NFC(near-field communication) nedir?

1st Said Enes SUBAŞI¨
Yıldız Technical University
˙Istanbul, Turkey
enes.subasi@std.yildiz.edu.tr
20011060

2nd Metehan TÜRKMEN˘
Yıldız Technical University
˙Istanbul, Turkey
metehan.turkmen@std.yildiz.edu.tr
20011048

3rd Efe Girgin¨
Yıldız Technical University
˙Istanbul, Turkey
efe.girgin@std.yildiz.edu.tr
19011095

4th Ahmet Celal YAZICI
Yıldız TechnicalUniversity
˙Istanbul, Turkey
yusuf.kiran1@std.yildiz.edu.tr
20011503

***Abstract* — Bu çalışma, NFC ve RFID iletişim teknolojilerini karşılaştırarak önemli farkları ortaya koymaktadır. NFC, yakın alan iletişimi sağlarken, mobil ödemeler gibi tüketici elektroniği uygulamalarında yaygın olarak kullanılmaktadır. NFC'nin güvenlik özellikleri, özellikle ödeme sistemlerinde ek kimlik doğrulama adımlarıyla desteklenmektedir. Ayrıca, NFC cihazlarının hızlı etkinleştirilmesi ve devre dışı bırakılması, kullanıcıların güvenliğini artırmaktadır.**

I.GİRİŞ

Yakın alan iletişimi (NFC), RFID tabanlı uzun zamandır kullanılan bir teknolojinin ilerlemesidir.NFC (Near Field Communication), genellikle 4 cm veya daha az mesafe gerektiren kısa menzilli yüksek frekanslı düşük hızlı kablosuz bir iletişim teknolojisidir.Esas olarak mobil veya el tipi cihazlarda veri paylaşımı için kullanılır.Bu tür cihazlar arasında cep telefonları, tabletler, dizüstü bilgisayarlar ve giyilebilir cihazlar bulunur.Ayrıca veri paylaşmanıza ek olarak içerik paylaşmanıza, kablosuz bağlantı kurmanıza veya onaylamanıza, cihazları eşleştirmenize, Bluetooth özellikli cihazları ve akıllı telefonları diğer cihazlara ve bilgisayarlara bağlamanıza ve ağ bağlantılı iki makine veya cihaz arasında bağlantı kurmanıza da olanak tanır. NFC, 13.56 MHz frekansında çalışan ve 106 ila 424 kbit/s arasında değişen veri hızlarında, manyetik indüksiyonu kullanarak çalışan ISO/IEC 18000-3 hava arayüzü standardına uyumlu bir iletişim teknolojisidir.

II.NASIL ÇALIŞIR

NFC'nin çalışma prensibi, bir başlatıcı cihazın (okuyucu) elektrik akımı geçirerek manyetik bir alan oluşturmasını ve bir hedef cihazın (etiket) bu alan içinde yer alarak yanıt vermesini içerir. böylece etikette saklanan veriler kablosuz olarak okuyucuya gönderilir.

Etkileşim, tek yönlü (bir NFC etiketi okumak gibi) veya iki yönlü (iki akıllı telefon arasında veri alışverişi gibi) olabilir. yani hem etiket hem de okuyucu görevi görebilirler.böylece esnek bir kullanım sunar.

NFC'nin benzersiz özelliklerinden biri, hedef cihazın (örneğin bir NFC etiketi) harici bir güç kaynağına ihtiyaç duymamasıdır. Hedef, aktif bir cihaz (genellikle bir akıllı telefon) tarafından oluşturulan alan içine getirildiğinde, bu alan üzerinden gerekli gücü alır. Bu özellik, NFC'yi enerji verimliliği ve maliyet açısından çeşitli uygulamalar için ideal kılar.

III. NFC CİHAZLARININ TİPLERİ

A. Aktif NFC Cihazları:

Bu cihazlar veri gönderme ve alma kapasitesine sahiptir. Akıllı telefonlar, toplu taşımadaki kart okuyucular ve dokunmatik ödeme terminalleri bu kategoriye girer.

B. Pasif NFC Cihazları:

Kendi güç kaynağına ihtiyaç duymadan bilgi gönderebilen etiketler ve küçük vericiler. Diğer kaynaklardan gönderilen bilgileri işlemez ve diğer pasif bileşenlere bağlanamazlar. Genellikle duvarlarda veya reklamlarda etkileşimli işaretler olarak kullanılırlar.

IV. NFC CİHAZLARININ ÇALIŞMA MODLARI

A. Aktif mod

Hem hedef hem de başlatıcı cihazlar aktiftir. İki aktif cihaz arasında çift yönlü veri iletişimi yapılabilir. Örneğin, iki NFC uyumlu akıllı telefon dosya aktarımı yapabilir.

B. Pasif mod

Başlatıcı cihaz bir taşıyıcı alan sağlar, hedef cihaz ise bu alanı modüle eder. Pasif cihaz gücünü başlatıcı cihazın elektromanyetik alanından alır.

V.NFC ETİKETLERİ

Yakın alan iletişiminin (NFC) düzgün çalışması için etiketler gereklidir. Bu, özellikle Nesnelerin İnterneti (IoT) cihazı kullanım durumları bağlamında geçerlidir .

A. Tip 1

Çeşitli NFC uygulamalarında kullanım için ideal olan basit ve uygun maliyetli bir etikettir. Bu etiket okuma ve okuma/yazma özelliğine sahiptir.Bu etiketin yaygın uygulamalarına örnek olarak mobil ödemeler ve Bluetooth cihazlarının bağlanması verilebilir.

B. Tip2

Bu etiket, daha hızlı olmasına rağmen tip 1 etiketine benzer. Bu etiket okuma ve okuma/yazma özelliğine sahiptir. Çarpışma önleme desteğine ve 2K bayta kadar genişletilebilen 96 baytlık belleğe sahiptir. Ayrıca 106 kbit/s iletişim hızına sahiptir. Bu etiketin yaygın uygulamalarına örnek olarak etkinlik ve toplu taşıma biletlerinin işlenmesi verilebilir.

C. Tip3

Bu etiket, Japonya'da daha yaygındır. Bu etiket okuma ve okuma/yazma özelliğine sahiptir. Etiket başına daha pahalıdır ve 1 M bayta kadar hafıza kapasitesine sahiptir. Çarpışma önleme desteğine ve 212 kbit/s iletişim hızına sahiptir. Bu etiketin yaygın uygulamalarına örnek olarak sağlık cihazları ve üyelik kartları verilebilir.

D. Tip4

Bu etiket aynı zamanda tip 1 etiketine benzer. Bu etiket okuma ve okuma/yazma özelliğine sahiptir. Çarpışma önleme desteğine ve maksimum 32k bayt bellek kapasitesine sahiptir. Ayrıca 106 kbit/s iletişim hızına sahiptir.

VI..NFC KULLANMANIN AVANTAJLARI

A. Kolay ve Hızlı İletişim

NFC, cihazlar arasında hızlı ve kolay bir şekilde bağlantı kurulmasını sağlar. Cihazların birbirine yakınlaştırılması yeterlidir ve bu sayede karmaşık eşleştirme süreçlerine gerek kalmaz. Bu özellikle ödeme sistemlerinde, erişim kontrolünde ve cihaz eşleştirmede büyük kolaylık sağlar

B. Güvenli İletişim

NFC, güvenli bir iletişim yöntemi sunar. Kısa mesafede çalışması, veri transferinin güvenliğini artırır. Ayrıca, kriptografik protokoller ve şifreleme yöntemleri ile veri iletimi korunur. Bu, ödeme işlemleri ve kişisel verilerin korunması için kritiktir. Mobil ödemelerde, akıllı telefonunuzun kilidini açmadan işlem yapılamaz, bu da ek bir güvenlik katmanı sağlar.

C. Çok Yönlülük ve Esneklik

NFC, birçok farklı uygulamada kullanılabilir. Mobil ödemeler (Apple Pay, Google Pay), erişim kontrolü (bina girişleri, toplu taşıma), veri transferi (fotoğraf, dosya paylaşımı) ve kimlik doğrulama (dijital kimlik kartları) gibi çeşitli alanlarda esneklik sunar. Ayrıca, telefonunuzu temassız kredi ve banka kartlarından ödeme kabul eden bir terminale dönüştürebilir

D. Kullanım Kolaylığı

NFC, kullanıcılar için son derece basit ve sezgisel bir kullanım sunar. Cihazların birbirine yakınlaştırılmasıyla anında bağlantı kurulabilir ve işlemler gerçekleştirilebilir. Bu kullanım kolaylığı, geniş bir kullanıcı kitlesi tarafından benimsenmesini sağlar. Örneğin, akıllı telefonunuz veya saatinizle ödeme yapmak için cihazı ödeme terminaline yaklaştırmanız yeterlidir.

E. Düşük Enerji Tüketimi

NFC, düşük enerji tüketimi ile çalışır. Bu, özellikle pil ömrünün önemli olduğu mobil cihazlar için büyük bir avantajdır. NFC'nin pasif modda çalışabilmesi, enerji tasarrufu sağlar ve cihazın pil ömrünü uzatır.

F. Gelişen Ekosistem

NFC teknolojisi, genişleyen bir ekosisteme sahiptir. Birçok cihaz, NFC desteği ile piyasaya sürülmekte ve NFC tabanlı uygulamalar giderek artmaktadır. Bu, kullanıcılar için daha fazla kullanım senaryosu ve yeni fırsatlar sunar. Akıllı telefonlar, akıllı saatler, ödeme terminalleri ve akıllı ev cihazları gibi birçok farklı cihazda NFC kullanılabilir.

G. İnteroperabilite

NFC, farklı cihazlar ve sistemler arasında uyumluluk sağlar. Standartlara dayalı bir teknoloji olduğu için, farklı markaların ve modellerin cihazları arasında sorunsuz bir iletişim kurmak mümkündür. Bu, kullanıcıların NFC özellikli cihazlarını farklı ortam ve senaryolarda kullanabilmesini sağlar.

H. Kapsamlı Kullanım Alanları

NFC'nin kullanım alanları oldukça geniştir. Akıllı telefonlar, tabletler, akıllı saatler, ödeme terminalleri, toplu taşıma kartları ve hatta akıllı ev

cihazları gibi birçok farklı cihazda kullanılabilir. Bu, NFC'nin günlük yaşamda birçok farklı amaç için kullanılabilmesini mümkün kılar. Örneğin, toplu taşıma kartlarını yeniden yükleme, dijital kimlik kartlarını doğrulama, güvenlik anahtarlarıyla kimlik doğrulama ve kulaklık ve hoparlörleri eşleştirme gibi birçok kullanım alanı bulunmaktadır.

VII. NFC KULLANIMININ DEZAVANTAJLARI

NFC'nin yakın alan iletişimi sağlama avantajlarına rağmen, bazı dezavantajları da vardır. NFC'nin iletişim mesafesi sınırlıdır ve genellikle 4 santimetreyi geçmez, bu da cihazların çok yakın olmasını gerektirir. Bu sınırlama, bazı uygulamalarda pratiklik sorunlarına yol açabilir. Ayrıca, NFC teknolojisi, veri iletim hızında ve kapasitesinde sınırlamalara sahip olabilir, bu da büyük veri transferlerinde yetersiz kalabilir. Güvenlik açıkları da önemli bir dezavantajdır; özellikle kötü niyetli kişilerin NFC etiketleri üzerinden zararlı yazılımlar veya komutlar iletebilme riski bulunmaktadır. NFC'nin enerji tüketimi düşük olsa da, sürekli aktif tutulması durumunda cihazın pil ömrünü olumsuz etkileyebilir. Bu dezavantajlar, NFC teknolojisinin kullanımını belirli senaryolarla sınırlandırabilir.

VIII. NFC'DE GÜVENLİĞİ SAĞLAYAN ETMENLER

A. Kısa Mesafe İletişimi

NFC'nin en belirgin güvenlik özelliği, iletişim mesafesinin çok kısa olmasıdır. Genellikle 4 santimetre veya daha az bir mesafede çalışır. Bu kısa mesafe, cihazların birbirleriyle fiziksel temas gerektirdiği anlamına gelir. Dolayısıyla, mesafeli saldırılara karşı doğal bir koruma sağlar. Bir saldırganın, verileri yakalayabilmesi veya manipüle edebilmesi için fiziksel olarak çok yakın olması gerekmektedir.

B. Kriptografi Kullanımı

NFC iletişimi, genellikle şifrelenmiş bir şekilde gerçekleştirilir. NFC cihazları arasında veri alışverişi yapılırken, çeşitli güvenlik protokolleri ve algoritmaları kullanılarak iletişim şifrelenir. Bu, iletilen verilerin üçüncü şahıslar tarafından ele geçirilmesini ve anlaşılmasını zorlaştırır. Özellikle ödeme sistemleri gibi hassas uygulamalarda, güçlü şifreleme yöntemleri kullanılır.

C. Kimlik Doğrulama ve Yetkilendirme

NFC tabanlı ödemeler gibi kritik işlemler genellikle ek bir kimlik doğrulama adımı gerektirir. Bu, kullanıcıların cihazlarını doğrulamaları ve işlemleri onaylamaları için bir PIN kodu veya biyometrik doğrulama (parmak izi, yüz tanıma) kullanmalarını içerir. Bu ek güvenlik katmanı, yetkisiz erişimi engellemeye yardımcı olur ve yalnızca yetkili kullanıcıların işlemleri gerçekleştirmesini sağlar.

D. Hızlı Etkinleştirme ve Devre Dışı Bırakma

NFC cihazları, kullanıcılar tarafından hızlı bir şekilde etkinleştirilebilir veya devre dışı bırakılabilir. Bu özellik, kullanıcıların istemedikleri durumlarda NFC özelliğini kapatmalarını sağlar. Özellikle güvenli olmayan ortamlarda veya gereksiz kullanım durumlarında, NFC'nin kapatılması izinsiz erişim riskini azaltır.

IX.NFC'DE GÜVENLİK TEHDİTLERİ

NFC, birçok güvenlik özelliği ve protokolü sayesinde güvenli bir iletişim aracı olarak kabul edilir. Ancak, teknolojinin güvenliğini artırmak için kullanıcıların bazı önlemleri alması gerekmektedir

A. Eavesdropping (Dinleme):

Dinleme, iki NFC cihazı arasında iletilen verilerin üçüncü bir tarafça ele geçirilmesidir. Saldırgan, NFC iletişimini izleyerek hassas bilgileri (örneğin, ödeme bilgileri) çalabilir. NFC'nin kısa iletişim mesafesi (genellikle 4 cm veya daha az) dinleme riskini azaltır, ancak saldırganlar özel ekipman kullanarak bu mesafeyi artırabilir.

B. Veri Değiştirme (Data Modification):

Veri değiştirme saldırılarında, saldırgan iki NFC cihazı arasındaki veri iletimini keserek gönderilen verileri değiştirebilir. Bu, örneğin, bir ödeme işlemi sırasında gönderilen miktarın değiştirilmesi anlamına gelebilir. Bu tür saldırılar, veri iletimi sırasında uygun şifreleme kullanılmadığında mümkündür.

C. Veri Bozulması (Data Corruption):

Veri bozulması, saldırganın, NFC iletişimi sırasında gönderilen verileri bozarak cihazlar arasında doğru bilgi alışverişini engellemesidir. Bu, cihazların yanlış veya eksik verilerle işlem yapmasına neden olabilir. Bu saldırı türü, genellikle sinyal gürültüsü ekleyerek veya iletilen verileri manipüle ederek gerçekleştirilir.

D. Man-in-the-Middle (MitM) Saldırıları:

Man-in-the-Middle saldırıları, saldırganın iki NFC cihazı arasındaki iletişimi gizlice ele geçirip değiştirdiği saldırılardır. Saldırgan, cihazların birbirleriyle doğrudan iletişim kurduğunu düşündüğü anda araya girer ve iletilen verileri okur veya değiştirir.

E. Relay (Yönlendirme) Saldırıları:

Yönlendirme saldırılarında, saldırgan, iki NFC cihazı arasındaki iletişimi fiziksel olarak uzağa yönlendirir. Örneğin, bir saldırgan, bir NFC kartının sinyalini uzaktan okuyarak bir başka cihazla iletişime geçirebilir. Bu tür saldırılar, özellikle temassız ödeme sistemlerinde ciddi güvenlik riskleri oluşturur.

F. Kötü Amaçlı NFC Etiketleri:

Kötü niyetli kişiler, zararlı yazılımlar veya kötü amaçlı komutlar içeren NFC etiketleri oluşturabilir. Bu etiketler, kullanıcıların cihazlarına zarar verebilir veya hassas bilgileri çalabilir. Kullanıcıların, tanımadıkları veya güvenmedikleri NFC etiketlerini cihazlarına okutması bu tür saldırılara yol açabilir.

X.NFC'NİN KULLANIM ALANLARI

NFC teknolojisi, biletleme, temassız ödemeler, veri aktarımı, elektronik oylama, sağlık ve fitness, reklam, kayıt tutma, otomatik check-in sistemleri ve ev otomasyonu gibi çeşitli alanlarda geniş bir uygulama yelpazesine sahiptir. Bu teknoloji, kağıt israfını azaltma, ödeme süreçlerini hızlandırma, veri aktarımını kolaylaştırma, oylama süreçlerini güvenli hale getirme ve akıllı ev cihazlarının bağlanmasını sağlama gibi birçok avantaj sunar.

Telefonlarda ise NFC, mobil ödemeler, toplu taşıma kartlarının yeniden yüklenmesi, dijital kimlik doğrulama ve hızlı cihaz eşleştirme gibi pratik ve güvenli uygulamalar sunar. Apple Pay ve Google Pay gibi sistemler, mobil ödemelerde yaygın olarak kullanılırken, NFC etiketleri ile çeşitli otomasyonlar da gerçekleştirilebilir. NFC, telefonlarda kullanım kolaylığı ve güvenlik sağlayarak günlük yaşamı daha pratik hale getirir.

XI.NFC VE RFID TEKNOLOJİLERİNİN KIYASLANMASI

A. İletim Mesafesi

NFC, yakın alan iletişimi sağlar ve iletişim mesafesi genellikle 4 santimetreye kadar (maksimum 10 cm) sınırlıdır. NFC cihazları, veri alışverişi yapabilmek için birbirlerine çok yakın olmalıdır. Özellikle güvenli ödeme sistemleri gibi hassas bilgilerin iletiminde büyük bir avantaj sağlar. RFID ise çok daha uzun mesafelerde iletişim sağlayabilir. RFID sistemleri, birkaç metreden birkaç yüz metreye kadar değişen iletişim mesafelerine sahiptir. RFID etiketleri ve okuyucuları arasında fiziksel temas gerekmez, bu da envanter yönetimi gibi uzaktan izleme ve tanımlama gerektiren uygulamalar için idealdir.

B. Uygulama Alanları

NFC, genellikle tüketici elektroniği ve mobil ödemeler gibi kullanım alanlarında yaygındır. Mobil ödemeler, akıllı kartlar ve akıllı ev cihazları gibi alanlarda sıkça kullanılır. RFID ise endüstriyel ve ticari uygulamalarda geniş bir yelpazede kullanılır. Lojistik ve tedarik zinciri yönetimi, envanter takibi, hayvan tanımlama ve otomatik geçiş sistemleri gibi alanlarda sıkça tercih edilir.

C. Güvenlik ve Yetkilendirme

NFC, güvenlik ve yetkilendirme konularında daha gelişmiş özelliklere sahiptir. Özellikle ödeme sistemlerinde, ek kimlik doğrulama adımları gerektirebilir ve iletişim sırasında veri şifreleme teknikleri kullanılır. Bu, NFC'nin daha güvenli olmasını sağlar. RFID sistemleri ise genellikle daha basit güvenlik önlemlerine sahiptir. Veriler genellikle açık bir şekilde iletilir ve okunur. Bu, düşük güvenlik gerektiren uygulamalar için yeterli olabilir, ancak hassas bilgilerin korunması gereken durumlarda ek güvenlik önlemleri alınmalıdır.

D. Maksimum Bağlantı Sayısı

NFC, tipik olarak tek bir eşzamanlı bağlantı sağlar. Bir NFC cihazı aynı anda yalnızca bir başka cihazla iletişim kurabilir. Örneğin, bir akıllı telefon, aynı anda tek bir NFC etiketiyle etkileşimde bulunabilir. RFID ise birçok cihazla eşzamanlı iletişim kurabilir. Bu, özellikle büyük ölçekli izleme ve tanımlama uygulamalarında büyük bir avantajdır. Bir RFID okuyucu, aynı anda birden fazla RFID etiketini okuyabilir veya yazabilir.