. Topolojide bulunan çok sayıda bağlantılı yolu nedeniyle uygulamada güvenlik ve güvenilirlik sağlar. Topolojide *"n"* düğümlü ağın güvenlik sorumluluğunu güvence altına alan*"n-1"* olarak bilinen emniyet kriteri uygulanmaktadır[13].

$$bağlantı\_sayısı=n(n-1) \tag{15}$$

n-1 ölçütü bir hattın bağlantısının kopması durumunda sistemin normal çalışmaya devam etmesini garanti eder. Elektrik iletim ve dağıtım şebekelerinde güç akışı mimarisi genel olarak radyal ve mesh topolojisi üzerine kurgulanmıştır. Radyal bağlı şebekelerde kapalı döngü olmayıp, geriye dönüp dolaşmadığınız sürece, bir baradan başlayıp çıkış barasını bulma imkânı olmaksızın güç akışı söz konusudur. Bu tip şebekede baraya bağlı bir hat arıza görürse o hatta bağlı olan tüm yüklerin bara ile bağlantısı kopar. Dolayısı ile enerjisiz ve iletişimsiz kalır denilir. Diğer yandan mesh şebeke topolojisinde kapalı döngüler bulunup gücün birbirine bağlı olduğu çoklu baradan transferi söz konusudur. Mesh topolojisi güç sistemleri için en güvenilir, kararlı ve maliyetçe de en yüksek olan ağ yapısıdır[14]. Mesh koordinatörü ile tüm düğüm bilgilerinin koordine edildiği yapı Şekil 4'de gösterilmiştir.



Şekil 4. Mesh Ağ Topolojisi

3. Bulgular

3.1. Güvenli Haberleşme Tabanlı Güç Akışı Yönetim Sistemi

Güvenli haberleşme tabanlı güç akışı yönetim sistemi IEEE-9 Bara, IEEE-14 Bara ve IEEE-30 Bara modelleri için fazör ölçüm ünitelerinin en uygun sayıda ve en uygun barada tespitinin yapılmasıyla başlamaktadır. Bu kapsamda açık kaynak kodlu PSAT güç akışı analiz aracı kullanılmış olup IEEE-14 bara modeli için derinlik yöntemine göre en uygun PMU cihaz sayısı ve lokasyonları belirlenmiştir. Buna göre {1, 4, 6, 8, 10 ve 14} nolu baralara olmak üzere 6 PMU yerleştirilmesi yapılmıştır. Bu cihazlar ile 16 adet akım fazörü ölçümü yapılacağı belirlenmiştir. Ölçüm yapılan bu hatlar Tablo 1'de sırasıyla verilmiştir.

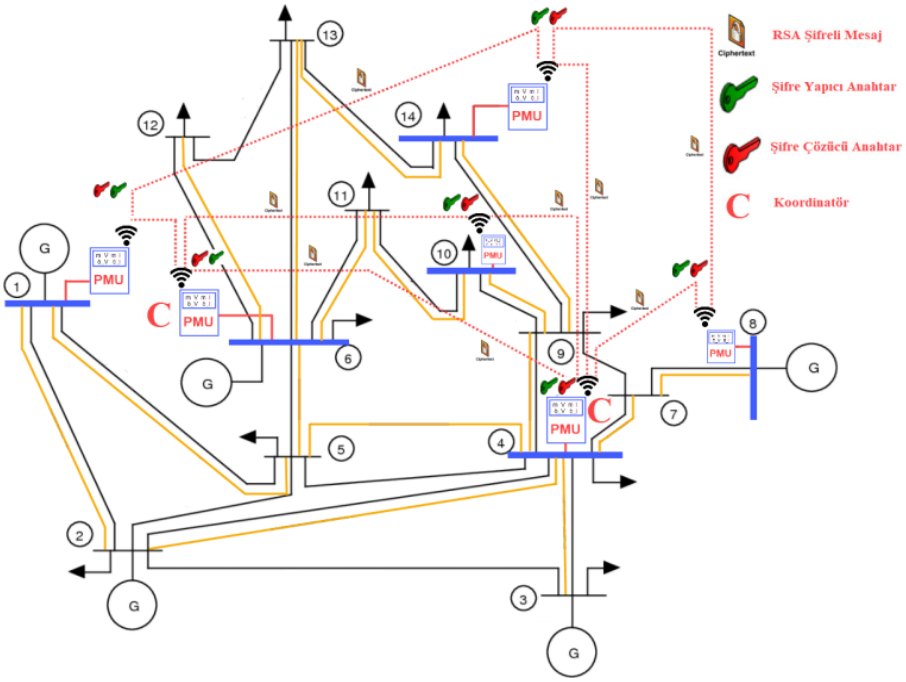
Tablo 1. IEEE-14 modeli derinlik yöntemi PMU ile ölçüm alınan dallar

1-2 Arası	4-5 Arası	6-11 Arası	9-10 Arası
1-5 Arası	4-7 Arası	6-12 Arası	9-14 Arası

2-4 Arası	4-9 Arası	6-13 Arası	10-11 Arası
3-4 Arası	5-6 Arası	7-8 Arası	13-14 Arası

IEEE-14 Bara modelinde 1, 2, 3, 6 ve 8 numaralı baralar üretim barası *(PV)* olup bu baralarda *P* ve *V*'nin sabit olduğu, geri kalan tüm baralar ise tüketim barası *(PQ)*'dur. Bu baralarda *P* ve *Q* değerlerinin sabit olduğu kabul edilir. *PV* barası gerilim kontrollerinin yapıldığı bara olup baraların gerilim açılarının referansları salınım barasına göre belirlenmiştir. PMU cihazlarının yerleştirildiği {1, 4, 6, 8, 10 ve 14} nolu baralarda mesh ağ topolojisine uygun bir iletişim yapısı oluşturulmuştur. PMU'ların derinlik metoduna göre en uygun yerleştirildiği IEEE-14 baralı güç sisteminde mesh ağ topolojisine uygun hiyerarşi üzerinden baralara paket alışverişi gerçekleştirilmiştir.

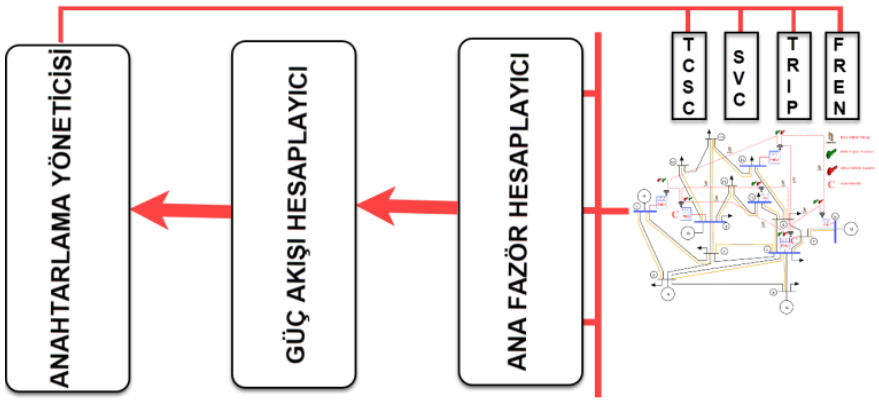
Şekil 5'de IEEE-14 bara modeli üzerine yerleştirilen PMU'ların RSA şifreli olarak haberleşme yapısı gösterilmiştir. Fazör ölçüm alma aşamasında IEEE modeli için belirlenen ağ topolojisi ile uyumlu bir veri koordinasyon hiyerarşisi oluşturulmuştur.



Şekil 5. Güç akışı yönetim sistemi master çalışma yapısı

Şekil 5'de gösterilen güvenli haberleşme tabanlı IEEE-14 bara sistemi için 4 ve 6 nolu PMU baralar mesh topolojisi koordinatörleri olarak belirlenmiştir. Bu koordinatörler iki ayrı mesh yapısıyla birbirine bağlı olan 14 baralı güç sisteminin birer saniye olarak belirlenen zaman dilimlerinde *f (frekans), m_V (gerilim genliği), δ_V (gerilim faz_açısı), m_I (akım genliği)* ve *δ_I (akım_faz_açısı)* koordinasyonunu RSA şifreli olarak sağlanmasından sorumludur.

Burada her iki PMU koordinatör yine RSA algoritmasına göre belirlenen zamanlarda ortak anahtar oluşturma görevlerini yerine getirmektedir. Koordinatör baralar, kendisine bağlı bulunan makinelerin ve kendisiyle doğrudan güç iletimi bağlantısı bulunan baralar ile belirlenen zaman aralıklarında haberleşme yaparak *f, m_V, δ_V, m_I* ve *δ_I* verilerini toplama görevini yürütmektedir. Koordinatör baralara doğrudan güç iletimi bağlantısı bulunan baralar mesh topolojisi hiyerarşisinde yardımcı koordinatör olarak belirlenmiştir. Yardımcı koordinatörler kendisine bağlı bulunan makinelerin ve kendisiyle doğrudan güç iletimi bağlantısı bulunan baralar ile belirlenen zaman aralıklarında haberleşme yaparak *f, m_V, δ_V, m_I* ve *δ_I* verilerini toplayarak koordinatör baraya ulaştırma görevini yürütmektedir.



Şekil 6. Güç akışı yönetim sistemi master çalışma yapısı

Şekil 6'da gösterildiği üzere mesh ağ topolojisiyle toplanan zaman damgalı PMU verileri koordinatör baralar üzerinden ana fazör hesaplayıcı sistemine aktarılarak alınan *f, m_V, δ_V, m_I* ve *δ_I* güç akışı denklemleri içerisinde değerlendirilip kararlı ve güvenilir güç akışı için iyileştirici müdahale adımları oluşturulmaktadır. Yapılan iyileştirici müdahaleler planlamasının kararlılık ve güvenilirlik fonksiyonlarını sağlayabilmesi en önemli ön koşuldur. Bu müdahaleler yine belirlenen hiyerarşide önce koordinatörlere ve buna bağlı baralara aktarılmaktadır.

PSAT ile elde edilen PMU baraları Java ile yapılan güç akışı yönetim sistemine "pmu_bara" integer dizi değişkeni olarak tanımlanmıştır. Mesh ağ topolojisi ile belirlenen hiyerarşide koordinatör PMU baralar üzerinden RSA tabanlı bir fazor bilgi paylaşımı yapılarak IEEE-14 bara sisteminin belirlenen bara durumları için çözülmüştür. Yapılan IEEE-14 güç akışı senaryosu dâhilinde 6 adet PMU verisi değerlendirilerek PMU'ların yerleşik halde bulunduğu 2, 3, 6 ve 8 nolu baralar için reaktif güç limiti aşımı tespiti yapılmıştır. Buna rağmen tüm baralara ait gerilimler, akım değerleri, aktif ve görünür güç değerleri kararlılık sınırları içerisinde olduğu tespit edilmiştir.

Tablo 2. IEEE 14 Modeli Güç Akışı Sonuç Tablosu

Baradan Baraya		Hat	Güç Akışı		Güç Kaybı	
			P(MW)	Q(MVAr)	P(MW)	Q(MVAr)
5	2	1	-56.0525	-5.1146	1.7855	1.885
12	6	2	-11.2444	-4.2536	0.1623	0.3378
13	12	3	-2.6814	-1.9928	0.02295	0.02076
13	6	4	-25.4783	-13.4402	0.51083	1.006
11	6	5	-11.6062	-12.313	0.25354	0.53095
10	11	6	-6.5985	-9.5407	0.10777	0.25227
10	9	7	-6.0015	1.4207	0.01181	0.03137
14	9	8	-11.8218	-0.13783	0.17875	0.38023
13	14	9	9.2597	7.3131	0.22147	0.45092
9	7	10	-37.8574	-20.5337	0	1.9888
2	1	11	-231.433	63.6317	10.2906	25.5696
2	3	12	104.965	1.4230	4.7473	15.3747
4	3	13	32.6082	-20.2551	0.9467	-1.0707
5	1	14	-104.378	9.3659	5.9276	19.2312
4	5	15	-83.8773	15.5363	0.97841	1.8053
4	2	16	-74.9649	1.0372	3.2848	6.063
6	5	17	-64.9356	2.0513	0	9.2911
9	4	18	-21.4565	-1.835	0	2.514
7	4	19	-37.8574	9.2255	0	2.9581

7	8	20	0	-31.748	0	1.6542

Yapılan şifrelemeler 512, 1024 ve 2048 bit olacak şekilde oluşturulmuştur.

Örnek PMU Verisi: *"SYNC/FRAME/SIZE/ID/SOC/FRAC/ CMD/PHASORS/RATE/CRC"*

Üstel Çarpan:

"13059886041861393582886368335225311834111233598880026366672340162513668429470342954665857293166407177014420715819444018813032824228302177158523544944138271"

Şifrelenmiş Veri:

"866547700396455916412560293671510903343124092214475031078016300592251152174395361871475471595389483383974239515886268292654114098527128541734961131228879324237480169587445256134180109200263356128980993458103109294935187852225929303350203502382427233913004984639743267887492160422706074087744224937710481944 6"

Şifreleme ve çözme süreleri i7-3770 K 3.5 GHz 8 çekirdek işlemci ve 16 GB RAM olan bir bilgisayar üzerinde kurulu Eclipse Java platformunda 512 bit için 1 sn, 1024 için 3 sn, 2048 bit için 24 sn'de başarılı olarak oluşturulmuştur.

Güvenli haberleşme güç akışı yönetim sisteminde analizleri yapılan IEEE güç sistemleri modelleri için sistemin çalışma başarımı, kararlılık limitleri dâhilinde yapılan güç akışı sonuçları ve RSA haberleşme paket alışverişinin oluşturulan haberleşme paketlerini eksiksiz bir şekilde gerçekleştirilmiş olması ile ölçeklenmiştir. İncelenen güç sistemleri için yapılan güç akışı analizlerinin bara gerilimi ve güç değeri kararlılık marjinlerinde olduğu gösterilmiştir. Aynı şekilde belirlenen ağ topolojisine uygun, RSA veri şifrelemeli paket alışverişlerinin tüm modeller için başarılı olarak uygulandığı ortaya koyulmuştur.

4. Tartışma

Güç sistemi yönetiminin gerçek zamanlı olarak yük ve üretim tarafında koordineli ve güvenilir olarak yapılması günümüzde akıllı şebeke çalışmalarının temel hedefidir. Akıllı şebekelerin bu fonksiyonu gerçek zamanlı ölçüm ve haberleşme yapabilen ve siber saldırılara karşı yeterli güvenlik algoritmaları ve donanımları barındıracak modern güç sistemleri bileşenleri ile yerine getirmesi mümkündür. Bu çalışmada geliştirilen güvenli haberleşme tabanlı bir güç akışı yönetim sistemi mikro bazda buna bir örnek olarak gösterilebilir.

Bu çalışmada tespit edilen baralar için reaktif güç akışı limitleri içerisinde tutmayı sağlayacak anahtarlama elamanı türü, kontrol yapısı ve reaktif güç enjeksiyonu yapılacak baraların tespit edilerek iyileştirici müdahale adımlarının detaylandırılması sonraki çalışmalar olarak planlanmıştır. Optimum güç akışı algoritmaları da kullanılarak birim üretim planlaması (unit commitment) problem için güvenli PMU tabanlı güç akış dinamikleri oluşturulabilir.

5. Sonuç

Bu çalışmada akıllı şebeke mimarisine uygun ve güvenli haberleşme tabanlı bir güç akışı yönetim sistemi geliştirilmiştir. Baraya bağlı olan elektriksel birimlerin anlık parametre paylaşımları PMU cihazları üzerinden seçilen ağ topolojisine ve IEEE modeli parametre değerlerine uygun olarak RSA şifreli olarak yapılmıştır. İncelenen güç sistemleri için yapılan güç akışı analizlerinin bara gerilimi ve güç değerlerinin kararlılık sınırlarının içinde kaldığı gösterilmiştir. Aynı şekilde

belirlenen ağ topolojisine uygun, RSA veri şifrelemeli paket alışverişlerinin tüm modeller için başarılı olarak uygulandığı ortaya koyulmuştur.

6. Referanslar

[1] Crow M (2002). *Computational Methods for Electric Power Systems* (2. basım), CRC Basım, USA.
[2] Tamura Y, Mori H, Iwamoto S (1983). Relationship between voltage instability and multiple load flow solutions in electric power systems. *IEEE Transactions on power apparatus and systems*, 5, 1115-1125.
[3] Pai MA, Chatterjee D (2014). *Computer Techniques in Power System Analysis*, McGraw-Hill Education, New Delhi.
[4] Vlach J, Singhal K (1983). *Computer Methods for Circuit Analysis and Design*, Springer Science & Business Media, Ontario, Canada.
[5] Elgerd O (1982). *Electric Energy Systems Theory*, McGraw-Hill, New York.
[6] Grainger J, Stevenson W (1994). *Power System Analysis*, McGraw-Hill, New York.
[7] Bergen A, Vittal V (2000). *Power Systems Analysis*, (2. Baskı), Prentice Hall, Upper Saddle River, New Jersey, USA.
[8] Gross C (1979). *Power System Analysis*, John Wiley & Sons, New York.
[9] Anshel M, Boklan KD (2007). Introduction to cryptography with coding theory. *The Mathematical Intelligencer*, 29(3), 66-69.
[10] Damrudi M, Aval KJ, Ithnin N (2015). A Parallel Method for RSA Cryptosystem Utilizing Topological Architecture. *Indian Journal of Science and Technology*, 8(30).
[11] Kaur S, Kaur H (2015). Implementing RSA Algorithm in MANET and Comparison with RSA Digital Signature. *International Journal For Advance Research In Engineering And Technology*, 3(V), 24–28.
[12] Portmann M, Amir AP (2007). *Wireless Mesh Networks for Public Safety and Disaster Recovery Communications*, Auerbach Publications, USA.
[13] Singh R, Dewra S (2015). Performance evaluation of star, tree & mesh optical network topologies using optimized Raman-EDFA Hybrid Optical Amplifier. *Trends in Automation, Communications and Computing Technology (I-TACT-15)*, 110-116, Bangalore, India.
[14] Ferreira dos Santos, T M (2013). Mesh Grid Structure vs. Radial Structure Performance and Perspectives of Evolution. Lisboa, Portugal.
[15] İpek, MAM (2008). Elektrik Güç Sistemlerinde Geniş Alan Ölçüm Sistemi ve Fazör Ölçüm Birimi Yerleşiminin İncelemesi, Yüksek Lisans Tezi, İTÜ Fen Bilimleri Enstitüsü, İstanbul, Türkiye.