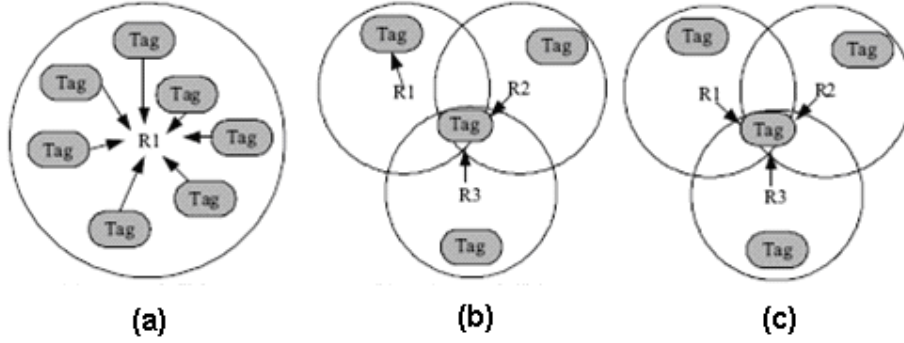


RFID Sistemlerde Tekilleme ve Çakışma Önlenmesi Teknikleri

(RFID Singulation & Anti-Collision Procedures)

Klasik bir RFID sisteminin işleyişinde genellikle bir tek RFID okuyucusunun okuma alanında birden fazla etiket bulunmaktadır. Okuyucunun gönderdiği sorguya etiketlerin aynı anda cevap vermesi çakışma problemini ortaya çıkarmaktadır. Bununla birlikte birden fazla okuyucu ortak bir okuma alanına sahip olduğunda yine aynı çakışma problemi ortaya çıkmaktadır (Bkz. Şekil-1). Çakışma sonucunda etiketler veya okuyucular birbirlerini çalışmaz hale getirmektedir. Etiketler sinyallerini tekrar yayınlamak zorunda kalmakta bu da band genişliğini ve gecikme zamanını arttırmaktadır. Bu noktada iki farklı haberleşme üzerinde durulmalıdır.



Şekil-1: Çakışma Problemleri Çeşitleri [1]:

a) Etiket-Etiket Çakışması b) Okuyucu-Etiket Çakışması c) Okuyucu-Okuyucu Çakışması

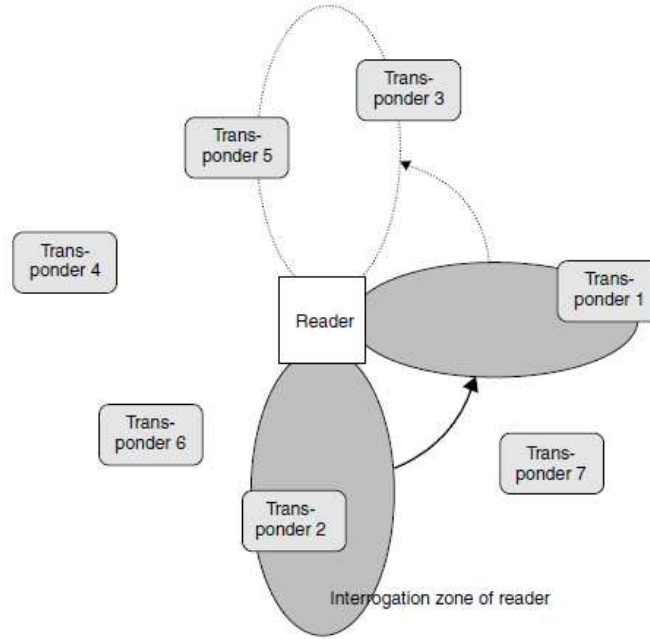
İlk önce okuyucu etiketleri sorgular. Sorgu sinyali bütün etiketler tarafından eş zamanlı olarak alınır. Bu haberleşme bir radyo istasyonu tarafından yayınlanan bir sinyalin yüzlerce alıcı tarafından eş zamanlı alınmasına benzemektedir. Bu haberleşme yayın (broadcast) olarak bilinmektedir. İkinci haberleşme ise okuyucunun sorgulama alanında bulunan etiketler, bilgilerini taşıyan sinyalleri okuyucuya göndermesidir. Bu tür haberleşme çoklu erişim (multi-access) olarak adlandırılmaktadır [1].

Birden fazla vericinin ortak bir alıcıya aynı anda ulaşabilme problemi olan çoklu erişim probleminin çözümü için farklı çözüm önerileri getirilmiştir. Her bir vericinin gönderdiği sinyalin bir diğerinden ayrılmasını amaçlayan dört farklı yaklaşım vardır: SDMA, FDMA, TDMA ve CDMA. Şimdi kısaca bu çözüm önerilerine bakalım [1].

1. Uzay Bölmeli Çoklu Erişim (Space Division Multiple Access, SDMA)

Bu teknik, okuyucunun sorgulama alanını (interrogation zone) belirli parçalara bölerek çoklu erişimi olanaklı hale getirmektedir. Bunun için elektronik olarak kontrol edilen doğrusal bir anten kullanılabilir, böylece bir etikete doğrudan ulaşılabilir (uyumlu –adaptive– SDMA). Sorgulama alanında farklı pozisyonlara sahip etiketler buldukları konumdan dolayı ayrıştırılabileceklerdir. Anten büyüklüğünden dolayı, uyumlu SDMA tekniği ancak çalışma frekansı 850 MHz (ör. 2.45 GHz)'in yukarısında olan RFID uygulamaları için kullanılabilir. Şekil-2'de görüldüğü üzere anten belirli bir alanda sorgulama yaparak okuyucunun sorgulama alanını taramaktadır. SDMA tekniğinin

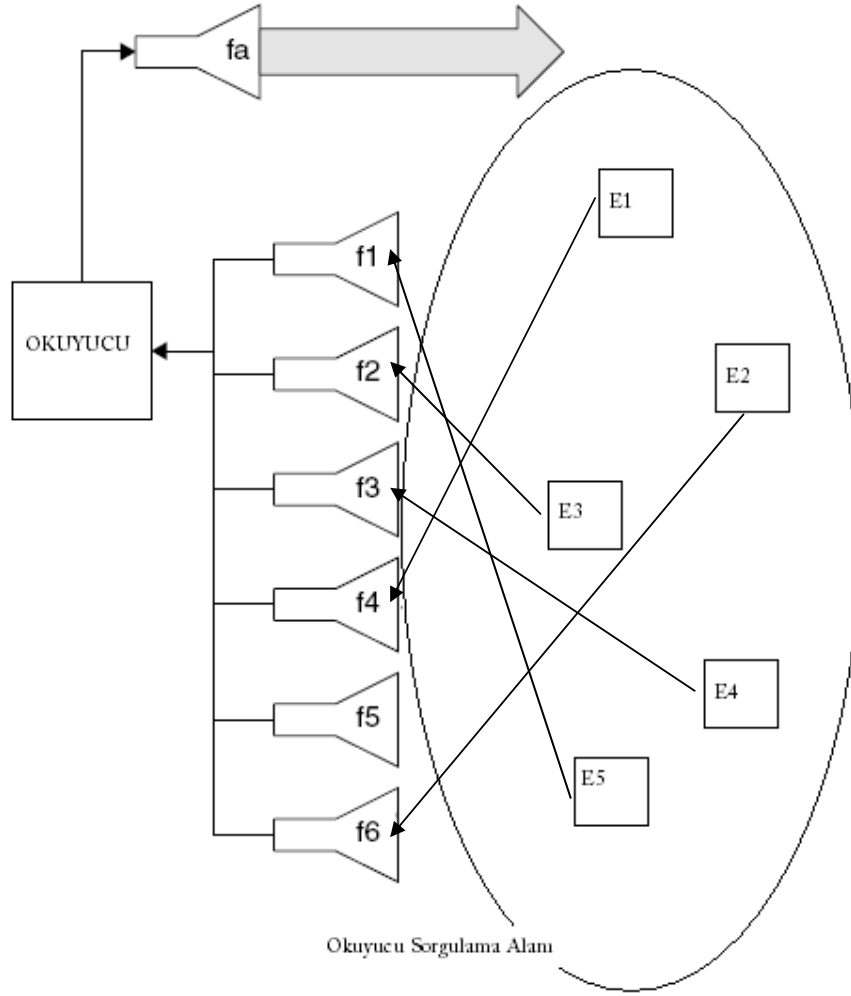
dezavantajı ise karmaşık bir anten sistemine ihtiyaç duymasından kaynaklanan maliyetlidir. Bu yüzden birkaç özel uygulama haricinde kullanılmamaktadır [1].



Şekil-2: SDMA Tekniği [1]

2. Frekans Bölmeli Çoklu Erişim (Frequency Division Multiple Access, FDMA)

Bu teknikte alıcı vericilerin aynı anda konuşabilmesi için birkaç farklı kanal oluşturmaktadır. Okuyucu sorgusunu f_a frekansında yapmaktadır. Etiketler de alıcı olan okuyucuya sinyallerini farklı frekanslarda göndermektedirler (Bkz. Şekil-3). Aynı anda farklı frekans bileşenlerine sahip sinyal okuyucunun alıcı devresiyle alınarak ortamda hangi etiketlerin bulunduğu karar verilmektedir. Bu teknik için farklı frekanslar kullanılmaktadır. Okuyucudan etikete olan haberleşmede (downlink) 135 kHz frekansı kullanılırken, etiketler okuyucuya cevap vermek için 433 – 435 MHz frekans aralığını kullanmaktadırlar. FDMA tekniği okuyucular açısından maliyetlidir çünkü okuyucu farklı kanallara uygun alıcı yapısına sahip olmalıdır.



Şekil-3: FDMA Tekniği

3. Zaman Bölmeli Çoklu Erişim (Time Division Multiple Access, TDMA)

Bu teknikte aynı frekansta zaman parçalara bölünerek birden fazla vericinin alıcıya çoklu erişimi sağlanmaktadır. TDMA tekniği sayısal radyo sistemlerinde yaygın bir şekilde kullanılmaktadır. RFID sistemlerinde çakışma (anti-collision) probleminin çözümü için tercih edilen bir yöntemdir.

ALOHA Tekniği

ALOHA çoklu erişim için kullanılan en basit tekniktir. Adını Hawaii'deki bir radyo ağında veri iletiminde çoklu erişimi sağlamak için geliştirilen ALOHANET'den almaktadır. ALOHA olasılıksal bir TDMA tekniğidir. Etiketler bilgilerini zamanda belirli aralıklarla göndermektedirler. Aralık süresi etiket tarafından belirlenmektedir. ALOHA'nın birkaç farklı şekilde uygulaması vardır.

Bölünmüş (Slotted) ALOHA Tekniği

ALOHA tekniğinin daha iyileştirilmiş bir şekli de Slotted ALOHA yöntemidir. Bu teknikte etiketler sinyallerini belirlenmiş bir zaman aralığında (time slot) yayınlarlar. Bu zaman aralığını okuyucu

belirler, bundan dolayı bu teknik okuyucu tarafından kontrol edilen olasılıksal TDMA çakışma önleyici tekniğidir. Bu tekniği daha iyi açıklamak için bir benzetim yapılabilir. Bu senaryo bir okuyucu ve üç etiket için tasarlanmıştır. Protokol SUS ve KES komutlarını kullanmaktadır. Boş bir oda düşünün. Bu odanın duvarına mili saniye mertebesinde hassas bir saat asıldığını düşünün. İçeriye okuyucu ve etiketler girmektedir. Protokol başlamaktadır.

Okuyucu: Kimse var mı ? Şimdi saat t , benim zaman aralıklarım ise $t+10$, $t+20$, $t+30$, $t+40$ ve $t+50$. Lütfen cevap verin.

Etiket-1: (Olasılıksal olarak seçim yapar, $t+40$ seçer)

Etiket-2: (Olasılıksal olarak seçim yapar, $t+20$ seçer)

Etiket-3: (Olasılıksal olarak seçim yapar, $t+10$ seçer)

(Saat $t+10$ çalar.)

Etiket-3: Üç!

Okuyucu: Herkes SUS, ben Üç ile konuşuyorum.

Etiket-3: Ben Üç!

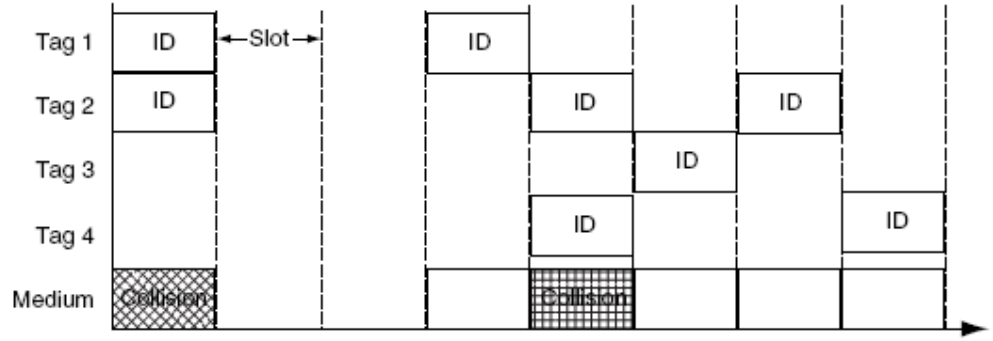
Okuyucu: Paylaşacağın bilgi var mı, Üç?

Etiket: AAAA0FC214B3FF00A0A0EE0F

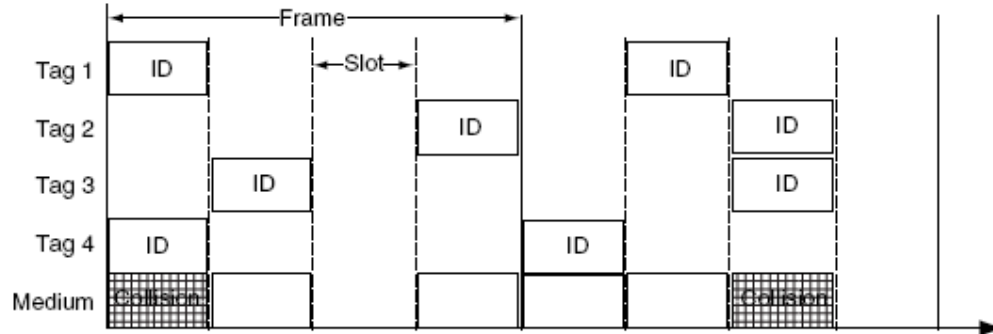
Okuyucu: Tamam Üç, şimdi sen sus.

Kimse var mı ? Şimdi saat t , benim zaman aralıklarım ise $t+10$, $t+20$, $t+30$, $t+40$ ve $t+50$. Lütfen cevap verin [4].

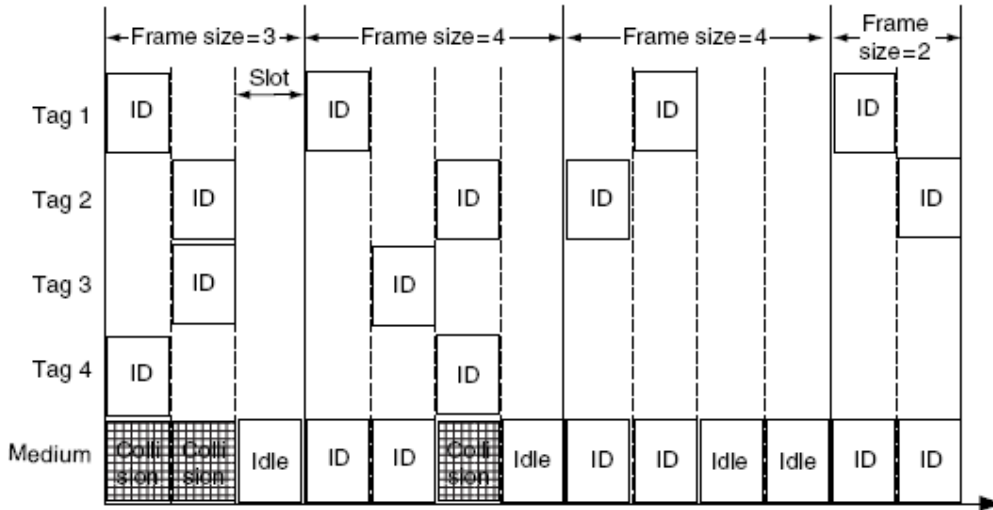
Örnekten de anlaşılacağı üzere okuyucu birçok etiketin bulunduğu bir ortamda etiketlerden biri ile iletişime bu protokol sayesinde geçebilmektedir. Bu örnekte okuyucu önce 3. etiketle iletişime geçmiştir. Onunla konuşması bitince 3. etikete sus komutu verir ve ortamdaki diğer etiketler ile iletişime geçmek için tekrar protokol başlatır.



(a)



(b)



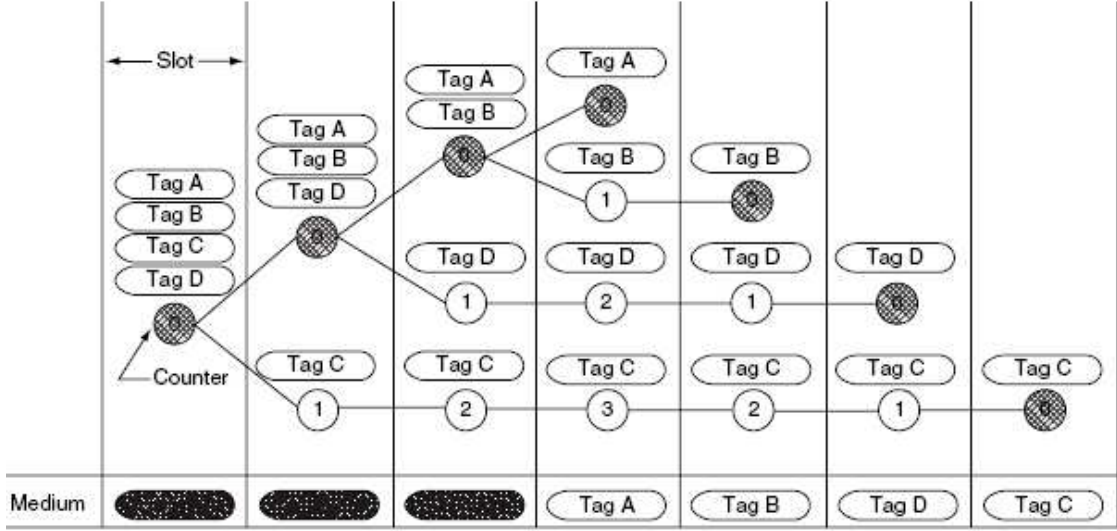
(c)

Şekil-4:ALOHA Protokol Örnekleri

- a) Bölünmüş (Slotted) ALOHA b) Çerçeve Bölünmüş (Frame Slotted) ALOHA
c) Uyumlu Çerçeve Bölünmüş (Adaptive Frame Slotted) ALOHA [2]

Ağaç Tabanlı Çakışma Önleyici Protokoller (Tree-Based Anticollision Protocols)

Bu protokollerde okuyucu etiketleri iki gruba ayırır, daha sonra bu grupları da iki gruba böler. Bir etiket kalıncaya kadar bu bölme işlemine devam edilir. Okuyucu kendi sorgulama alanındaki bütün etiketleri böylece tanımlar. Sorgu Ağacı (Query Tree) ve İkili Ağaç (Binary Tree, BT) olmak üzere farklı ağaç tabanlı protokoller bulunmaktadır.



Şekil-5: İkili Ağaç Protokolü Örneği [2]

BT protokolünde etiketleri iki gruba ayırmak için rastsal sayı üretici kullanılır. Etiketler içlerindeki sayıcı değişkeni sayesinde tanınırlar. Başlangıçta okuyucu etiketler için bir başlangıç mesajı gönderir. Bu mesajı alan etiketler rastsal olarak “0” veya “1” üretirler ve sayıcılarını rastsal olarak ürettikleri değer ile toplarlar. Böylece etiketler sayıcılarındaki değeri “0” ve “1” olan iki gruba ayrılmış olur. Sayıcısındaki değeri “0” olanlar cevap verirler ve okuyucuyu beklerler. Eğer çakışma oluşursa, cevap veren etiketler tekrar rastsal sayı üreticileri kullanarak yeni değerler üretirler ve bu değerleri yine sayıcıları ile toplarlar. Bir önceki konuşmada cevap vermeyen etiketler ise sayıcı değerlerini bir artırırlar. Böylece sadece bir etiket “A” tanımlarlar (Bkz. Şekil-5). Daha sonra etiketler sahip oldukları sayıcı değerlerini her okuyucu sorgulaması ile bir azaltırlar. Sayıcısı “0” değerine ulaşan tanımlanır. Sonuçta, gruptaki tüm etiketler tanımlanmış olur.

Yoğun Okuyucu Ortamı

Birden fazla okuyucu ortak bir sorgulama alanına sahip olduklarında çakışma problemi ortaya çıkmaktadır. Bu problem için ABD’de frekans atlama yöntemi kullanılırken band genişliğinin dar olmasının nedeniyle Avrupa’da konuşmadan önce dinle “listen before talk” protokolü çözüm olarak kullanılmaktadır [3].

KAYNAKLAR

[1] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, John Wiley & Sons, New York, 2003

[2] Wonjun Lee, Jihoon Choi and Donghwan Lee, Comparative Performance Analysis of Anticollision Protocols in RFID Networks

[3] Pedro Peris Lopez, *Lighthweight Cryptography in Radio Frequency Identification (RFID) Systems*, Ph. D. Thesis, 2008

[4] Bill Glover, Himanshu Bhatt, “RFID Essentials”, O’Reilly Media, January 2006