KABLOSUZ AĞLARDA GÜVENLİK PROTOKOLLERİNİN KARŞILAŞTIRMALI İNCELENMESİ

[1]Ali Osman HARMANKAYA, [2]H. Engin DEMİRAY, [3]İsmail ERTÜRK, [4]Cüneyt BAYILMIŞ, [5]Necla BANDIRMALI

Kocaeli Üniversitesi

[1]Enformatik Bölümü, [2]Mühendislik Fakültesi, [3,4,5]Teknik Eğitim Fakültesi

41380 Kocaeli

{[1]harmankaya, [2]demiray, [3]erturk, [4]cbayilmis, [5]nbandirmali}@kou.edu.tr

ABSTRACT

The need for secure networking has been gaining importance in parallel to the progresses in wireless communication technologies. As an important type of wireless communications, wireless sensor networks have been widely applied with different security characteristics and requirements. This paper presents the security protocols for both wireless networks and wireless sensor networks indicating the main differences. The RSN, in addition to the WPA and WEP, is one of the most preferred security protocols for wireless networks as it employs the AES cryptography method. On the other hand, most of the current wireless sensor network applications prefer the LISP security protocol with many benefits compared to its SNEP and LEAP counterparts.

Key words: Wireless Networks, Wireless Sensor Networks, Security Protocols.

1. GİRİŞ

Günümüzde gelişen ağ iletişim teknolojilerine paralel, kablosuz iletişim sistemlerinin kullanımları da hızla artmaktadır. Buna bağlı olarak kablosuz iletişim sistemlerindeki veri güvenliğini sağlamak önem kazanmaktadır. Bu çalışmanın temel amacı, kablosuz iletişim sistemlerindeki güvenlik protokollerini karşılaştırarak farklı uygulamalar için en uygun olanlarını tespit etmektir.

Kablosuz algılayıcı ağlar, sınırlı kapasiteli, kısa mesafede kablosuz ortam üzerinden haberleşebilen düşük güçlü ve düşük maliyetli algılayıcı düğümlerinden meydana gelmektedir ve bu özellikleriyle genel kablosuz sistemler içerisinde ayrı bir öneme sahiptir. Gözlem yapılacak ortama rasgele dağıtılabilen bu düğümler, birbirlerini tanıyabilmekte ve ortak gayret sarf ederek geniş bir alanda ölçüm vazifesini gerçekleştirebilmektedir. Bu avantajlarından dolayı sağlıktan askeri uygulama alanlarına, bir binanın güvenliğinin sağlanmasından orman yangınlarının önceden tespitine kadar çok çeşitli şekillerde kullanılabilmektedirler.

Güvenlik, kablolu veya kablosuz her türlü ağ için oldukça önemli bir konudur. Klasik bir kablolu ağ üzerinden iletişim, fiziksel kablolar üzerinden sağlanır ve güvenlik, genellikle fiziksel altyapıda dahili olarak bulunur. Kablosuz ağlarda ise çoğunlukla RF sinyalleri kullanılır ve bu nedenle aynı güvenlik önlemlerinin uygulanması mümkün olmayabilir. Kablosuz ağ kullanıcılarının ve verilerinin, bilgisayar korsanlarının saldırılarına, kurumsal casusluğa karşı daha güvenli hale getirilmesi için çeşitli güvenlik özelliklerinden yararlanılır.

Kablosuz ağlara özgü çeşitli güvenlik tedbirleri bulunmaktadır. Bunların başlıcaları, SSID kullanımı, cihaz kimlik doğrulama mekanizmaları, MAC adresi filtreleme ve şifreleme teknolojisi olan WEP şeklinde sıralanabilir.

Kablosuz algılayıcı ağ (KAA) düğümlerinin sınırlı donanımsal kaynaklara ve güç birimlerine sahip olması, bazı çözüm bekleyen güvenlik açıklarını da beraberinde getirmektedir. Ortam erişim protokolünün açıklarından faydalanarak algılayıcı düğümlerin iletişimlerinin kesilmesine ya da anormal durumların oluşmasına ve böylece ağ ömrünün kısalmasına sebep olan hizmet engelleme (Denial of Service-DoS) saldırıları, kablosuz algılayıcı ağ güvenliği için önemli bir tehdit unsuru oluşturmaktadır. Kablosuz algılayıcı ağlar için tasarlanan ortam erişim protokolleri arasında en yaygın olarak bilinen S-MAC (Sensor Medium Access Control – Algılayıcı Ortam Erişim Kontrolü) ve türevleri (T-MAC, D-MAC v.b.) bu tür saldırılara karşı savunmasızdır. Dolayısıyla güvenlik protokollerine ihtiyaç duyulmaktadır.

1. bölümdeki giriş kısmında kablosuz ağlar, kablosuz algılayıcı ağlar ve veri güvenliği üzerinde durulmaktadır. Bölüm 2'de kablosuz ağlardaki güvenlik gereksinimi ve güvenlik protokollerinden bahsedilmektedir. Ayrıca kablosuz ağlar için güvenlik protokolleri anlatılarak, karşılaştırmalı olarak kıyaslanmaktadır. 3. bölümde kablosuz algılayıcı ağlar için güvenlik protokolleri üzerinde durulmaktadır. Son bölümde ise karşılaştırma sonuçları ve değerlendirmeler sunulmaktadır.

2. KABLOSUZ AĞ GÜVENLİK PROTOKOLLERİ

Son yıllarda İnternet'in ve İnternet üzerinden ticaretin gelişmesiyle birlikte, bilgisayar ağları oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Bilgisayar ağlarının bu zafiyetleri, kritik ticari uygulamalarda ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur.

Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hala büyük bir tehlike oluşturmaktadır. Günümüzde İnternet, gerek kişisel gerekse ticari ilişkilerde bilgi akışını sağlayan, dünyanın en büyük iletişim aracı haline gelmiştir. İnternet'in tüm dünyada böylesine yaygın kullanımı, güvenlik açıklarını ve tehditlerini (bilgi kayıpları veya gizlilik ihlalleri) de artırmaktadır.

Bilgisayar ağlarında, kullanıcılardan, işletim sistemlerinden veya ağ protokollerinden kaynaklanan açıklar ile çok sık karşılaşılmaktadır. Güvenli bir bilgisayar ağı için mutlaka güvenlik politikaları oluşturmalıdır ve güvenlik sistemleri buna göre tercih edilmelidir. Ayrıca kullanıcılara gerektiği kadar erişim imkanı sağlanmalı ve kullanıcılar bu konular hakkında bilinçlendirilmelidir.

Kablosuz ağlar için literatürde sunulan önemli güvenlik protokollerinden üçü (WEP, WPA ve RSN) ayrıntılı olarak alt bölümlerde açıklanmaktadır.

2.1. WEP

Kablosuz ağların geliştirildiği ilk yıllarda IEEE 802.11'de geçerli olan tek güvenlik protokolü WEP'dir (Wireless Equivalent Privacy) [3]. Özellikle son yıllarda bu protokolün önemli zayıflıkları ortaya çıkmıştır. IEEE 802.11 standartları için güvenlik protokolü tasarlanırken gerekli koşullar şunlardır:

- Makul bir şekilde güçlü olmalı (algoritma kolayca kırılmamalı),
- Etkin olmalı (donanım veya yazılım ile gerçeklenebilmeli),
- İhraç edilebilir olmalı,
- Kullanımı isteğe bağlı olmalı.

WEP güvenlik protokolünün şifreleme algoritması RC4 (Rivest Cipher), anahtar uzunluğu 40 bit (veya 104 bit), IV (Initialization Vector) uzunluğu 24 bit, veri bütünlüğü yöntemi ise ICV'dir (Integrity Check Value). Kullanılan şifreleme algoritması RC4 bir akış şifreleyicisi olup simetrik anahtar içermektedir.

Veri iletişimi başlamadan önce, kullanıcılar ve erişim noktaları arasında ilişkilendirilme yapılır. Bu ilişkilendirilme öncesinde asıllama yapılması gerekmektedir. IEEE 802.11, farklı asıllama yöntemleri uygulamaktadır. Bunlar;

- Açık güvenlik (SSID – Service Set Identifier): Erişim noktasına SSID (erişim noktası ayırt edici) bilgisi ile gelen tüm asıllama istekleri kabul edilir.
- Ortak anahtarlı asıllama: Asıllama paylaşılan bir anahtar ile yapılır. Bu anahtarın kullanıcıya daha önceden bildirilmiş olması gereklidir.
- MAC adresi ile asılama: Erişim noktası üzerinden haberleşebilecek kullanıcıların MAC (Media Access Control) adresleri bir sunucuda RADIUS (Remote Authentication Dial-In User Service) tutulmaktadır. Sadece daha önceden belirlenmiş MAC adresine sahip kullanıcılar asıllanmaktadır.

WEP güvenlik protokolünde kullanılabilecek anahtarlar iki gruba ayrılır. Bunlar ön seçili anahtarlar ve kullanıcıya özel anahtarlardır. Ön seçili anahtarlı yapıda erişim noktası ve kullanıcılar veri şifrelemede aynı anahtarı kullanır. Açıkça görüldüğü gibi bu yöntem kullanıldığında tüm kullanıcılar tüm verileri çözebilirler. İkinci yöntemde ise erişim noktası her kullanıcıya karşılık farklı anahtarlar bulundurmaktadır ve böylece kullanıcı sadece kendine gelen verileri çözme yeteneğine sahip olacaktır.

WEP şifreleme ve şifre çözme yönteminde, 24 bitlik başlangıç vektörü (IV), 40 bitlik paylaşılan anahtara eklenir. Bu anahtardan RC4 algoritması kullanılarak şifrelenecek veri uzunluğunda akış şifresi elde edilir. IV'nin değişmesi ile her seferinde farklı akış şifreleri elde edilmektedir. Bu sırada veri bütünlüğünü sağlamak için asıl veri üzerinden ICV hesaplanır ve verinin sonuna eklenir. Elde edilen akış şifresi ile (veri + ICV) özel veya (EXOR) işleminden geçirilerek şifreli metin hazırlanır. Son adım olarak, alıcının şifreyi çözebilmesi için gerekli olan IV, çerçevenin başına şifrelenmeden eklenir. Böylece gönderilecek çerçeve tamamlanır.

Şifre çözmede ise alıcı, IV'yi çerçeveden okuyarak akış şifresini elde edebilir. Anahtar alıcıda bulunduğundan, şifreleme işlemleri ters sıra ile gerçekleştirilerek, açık veri elde edilir.

WEP güvenlik protokolünün tekrar saldırısı, bit zayıflığı, IV'lerin tekrar kullanılması ve RC4'ün zayıf anahtarlar üretmesi gibi güvenlik açıkları ve zafiyetleri bulunmaktadır.

Sonuç olarak özetle;

- WEP, tekrar saldırılarını önleyemez.

- RC4 algoritmasında zayıf anahtarlar kullanılması, şifreleme anahtarının kolayca ele geçmesine neden olabilir.
- WEP, IV'leri tekrar kullanır. Bazı kriptoanaliz yaklaşımları ile şifreleme anahtarı bilinmeden veri çözülebilir.
- ICV'nin elde edilme yönteminin zayıflığı nedeni ile mesaj bütünlüğü araya giren üçüncü şahıslar tarafından bozulabilir.

2.1. WPA

WEP güvenlik protokolünün çok sayıdaki açıklarından dolayı, endüstrinin acil ihtiyacı için 802.11i standartlarına (draft 3.0) uygun geçici bir güvenlik sistemi, Wi-Fi grubu tarafından oluşturulmuştur. WPA (Wireless Protected Access) [5], WEP'in bilinen tüm güvenlik açıklarını kapatır. Donanım değişikliğine gidilmeden yükseltme yapılabiliyor olması, WEP'e göre daha güçlü şifreleme (TKIP, Temporal Key Integrity Protocol) ve asıllama (802.1x) yapısına sahip olması önemli kullanım kolaylıkları sağlamaktadır. Ayrıca WEP'de bulunmayan bir anahtar yönetim mekanizmasına da (802.1x) sahiptir.

TKIP (Geçici Anahtar Bütünlüğü Protokolü), RC4 akış şifreleyici algoritma üzerine kuruludur. 4 yeni algoritma ile WEP şifreleme mekanizmasını geliştirir. Bunlar;

- IV 48 bite çıkarılmıştır ve paket numarası olarak kullanılmaktadır.
- Zayıf anahtarlar kullanılmamaktadır.
- Yeni bir mesaj bütünlük kontrol mekanizması olan Michael MIC'i (Message Integrity Check) kullanır.
- Anahtar temini ve dağıtımı için yeni bir metot getirir (802.1x).
- Her çerçeve için yeni bir anahtar oluşturulur.

802.1x Genişletilebilir Kimlik Doğrulama Protokolü (Extensible Authentication Protocol, EAP) ile asılama, IEEE standartları üzerine kurulan bir yapıdır. Hem WLAN hem de LAN'larda kullanılmaktadır.

WEP'deki ICV'nin bilinen birçok zayıflıkları bulunmaktadır. WPA'da, Michael olarak bilinen bir yöntem yardımıyla 8 baytlık bir ileti bütünlüğü kodu (MIC) hesaplayan yeni bir algoritma tanımlamaktadır. MIC alanı, çerçeve verileri ve ICV ile birlikte şifrelenir. Alıcı/gönderici MAC adresleri ve mesaj bir "hash" fonksiyonuna tabi tutulur ve 8 baytlık bir çıktı oluşturulur. MIC, IEEE 802.11 çerçevesinin veri bölümü ile 4 baytlık ICV arasına yerleştirilir ve daha sonra çerçeve verileri ve ICV ile birlikte şifrelenir. MIC doğrusal bir algoritma ile oluşturulmadığından, ICV gibi zayıflıkları bulunmamaktadır. Böylece, araya giren üçüncü şahıslar, mesajı değiştirdiğinde anlaşılması sağlanır.

WPA'nın WEP'den önemli bir farkı olarak anahtar yönetimi gösterilebilir. WPA'da 2 çeşit anahtar yapısı vardır:

- Oturum anahtar kümesi: 2 kablosuz cihazın haberleşmesinde kullanılır. Genellikle bir kullanıcı ve erişim noktası arasında kullanılır (unicast).
- Grup anahtar kümesi: Ağ içinde tüm kullanıcıların bildiği ve yayım (braoadcast) yapılması için kullanılan anahtarlardır (multicast).

Oturum ana anahtarı ve grup ana anahtarı, ana anahtardan elde edilir. Ana anahtar ise asıllama sırasında asıllama sunucusu tarafından üretilmiştir. Oturum ana anahtarından elde edilen anahtarlar geçicidir. Her yeni düğümle bağlantı yeniden kurulduğunda ya da ağdan ayrılıp tekrar girildiğinde yeniden oluşturulur. Üretilen anahtarların ikisi şifreleme ve veri bütünlüğü için kullanılır.

Grup ana anahtarları da grup geçici anahtarı ile erişim noktaları tarafından belirlenip kullanıcılara dağıtılmaktadır.

TKIP'in genel yapısı incelenildiğinde, farklı anahtar üretme yöntemleri ile anahtar elde edildiği görülmektedir. Mesaj bütünlük kodu hesaplanır ve mesajın sonuna eklenir. Mesaj parçalara ayrılarak IV ve anahtardan elde edilmiş akış şifresi ile şifrelenir ve alıcıya gönderilir.

2.3. RSN

WPA günümüzde kırılmamış olsa da WEP tabanlı bir yapı olduğu ve eksiklerinin çıkabileceği şüphesinden hareketle (RC4 algoritmasının zayıflıkları düşünüldüğünde) IEEE 802.11i standartlarına uygun yeni bir protokol geliştirilmiştir. Bu protokol WEP üzerine kurulmadam, yeni ve farklı bir yapıda geliştirilmiştir. 2004'den itibaren RSN'i destekleyen WPA uyumlu ürünler, WEP'i desteklememektedir.

RSN (Robust Security Network) [4], asıllamayı ve anahtar yönetimini IEEE 802.1x standartları ile gerçekler. Veri bütünlüğü MIC ile sağlanır. Gezginlik (roaming) fonksiyonlarının da desteklendiği gerçek zamanlı iletişimlerde önem kazanır, çünkü; veri kaybını engelleyen bir yaklaşım içermektedir. RSN, gezginliği iki farklı şekilde desteklemektedir:

- Önceden asıllama: Kullanıcı bir erişim noktasına bağlı iken diğer bir erişim noktasının varlığının farkına varırsa, 802.1x anahtar

değişimi ile bu erişim noktası için de anahtarları elde eder ve saklar.
- Anahtar ön bellekleme: Erişim noktası ile daha önceden anahtar belirlendi ise bu anahtarlar bellekte saklanır.

RSN'de şifreleme TKIP veya CCMP (Counter Mode with CBC-MAC Protocol) ile gerçeklenir. CCMP zorunlu iken, TKIP ise isteğe bağlıdır.

CCMP, şifreleme algoritması olarak AES'i (Advanced Encryption Standart) kullanır. AES, simetrik anahtar kullanılan, güvenilir ve hızlı bir algoritmadır. AES'in bir çok kullanım modu bulunmaktadır. CCMP içinde olan kullanım modları şunlardır;

- Counter mode (gizlilik amaçlı): Sayaç yönteminin kullanılma amacı, aynı veriyi içeren bloklar aynı şifre ile şifrelendiğinde farklı çıkışların olmasının istenmesidir. Zira, mesajın tekrar eden bloklardan oluştuğunun bilinmesi bir güvenlik zafiyetidir. Bu modda 128 bitlik şifreleme anahtarı kullanılır.
- CBC- MAC modu (bütünlük): MIC hesaplanmasında kullanılır. Eğer mesajda 1 bit değişirse, MIC'de büyük değişiklikler olur ve tahmin edilemez. MIC hesabı geri dönülmez bir şekilde yapıldığı için araya giren üçüncü şahısların, mesaja uygun bir MIC hesaplaması mümkün değildir.

CCMP çalışma yapısında öncelikle MIC hesabı için CBC-MAC (Cipher Block Chaninig - Message Authentication Code) kullanılır. Burada oluşan 128 bitin 64'ü kullanılır. Mesajın şifrelenmesinde de sayaçtan bir değer alınır ve AES algoritması ile şifrelenip daha sonra çıkan sonuç mesajın 128'lik ilk bloğu ile özel veya (EXOR) işleminden geçer. Daha sonraki bloklarda sayaç birer arttırılarak elde edilen sayılar ile şifrelenir.

2.4. Kablosuz Ağ Güvenlik Protokollerinin Karşılaştırılması

Kablosuz ağ güvenlik protokollerinin karşılaştırılması Tablo 1'de sunulmaktadır. WEP protokolü RC4 algoritmasını kullanırken, WAP TKIP/RC4 algoritmasını kullanmaktadır. RSN, CCMP/AES ve CCMP/TKIP algoritmalarını kullanır. WEP 40 bitlik şifreleme anahtarı kullanırken, WPA 128 bitlik anahtar kullanmaktadır. RSN ise daha güvenlikli 128 bitlik şifreleme anahtarı kullanır. WEP'deki IV 24 bit iken, WPA ve RSN'de 48 bittir. WEP'deki anahtar sabittir. WPA her oturum için anahtar değiştirirken RSN'de anahtar değişikliğine gerek yoktur. WEP anahtar yönetimi kullanmazken, WPA ve RSN 802.1x anahtar yöntemini kullanır. WEP'de asıllama yöntemi zayıftır. WPA ve RSN 802.1x EAP asıllama yöntemini kullanır. Veri bütünlüğü, WEP'de ICV ile, RSN ve WAP'da ise MIC ile sağlanır.

Tablo 1. WEP, WPA ve RSN Karşılaştırması

	WEP	WPA	RSN
Şifreleme	RC4 algoritması (Şifreleme yapısı kırılmıştır)	TKIP/RC4 (WEP'in açıklarını kapatıyor)	CCMP/AES CCMP/TKIP
Şifreleme Anahtarı	40 bit	128 bit	128 bit
IV	24 bit	48 bit	48 bit
Anahtar Değişikliği	Anahtar sabittir	Anahtarlar her oturum, her paket için değişir	Anahtar değişikliğine gerek yoktur
Anahtar Yönetimi	Anahtar yönetimi yoktur	802.1x	802.1x
Asıllama	Zayıf bir yöntem	802.1x EAP	802.1x EAP
Veri Bütünlüğü	ICV	MIC	MIC

Kablosuz ağlar için ilk olarak geliştirilen güvenlik protokolü WEP, artık etkin bir güvenlik önlemi olarak kabul görmemektedir. WEP esas alınarak geliştirilen ve açıklarını kapatan WPA ise, kırılmamış bir yapıya sahip olsa da RC4'ün zayıflıklarını taşımaktadır. Son olarak 2004 yılında tamamlanan RSN ise AES şifreleme algoritmasının gücü ile kablosuz ağlar için mevcut en etkin ve tercih edilen güvenlik önlemidir. Fakat, RSN ile düğümler üzerinde ciddi donanım ve yazılım değişiklikleri yapılması gereklidir.

3. KABLOSUZ ALGILAYICI AĞ GÜVENLİK PROTOKOLLERİ

Kablosuz algılayıcı ağlar (KAA'lar), klasik kablosuz ağlardan önemli farklılıklar içermektedir. Buna paralel olarak, KAA güvenlik ihtiyaçları ve bunların karşılanması amaçlarıyla literatürde ayrıca değerlendirilmektedir. KAA'lar için önerilen ve kullanılan güvenlik protokolleri bu bölümde ayrıntılı şekilde açıklanmaktadır.

3.1. LEAP

LEAP (Localized Encryption and Authentication Protocol), kablosuz algılayıcı ağlar için bir anahtar yönetim protokolüdür. LEAP, ağdaki pasif ortaklık gibi işlem tekniklerini desteklemek için tasarlanmıştır. Çoklu simetrik anahtarlama tekniklerini desteklemektedir [2].

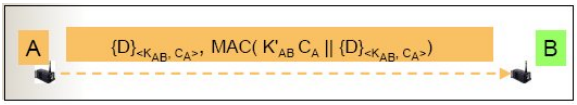
- Kişisel anahtarlar: Her düğüm benzersiz bir anahtara sahiptir. Bu anahtar, baz istasyonu ile çift yol paylaşımı yaparak güvenli haberleşmeyi sağlamaktadır.
- Paylaşımlı çift yol anahtarları: Her düğüm kendi komşularının her biri ile çift yollu anahtarı paylaşır. Bu anahtar ile güvenli bir iletişim sağlanır.
- Küme anahtarlar: Düğüm ile komşuları arasında paylaşılır. Küme anahtarlar güvenli yerel mesaj yayımları için kullanılır.
- Grup anahtarlar: Genel paylaşımlar için kullanılmaktadır. Baz istasyonu tarafından gurubun tamamına şifrelenmiş mesaj yayımlarında grup anahtarları kullanılmaktadır.

LEAP güvenlik protokolü çeşitli KAA uygulamalarında farklı güvenlik gereksinimlerini desteklemektedir. LEAP güvenlik protokolünde kullanılan anahtarlar, her bir düğümün haberleşmesini ve enerji verimliğini düzenlemektedirler. Baz istasyonu ile etkileşimi en aza indirir. Ağdaki pasif ortaklık ve yerel çakışma için düğümlerin uzlaşması gibi önemli işlem mekanizmalarını desteklemektedir. LEAP, kablosuz algılayıcı ağlardaki çoğu saldırıyı önleyebilir ya da azaltabilmektedir.

3.2. SNEP

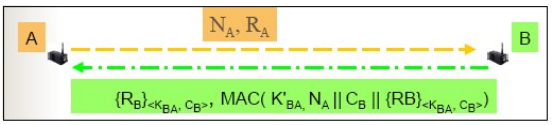
SNEP (Secure Network Encryption Protocol), kablosuz algılayıcı ağlarda güvenli veri iletimi için kullanılan bir protokoldür. SNEP güvenlik protokolünde veri iletimi şifrelenerek gerçekleştirilir [9], [7]. A ve B gibi iki algılayıcı düğüm arasında veri iletişimi yapılmak istendiğinde, veri mesajı şifrelenmektedir.

M = MAC(K_{MAC},C|E) formülü, MAC (Message Autentication Code) mesaj doğruluk kodudur. Bu formüldeki C paylaşım sayacı, E şifrelenmiş veri, K_{MAC} ise MAC anahtarıdır. A düğümünden B düğümüne veri gönderilmesi Şekil 1'deki formül ile ifade edilmektedir. Burada K_{AB}, A düğümümden B düğümüne şifre anahtarı K_{BA} ise B düğümünden A düğümüne şifre anahtarıdır. C_A A düğümündeki sayaç, C_B ise B düğümündeki sayaçtır. D mesajı, A düğümünden B düğümüne şifrelenmiş mesajı içermektedir.



Şekil 1. A düğümünden B düğümüne şifreli mesaj iletimi [7].

SNEP protokolünde sayaç güncellik açısından zayıftır; ancak, A düğümünün istek cevabında, B düğümünde oluşturulan mesaj görüntülenemez. Güçlü güncelliği sağlamak için "nonce" olarak adlandırılan sahte numara kullanmak gerekir. N_A, A düğümünden bir "nonce" ve R_A istek mesajı olarak düşünüldüğüne, yeni mesaj Şekil 2'deki gibi oluşmaktadır.



Şekil 2. A düğümünden B düğümüne mesaj iletimi ve B'den A'ya istek mesajı [7].

SNEP güvenlik protokolünün sağladığı önemli avantajlar bulunmaktadır. Algılayıcı düğümler birer sayaç içerirler. Sayaç, her blok ulaştığında bir artar, ancak iletim olmadığında durağandır. Düşük iletimde, her mesaja 8 bit eklenerek mesaj güçlendirilir. Güvenliği, ağı gizlice dinleyenlere karşı tam mesaj elde etmelerine izin vermeyerek sağlamaktadır. Veri doğruluğu MAC ile sağlanır. MAC'deki sayaç yardımıyla eski mesajlara cevap verilmesi önlenir. SNEP basit, efektif ve güçlü bir güvenlik protokolüdür ve bu yönüyle KAA'lar için bir çözüm olabilmektedir.

3.3. LISP

Sınırlı kaynaklı algılayıcı düğümlerden oluşan, büyük ölçekli kablosuz ağlarda güvenlik çözümlerini amaçlar. Çok sayıda algılayıcı düğümden oluşan ağları ölçeklemek için kümelere ayırmaktadır. Her küme için küme başı seçer ve anahtar sunucu oluşturur.

LISP (Lightweight Security Protocol) güvenlik protokolü yeni bir anahtarlama mekanizmasını içermektedir [6]. Anahtarlama yöntemini, küme başlarını ve anahtar sunucuları kullanarak uygulamaktadır. Bu yönteminin çeşitli avantajları şunlardır:

- ACK'ların gönderilmesini gerektirmeyen etkin anahtar yayını kullanır,
- Veri mesajına eklenmeksizin oluşturulan doğruluk bitlerini kullanır,
- Kaybolan anahtarları kurtarabilir,
- Veri şifreleme/çözme olmaksızın anahtar yeniler,

LISP, saldırılara karşı kritik bilgileri korumak için sağladığı faydalar ise şu şekilde özetlenebilir:

- Gizlilik, üçüncü şahısların ağı dinlediğinde, şifresiz metinlere ulaşmak yerine bu metinlerin

birden fazla şifrelenmiş metinlerine ulaşmaları ile sağlanır.

- Veri bütünlüğü, gönderilen verilerin değiştirilmesini engeller.
- Erişim kontrolü, ağa girişlerin kontrol edilmesiyle sağlanır.
- Anahtar yenileme, ağı tehlikeye atacak düğümlere karşı koruma sağlar.

LISP protokolü, güvenlikle beraber diğer servisleri de (yönlendirme, veri dağıtımı, konum) birleştirebilmektedir. LISP esnek ve enerji duyarlı bir protokoldür. Ayrıca ACK ve diğer kontrol paketlerine gerek duymadığından DoS [10] saldırılarına karşı oldukça güçlüdür.

3.4. Kablosuz Algılayıcı Ağ Güvenlik Protokollerinin Karşılaştırılması

Kablosuz algılayıcı ağ güvenlik protokollerinin karşılaştırılması Tablo 2'de sunulmaktadır. LEAP anahtar yönetimi için, SNEP şifreleyerek veri iletimi için, LISP ise büyük ölçekli ağlarda güvenlik için tasarlanmıştır. LEAP çoklu anahtarlama yöntemini kullanırken, LISP yeni bir anahtarlama yöntemini kullanmaktadır. Veri bütünlüğünü SNEP ve LISP protokolleri sağlarken, LEAP bu noktada yetersiz kalmaktadır. Veri gizliği SNEP ve LISP güvenlik protokollerinde mevcut iken LEAP güvenlik protokolünde yoktur. LEAP, düğümler arasında uzlaşma sağlayarak çakışmaları önleyebilir, ancak SNEP çakışmaları önleyemez. LISP protokolü ise ancak erişim kontrolü ile çakışmaları önleyebilmektedir. Enerji tüketimi açısından LEAP ve LISP protokolleri verimli iken SNEP kullanışsızdır. LEAP genel olarak saldırıları önleyebilir. SNEP, basit, güçlü ve efektif bir güvenlik protokolüdür. LISP ise esnek ve DoS saldırılarına karşı güçlü bir protokoldür.

Tablo 2. LEAP, SNEP,ve LISP Karşılaştırması

	LEAP	SNEP	LISP
Tasarlanma Amacı	Anahtar yönetimi	Şifreleyerek veri iletimi	Büyük ölçekli ağlar için güvenlik
Anahtarlama	Çoklu simetrik	Yok	Yeni anahtarlama mekanizması
Veri Bütünlüğü	Yok	Var	Var
Veri Gizliliği	Yok	Var	Var
Çakışma	Önlenir	Önlenemez	Önlenir
Enerji Verimliliği	İyi	Kötü	İyi
Avantajları	Saldırıları önler	Basit, güçlü ve efektiftir	Esnek ve DoS'a karşı güçlüdür

4. DEĞERLENDİRMELER

Kablosuz ağlar gezginlik, kolay kurulum, kullanım kolaylığı gibi özellikleri ile klasik eşleniklerinden ayrışmaktadır. Diğer taraftan, artan güvenlik gereksinimi, bu kablosuz iletişim türünde büyük önem arz etmektedir. Kablosuz ağlar için sunulan ilk güvenlik protokolü olan WEP, artık bir güvenlik önlemi olarak kabul görmemektedir. WPA ise, kırılmamış bir yapıya sahip olsa da RC4 algoritmasının zayıflıklarını taşımaktadır. Üçüncü ve önemli bir alternatif olan RSN, AES şifreleme algoritmasının sağladığı avantajlarla, mevcut en güçlü güvenlik önlemlidir. Bununla birlikte RSN ile cihazlar üzerinde ciddi donanım ve yazılım değişiklikleri yapılması gereklidir. Kablosuz algılayıcı ağlar için sunulan güvenlik protokollerinden LEAP saldırıları önleyebilirken, diğer önemli bir alternatif olan SNEP, basit, güçlü ve efektiftir, LISP ise esnek ve DoS saldırılarına karşı güçlü bir protokoldür.

KAYNAKLAR

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks", *IEEE Communication Magazine*, pages 102-114, August (2002).

[2] S. Zhu, S. Setia, and S. Jajodia, "LEAP – Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", Conference on Computer and Communications Security, 10th ACM, pp. 62 – 72, (2003).

[3] IEEE Std 802.11b-1999 and IEEE Std 802.11b-1999-Cor1-2001, Amendment to IEEE Std. 802.11-1999 Edition.

[4] IEEE P802.11i/D9.0, March 2004, Amendment to ANSI/IEEE Std. 802.11-1999 Edition as amended by IEEE Std. 802.11g-2003 and IEEE Std. 802.11h-2003.

[5] Borisov, Goldberg, Wagner "Intercepting Mobile Communications: The Insecurity of 802.11", 7th Annual International Conference on Mobile Computing and Networking, pp. 16-21, (2001).

[6] T. PARK, K. G. SHIN, "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks", ACM Transactions on Embedded Computing Systems, Vol. 3 (3), pp. 1-27, (2004).

[7] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *Mobile Computing and Networking,* Italy , (2001).

[8] A. Perrig, R. Canetti, D. Song, J.D. Tygar, "Efficient and Secure Source Authentication for Multicast", *Network and Distributed System Security Symposium (NDSS)*, (2001).

[9] H. Cam, S. Ozdemir, D. Muthuavinashiappan, P. Nair, “Energy-Efficient Security Protocol for Wireless Sensor Networks”, *IEEE VTC Fall 2003 Conference*, October, (2003).

[10] A. D. Wood, J. A. Stankovic, “Denial of Service in Sensor Networks”. Computer, Vol. 35 (10), pp. 54 - 62, (2002).