ÖZET

BİRİNCİL KULLANICI EMÜLATÖRÜ/SİNYAL KARIŞTIRICI SALDIRISI TESPİT YÖNTEMİ

Buluş konusu yöntem, birincil kullanıcı emülatörü / sinyal karıştırıcı saldırısı tespitinde seyrek kodlamanın yakınsama kalıplarından yararlanılması ile ilgilidir. Bahsedilen yöntem temel olarak bir eğitim aşaması ile bir test aşaması içermektedir. Yöntem ile birincil kullanıcının olmadığını ve yalnızca gürültü olduğunu gösteren hipotez (H_0), spektrumu kullanmaya hakkı olana bir birincil kullanıcının mevcut olduğunu ve ikincil kullanıcının spektrumu kullanmaması gerektiğini gösteren hipotez (H_1) ve ortamda bir birincil kullanıcı emülatörü / sinyal karıştırıcının olduğunu gösteren hipotezleri (H_2) ayırt edilebilmektedir.

(Şekil 1)

İSTEMLER

1. Birincil kullanıcı emülatörü / sinyal karıştırıcı (PUE/J) saldırısının tespitine yönelik bir yöntem olup, **özelliği**;

Birincil kullanıcının (PU) olmadığını ve yalnızca gürültü olduğunu gösteren hipoteze (H_0) karşılık gelen sinyal (y_0^i),

Spektrumu kullanmaya hakkı olan bir birincil kullanıcının (PU) mevcut olduğunu ve ikincil kullanıcının (SU) spektrumu kullanmaması gerektiğini gösteren hipoteze (H_1) karşılık gelen sinyal (y_1^i),

Ortamda bir birincil kullanıcı emülatörü / sinyal karıştırıcının (PUE/J) olduğunu gösteren hipoteze (H_2) karşılık gelen sinyal (y_2^i)

üçlüsünün kullanılarak

- Bahsedilen her üç sinyal için, yasal birincil kullanıcıya (PU) karşılık gelen kanal (h_{PU}^i) ile rastgele seçilmiş bir veri kümesinin (SD) birleştirilerek birincil kullanıcıya (PU) bağımlı sözlük (D_{PU}) hesaplanması,
- Bahsedilen üç sinyalden her birinin, artık enerji profilini ($\|\mathrm{r}\|_2$) tekrarlayan dikgen eşleştirme algoritması ve karşılık gelen eğitim öznitelik vektörüyle birlikte kombinlenen mutlak gradyanının ($|\mathrm{G}|$) hesaplanması esnasında bu sözlük (D_{PU}) ile seyrek kodlama (SC) işlemine tabi tutulması ve bu işlem ile bahsedilen her üç hipoteze karşılık gelen özellik verilerinin (f) bulunması,
- Bahsedilen eğitim öznitelik vektörlerinden, makine öğrenmesi (ML) temelli bir sınıflandırma (C) işlemi sonucunda sınıf etiketleriyle birlikte bir sınıflandırma modeli (CM) elde edilmesi

işlem adımlarını içeren bir eğitim aşaması ile

- Yasal kullanıcılara karşılık gelen kanallar (h_{PU}) ile örneklenmiş verinin (SD) sözlük hesaplaması (DC) sonucunda bir sözlük (D_{PU}) elde edilmesi
- Her test sinyali (y) için, bahsedilen sözlük (D_{PU}) üzerinden seyrek kodlama (SC) gerçekleştirilmesi ve öznitelik çıkarımı (FE) yapılması
- Çıkarılan öznitelik vektörünün sınıflandırıcı model (CM) ile birlikte sınıflandırıcıya (C) verilmesi,

- Bahsedilen sınıflandırıcının (C), ilgilenilen mevcut özellik verisine (f) karşılık gelen hipotez hakkında bir karar (D) vermesi

işlem adımlarını içeren bir test aşamasını içermesidir.

2. İstem 1'e uygun birincil kullanıcı emülatörü / sinyal karıştırıcı (PUE/J) saldırısının tespitine yönelik bir yöntem olup, **özelliği** f_0^i, f_1^i, f_2^i sinyallerinin karşılık geldikleri eğitim öznitelik vektörlerine sırası ile 0, 1 ve 2 şeklinde eklemesi ve bu özellikler kullanarak saldırı tespiti yapılmasıdır.

3. İstem 1'e uygun birincil kullanıcı emülatörü / sinyal karıştırıcı (PUE/J) saldırısının tespitine yönelik bir yöntem olup, **özelliği** sözlük (D_{PU}) hesaplanması işleminin $D_{PU} = h_{PU} * SD$ eşitliği kullanılarak yapılmasıdır.

TARİFNAME

BİRİNCİL KULLANICI EMÜLATÖRÜ / SİNYAL KARIŞTIRICI SALDIRISI TESPİT YÖNTEMİ

Teknik Alan

Buluş, birincil kullanıcı emülatörü / sinyal karıştırıcı saldırısı tespiti ile ilgilidir.

Buluş özellikle birincil kullanıcı emülatörü / sinyal karıştırıcı saldırısı tespitinde seyrek kodlamanın yakınsama kalıplarından yararlanılması ile ilgilidir.

Tekniğin Bilinen Durumu

Kablosuz iletişim teknolojisindeki ve hizmetlerindeki hızlı büyüme nedeniyle, kablosuz spektrumun azlığı büyük bir problem haline gelmiştir [1]. Gelecekteki kablosuz servislerin gereksinimleri ile spektrum kıtlığı arasındaki çatışmayı çözmek için bilişsel radyo (CR) en umut verici çözümlerden biridir. CR, birincil kullanıcılar ve ikincil kullanıcılar arasında spektrum paylaşımına izin verir [2]. Her ne kadar CR, spektrum kıtlığı sorununu gidermek için umut verici bir çözüm olsa da, hem geleneksel hem de yeni güvenlik tehditlerine karşı doğal olarak savunmasızdır [3]. Bu, kablosuz sistemlerin doğası ve CR'nin benzersiz özelliklerinden kaynaklanmaktadır. Geleneksel güvenlik tehditleri arasında gizli dinleme, sahtekarlık ve sinyal bozma yer almaktadır [4]. Yeni güvenlik tehditleri arasında ise, spektrum algılayıcı veri sahteciliği (SSDF) ve birincil kullanıcı emülasyon saldırısı (PUEA) [5] bulunmaktadır. Bir SSDF saldırısında, kötü niyetli bir CR, işbirlikçi spektrum algılama yaklaşımının performansını düşürmek için yanlış bilgi üretir. Öte yandan, PUEA ise, ikincil kullanıcıları aldatmak ve mevcut spektrum boşluklarını kullanmalarını engellemek için birincil kullanıcıların iletim özelliklerini taklit etmeye çalışmaktadır [5]. Her iki durumda da, saldırı tespiti için yeni ve etkili çözümler geliştirmek, pratik ve güvenli bir CR sistemi için önemli bir gerekliliktir.

Literatürde, sinyal bozucu ve birincil kullanıcı emülasyon saldırısı (PUEA) tespiti için çeşitli yaklaşımlar önerilmiştir. [6]'da, sinyalin enerji algılama yoluyla güç seviyesi kaynağı üzerinde yol gösterici olabileceği belirtilmiştir. Enerji saptamaya dayalı yaklaşımlar basittir; ancak yüksek düzeyde yanlış alarm oranları vardır. Kablosuz kanal

ve iletişim cihazlarının doğal fiziksel özellikleri, PUEA tespiti için de etkilidir [7] [8] [9]. Bununla birlikte, bu tekniklerin uygulanması ekstra yazılım ve donanım ek yükleri gerektirir. Yerini belirleme tabanlı algılama (localization based detection), PUEA algılama için de popülerdir. Buradaki temel fikir, alınan sinyali kullanarak sinyalin kaynağının konumunun anlaşılması ve yasal birincil kullanıcıların (PU) önceden bilinen konumlarının bir veri tabanıyla karşılaştırılmasıdır. Ancak, bu teknikler yalnızca statik birincil kullanıcı senaryoları durumunda uygulanabilmektedir [10] [11]. Çeşitli uygulama alanlarında [12] kullanılan sıkıştırılmış algılama (CS), aynı zamanda birincil kullanıcı emülasyon saldırısı (PUEA) tespitinde de kullanılmıştır. Bu alandaki çalışmalar CS'ye dayanan PUEA tespitini ve alınan sinyal gücünü içerir [13]. Bu yaklaşım ağ boyunca birçok sensöre ihtiyaç duyar ve oldukça karmaşıktır. Diğer bir örnek ise, PUEA tespiti için kanı yayılma algoritmasını (belief propagation) ve CS'den yararlanmayı ele almaktadır [14]. Yine de, bunun uygulanması için merkezi bir düğüm gereklidir.

Mevcut teknikte yer alan CN105743594 (A) patent dokümanı, CR sistemlerinde birincil kullanıcı emülatör saldırısı (PUEA) tespiti için kullanıcılar arası iş birliğine dayalı bir metot önermektedir. Bahsedilen metot, kullanıcı ve saldıranın sinyal enerjileri şemalarını baz almakta; ancak seyrek kodlama ile ilgili herhangi bir öneri sunmamaktadır. Ayrıca, bu dokümanda makine öğrenmesi temelli bir sınıflandırma işleminden de söz edilmemektedir.

Sonuç olarak, yukarıda anlatılan olumsuzluklardan dolayı ve mevcut çözümlerin konu hakkındaki yetersizliği nedeniyle ilgili teknik alanda bir geliştirme yapılması gerekli kılınmıştır.

Buluşun Amacı

Buluş, mevcut durumlardan esinlenerek oluşturulup, yukarıda belirtilen olumsuzlukları çözmeyi amaçlamaktadır.

Buluşun ana amacı, birincil kullanıcı emülatörü / sinyal karıştırıcı saldırısının tespit edilmesidir.

Buluşun bir başka amacı; alınan bozulmuş sinyalin seyrek kodlamasına karşılık gelen ve yasal birincil kullanıcıya karşılık gelen gerçek kanala bağlı olan sözlükler tasarlayarak bilişsel radyodaki sinyal bozma ve birincil kullanıcı emülasyon saldırılarının tespiti için algoritmalar önermektir.

Buluşun bir başka amacı da, seyrek kodlayan artık (residual) sinyal enerji bozulma oranları ile karakterize edilen yakınsama kalıplarının (convergence patterns) bu sözlüklerle birlikte bir spektrum boşluğunu, yasal bir kullanıcıyı veya sinyal bozucu/emulatörü ayırmak için kullanılmasıdır.

Buluşun bir diğer amacı saldırı tespiti esnasında şu hipotezleri ayırt etmektir:

- Birincil kullanıcının olmadığını ve yalnızca gürültü olduğunu gösteren hipotez (H_0)
- Spektrumu kullanmaya hakkı olana bir birincil kullanıcının mevcut olduğunu ve ikincil kullanıcının spektrumu kullanmaması gerektiğini gösteren hipotez (H_1) ve
- Ortamda bir birincil kullanıcı emülatörü / sinyal karıştırıcının olduğunu gösteren hipotez (H_2)

Yukarıda anlatılan amaçları yerine getirmek üzere buluş konusu birincil kullanıcı emülatörü / sinyal karıştırıcı saldırısı tespit yöntemi temel olarak bir eğitim aşaması ile bir test aşaması içermektedir.

Bahsedilen eğitim aşaması;

- Bahsedilen her üç sinyal için, yasal birincil kullanıcıya karşılık gelen kanal ile rastgele seçilmiş bir veri kümesinin birleştirilerek birincil kullanıcıya bağımlı sözlük hesaplanması,
- Bahsedilen üç sinyalden her birinin, artık enerji profilini ($\|\mathrm{r}\|_2$) tekrarlayan dikgen eşleştirme algoritması ve karşılık gelen eğitim öznitelik vektörüyle birlikte kombinlenen mutlak gradyanının ($|\mathrm{G}|$) hesaplanması esnasında bu sözlük (D_{PU}) ile seyrek kodlama (SC) işlemine tabi tutulması,
- Bahsedilen eğitim öznitelik vektörlerinden, makine öğrenmesi (ML) temelli bir sınıflandırma işlemi sonucunda sınıf etiketleriyle birlikte bir sınıflandırma modeli elde edilmesi

işlem adımlarını içermektedir.

Bahsedilen test aşaması ise;

- Yasal kullanıcılara karşılık gelen kanallar ile örneklenmiş verinin sözlük hesaplaması sonucunda bir sözlük elde edilmesi
- Her test sinyali için, bahsedilen sözlük üzerinden seyrek kodlama gerçekleştirilmesi ve öznitelik çıkarımı yapılması

- Çıkarılan öznitelik vektörünün sınıflandırıcı model ile birlikte sınıflandırıcıya verilmesi,
- Bahsedilen sınıflandırıcının, ilgilenilen mevcut test sinyaline karşılık gelen hipotez hakkında bir karar vermesi

işlem adımlarını içermektedir.

Buluşun yapısal ve karakteristik özellikleri ve tüm avantajları aşağıda verilen şekiller ve bu şekillere atıflar yapılmak suretiyle yazılan detaylı açıklama sayesinde daha net olarak anlaşılacaktır ve bu nedenle değerlendirmenin de bu şekiller ve detaylı açıklama göz önüne alınarak yapılması gerekmektedir.

Buluşun Anlaşılmasına Yardımcı Olacak Şekiller

Şekil 1, birincil kullanıcı emülatörü / sinyal karıştırıcının ortamda yer aldığı şematik görünümdür.

Şekil 2, buluşa konu olan birincil kullanıcı emülatörü / sinyal karıştırıcı tespit yönteminin eğitim aşamasının şematik görünümüdür.

Şekil 3, buluşa konu olan birincil kullanıcı emülatörü / sinyal karıştırıcı tespit yönteminin test aşamasının şematik görünümüdür.

Parça Referanslarının Açıklaması

PU: Birincil kullanıcı

SU: İkincil kullanıcı

PUE/J: Birincil kullanıcı emülatörü / sinyal karıştırıcı

SD: Örneklenmiş sözlük

h_{PU}^{i}: Yasal birincil kullanıcıya karşılık gelen kanal

h_{PU}: Yasal kullanıcılara karşılık gelen kanallar

DC: Sözlük hesaplama

D_{PU}: Birincil kullanıcıya bağlı sözlük

y_0^i : Birincil kullanıcının olmadığını ve yalnızca gürültü olduğunu gösteren hipoteze karşılık gelen sinyal

y_1^i : Spektrumu kullanmaya hakkı olan bir birincil kullanıcının mevcut olduğunu ve ikincil kullanıcının spektrumu kullanmaması gerektiğini gösteren hipoteze karşılık gelen sinyal

y_2^i : Ortamda bir birincil kullanıcı emülatörü / sinyal karıştırıcının olduğunu gösteren hipoteze karşılık gelen sinyal

f_0^i : Birincil kullanıcının olmadığını ve yalnızca gürültü olduğunu gösteren hipoteze karşılık gelen özellik verisi

f_1^i : Spektrumu kullanmaya hakkı olan bir birincil kullanıcının mevcut olduğunu ve ikincil kullanıcının spektrumu kullanmaması gerektiğini gösteren hipoteze karşılık gelen özellik verisi

f_2^i : Ortamda bir birincil kullanıcı emülatörü / sinyal karıştırıcının olduğunu gösteren hipoteze karşılık gelen özellik verisi

y : Test sinyali

f : Özellik verisi

SC: Seyrek kodlama

FE: Öznitelik çıkarımı

C: Sınıflandırma

CM: Sınıflandırılmış model

D: Karar

Buluşun Detaylı Açıklaması

Bu detaylı açıklamada, buluşa konu olan faz ve frekans senkronizasyonu sağlayan yöntem ve sistem konunun daha iyi anlaşılmasına yönelik olarak açıklanmaktadır.

Buluşa konu yöntemin kullandığı sistem modeli Şekil 1'de gösterilmektedir. Bu model, bir birincil kullanıcı (PU) düğümü, bir ikincil kullanıcı (SU) düğümü ve bir yasal olmayan düğüm (birincil kullanıcı emülatörü/sinyal karıştırıcı (PUE/J) içermektedir. İkincil kullanıcı (SU) düğümü, bir sinyal karıştırıcı saldırısı ya da birincil kullanıcı emülatörü saldırısını (PUEA) başlatabilecek yasal olmayan bir düğüm varlığında, spektrumdan yararlanmak ister. Birincil kullanıcı (PU) düğümü ve birincil kullanıcı emülatörü (PUE) yapılandırılmış sinyaller iletirken, sinyal karıştırıcı rastgele bir sinyal gönderir. Herhangi bir düğümden gönderilen alıcıdaki sinyal $y = h_x + n$ şeklindedir. Buradaki h_x herhangi bir verici-alıcı çifti arasındaki genel kanal vektörünü (veya matrisini); n ise, toplamalı beyaz Gauss gürültüsünü ifade etmektedir. Mekânsal (spatial) de-korelasyon konsepti nedeniyle, farklı verici-alıcı çiftleri arasındaki h_x kanalı farklıdır [1]. Verici ve alıcı düğümleri arasındaki genel kanal, h_x [2]'de sunulan kanal modeline dayanmaktadır.

Bahsedilen yöntem temel olarak; eğitim aşaması ve test aşaması olmak üzere iki aşamadan meydana gelmektedir.

Şekil 2, buluşa konu yöntemin içerdiği eğitim aşamasını göstermektedir. Eğitim aşamasında H_0 hipotezine karşılık gelen y_0^i, H_1 hipotezine karşılık gelen y_1^i, H_2 hipotezine karşılık gelen y_2^i test sinyalleri kullanılmaktadır. Buna göre, eğitim aşaması sırasıyla şu işlem adımlarını içermektedir:

- Bahsedilen her üç sinyal için, yasal birincil kullanıcıya (PU) karşılık gelen kanal (h_{PU}^i) ile rastgele seçilmiş bir veri kümesinin (SD) birleştirilerek birincil kullanıcıya (PU) bağımlı sözlük (D_{PU}) hesaplanması,
- Bahsedilen üç sinyalden her birinin, artık enerji profilini ($\|\mathrm{r}\|_2$) tekrarlayan dikgen eşleştirme algoritması ve karşılık gelen eğitim öznitelik vektörüyle birlikte kombinlenen mutlak gradyanının ($|\mathrm{G}|$) hesaplanması esnasında bu sözlük (D_{PU}) ile seyrek kodlama (SC) işlemine tabi tutulması ve bu işlem ile bahsedilen her üç hipoteze karşılık gelen özellik verilerinin (f) bulunması,
- Bahsedilen eğitim öznitelik vektörlerinden, makine öğrenmesi (ML) temelli bir sınıflandırma (C) işlemi sonucunda sınıf etiketleriyle birlikte bir sınıflandırma modeli (CM) elde edilmesi.

Buluşa konu yöntemin tercih edilen bir yapılanmasında, f_0^i, f_1^i, f_2^i özellik verileri karşılık geldikleri eğitim öznitelik vektörlerine sırası ile 0, 1 ve 2 şeklinde eklenir ve bu şekilde saldırı tespiti yapılır.

Buluşa konu yöntemin tercih edilen başka bir yapılanmasında ise, sözlük (D_{PU}) hesaplanması işlemi $D_{PU} = h_{PU} * SD$ eşitliği kullanılarak yapılır. Bu eşitlikte yer alan * konvolüsyonu ifade etmektedir.

Şekil 3 ise, buluşa konu yöntemin test aşamasını içermektedir. Buna göre bahsedilen test aşaması şu işlem adımlarını içermektedir:

- Yasal kullanıcılara karşılık gelen kanallar (h_{PU}) ile örneklenmiş verinin (SD) sözlük hesaplaması (DC) sonucunda bir sözlük (D_{PU}) elde edilmesi,
- Her test sinyali (y) için, bahsedilen sözlük (D_{PU}) üzerinden seyrek kodlama (SC) gerçekleştirilmesi ve öznitelik çıkarımı (FE) yapılması,
- Çıkarılan öznitelik vektörünün sınıflandırıcı model (CM) ile birlikte sınıflandırıcıya (C) verilmesi,

  Bahsedilen sınıflandırıcının (C), ilgilenilen mevcut özellik verisine (f) karşılık gelen hipotez hakkında bir karar (D) vermesi.

Referanslar

[1] Y. Arjoune and N. Kaabouch, “A comprehensive survey on spectrum sensing in cognitive radio networks: Recent advances, new challenges, and future research directions,” Sensors, vol. 19, no. 1, p. 126, 2019.

[2] T. Yucek and H. Arslan, “A survey of spectrum sensing algorithms for cognitive radio applications,” IEEE Commun. Surveys Tuts., vol. 11, no. 1, pp. 116–130, First 2009.

[3] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, “A survey on security threats and detection techniques in cognitive radio networks,” IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 428–445, First 2013.

[4] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, “An anti-jamming stochastic game for cognitive radio networks,” IEEE J. Sel. Areas Commun., vol. 29, no. 4, pp. 877–889, April 2011.

[5] D. Chaitanya and K. M. Chari, “Performance analysis of puea and ssdf attacks in cognitive radio networks,” in Computer Communication, Networking and Internet Security. Springer, 2017, pp. 219–225.

[6] F. Jin, V. Varadharajan, and U. Tupakula, “Improved detection of primary user emulation attacks in cognitive radio networks,” in 2015 International Telecommunication Networks and Applications Conference (ITNAC), Nov 2015, pp. 274–279.

[7] S. U. Rehman, K. W. Sowerby, and C. Coghill, “Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios,” IET Communications, vol. 8, no. 8, pp. 1274–1284, 2014.

[8] W. Chin, C. Tseng, C. Tsai, W. Kao, and C. Kao, “Channel-based detection of primary user emulation attacks in cognitive radios,” in 2012 IEEE 75th Vehicular Technology Conference (VTC Spring), May 2012, pp. 1–5.

[9] N. T. Nguyen, R. Zheng, and Z. Han, “On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification,” IEEE Trans. Signal Process., vol. 60, no. 3, pp. 1432– 1445, March 2012.

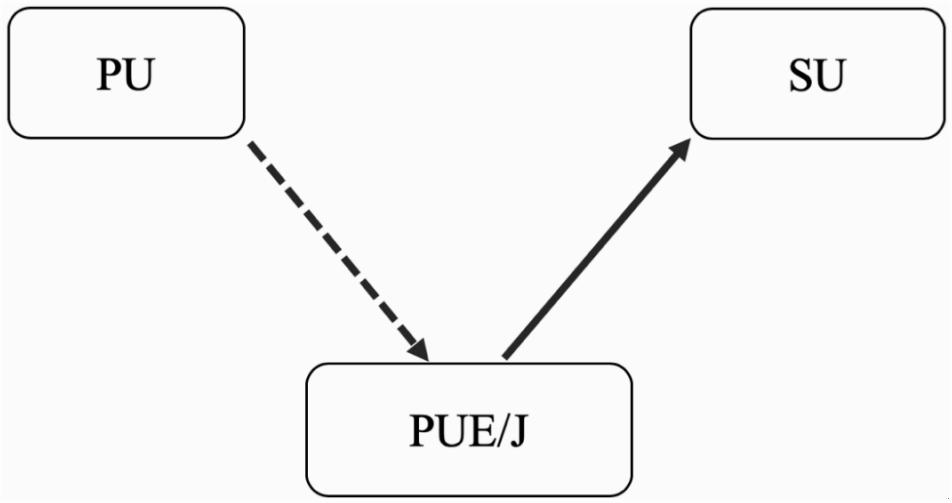
[10] R. Chen, J. Park, and J. H. Reed, “Defense against primary user emulation attacks in cognitive radio networks,” IEEE J. Sel. Areas Commun., vol. 26, no. 1, pp. 25–37, Jan 2008.

[11] N. Patwari and S. K. Kasera, “Robust location distinction using temporal link signatures,” in Proceedings of the 13th Annual ACM International Conference on Mobile Computing and Networking, ser. MobiCom ’07. New York, NY, USA: ACM, 2007, pp. 111–122.

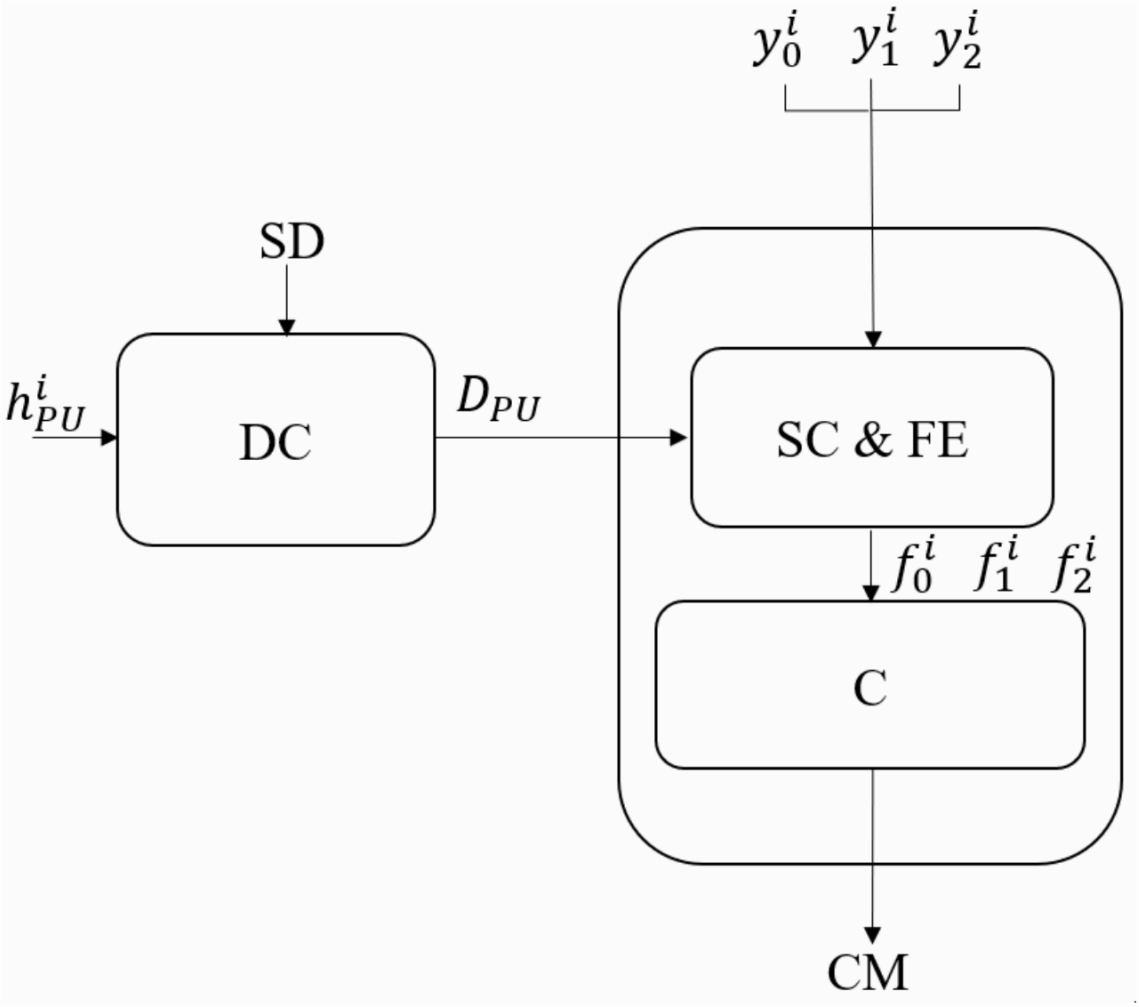
[12] X. Zhang, Y. Ma, Y. Gao, and S. Cui, “Real-time adaptively regularized compressive sensing in cognitive radio networks,” IEEE Trans. Veh. Technol., vol. 67, no. 2, pp. 1146–1157, Feb 2018.

[13] F. Ye, X. Zhang, Y. Li, and H. Huang, “Primary user localization algorithm based on compressive sensing in cognitive radio networks,” Algorithms, vol. 9, no. 2, 2016.

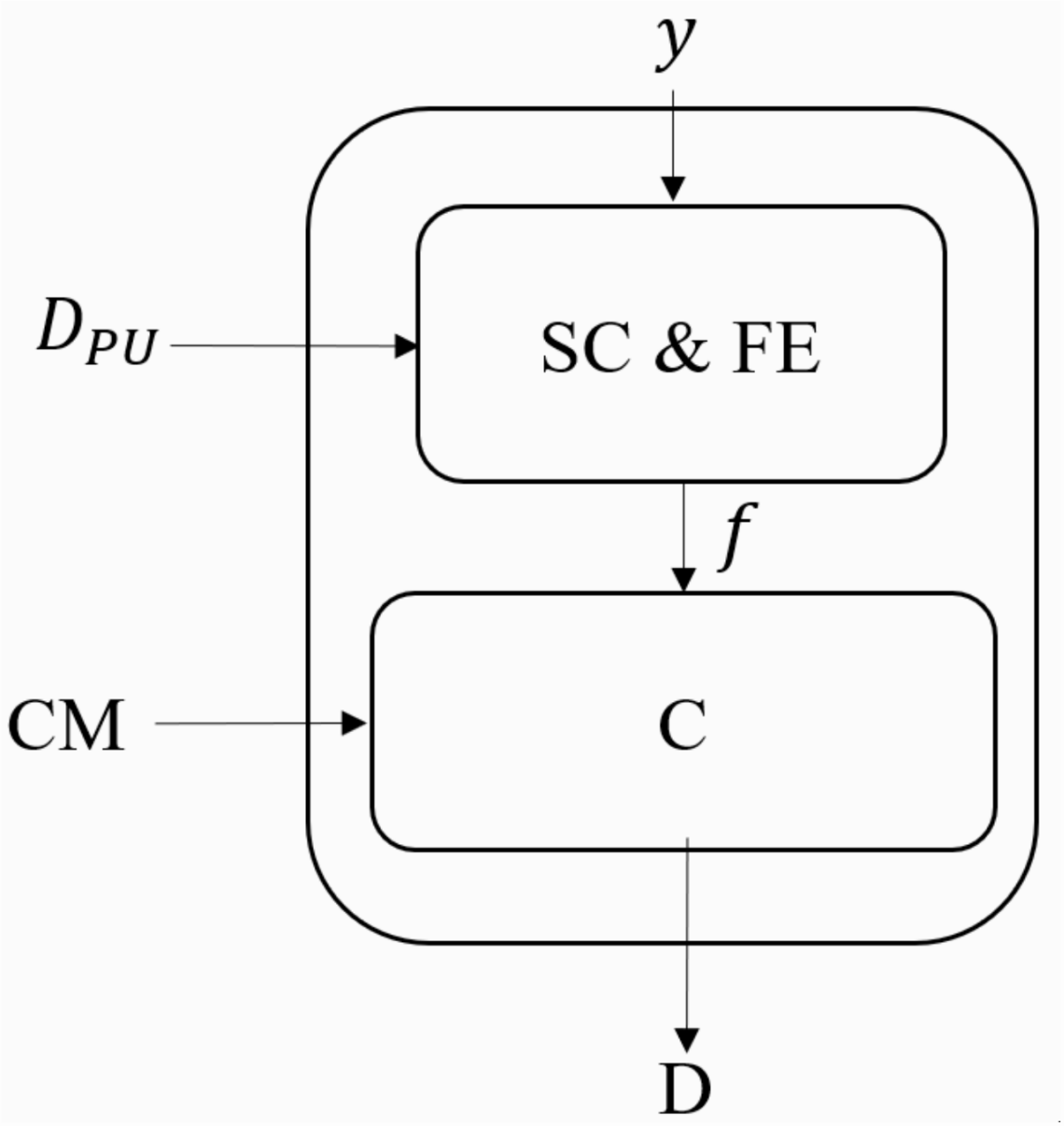
[14] S. Maric, A. Biswas, and S. Reisenfeld, “A complete algorithm to diagnose and alleviate the effects of physical layer attacks,” in 2017 International Conference on Signals and Systems (ICSigSys), May 2017, pp. 29–34.



Şekil 1



Şekil 2



Şekil 3