TASARSIZ AĞLARDA ELİPTİK EĞRİ ŞİFRELEME ALTYAPISI KULLANARAK ANAHTAR DAĞITIMI

Ömer Özgür Bozkurt

Bilgisayar Mühendisliği Bölümü
Elektrik-Elektronik Fakültesi
Yıldız Teknik Üniversitesi, 34349, Beşiktaş, İstanbul
e-posta: ozgur@ce.yildiz.edu.tr

Anahtar sözcükler:Tasarsız Ağlar, Eliptik Eğri Şifreleme, Eliptik Eğri Anahtar Değişimi,Güvenlik

ABSRACT

Security is one of the weaknesses of ad hoc networks. Symmetric cryptography is one of the solutions to overcome this weakness. However, keys used for symmetric cryptography are distributed before the motes are deployed and the same keys are used throughout the lifetime of the motes. In this study, a method that uses elliptic curve cryptography for distributing keys to be used for symmetric key cryptography among the motes is explained. The implementation and performance considerations are also discussed.

1. GİRİŞ

Tasarsız ağlar; doğal gözlem, sağlık durumunun gözlenmesi, acil sağlık desteği, araç takibi ve askeri uygulamalar benzeri ortamlarda kullanım için öngörülmektedir [1]. Bu ortamların tümünde de yetkilendirme, bütünlük, gizlilik ve güvenlik gereksinimlerinin farklı bileşimlerine ihtiyaç duyulmaktadır. Tasarsız ağlarda kullanılan cihazların sınırlı kapasiteleri mevcut güvenlik uygulamalarını bu tür ortamlar için uygulanamaz kılmaktadır. Bu tür cihazlar için, çok fazla işlem gücü ya da enerji gerektiren işlemler uygun olmadığından asimetrik şifreleme algoritmaları güvenliği sağlamak için kullanışlı gözükmemektedir. Asimetrik şifreleme, veri aktarım güvenliğinin sağlanması için kullanılamazken, simetrik şifreleme anahtarlarının dağıtılması için uygun bir çözüm olabilir.

2. TinyOS

Tasarsız ağın her bir cihazının taşıması gereken bir çok özellik bulunmaktadır. Belleğinin sınırlı olması, üzerinde çalışan yazılımın çok fazla tampon alan kullanamayacağı anlamına gelmektedir. Bu nedenle talep-yanıt ikilisi yerine yazılımın akışı işleyebilecek yapıda olması gereklidir. Maliyet ve enerji kısıtlamaları nedeniyle cihaz üzerinde bulunabilecek donanım sınırlıdır, dolayısıyla, yazılımın kısıtlı donanım kaynaklarına rağmen yoğun olarak gerçekleşen eş zamanlı işlemlere yanıt verebilmesi gerekmektedir. Tasarsız ağın oldukça farklı uygulamalar içi özelleşmiş cihazlardan oluşturması yüksek bir ihtimal olduğundan, cihazların işletim sistemlerinin bir birinden oldukça farklı uygulamaları destekleyebilmesi gerekmektedir. Son olarak, sistemin bütününün, bileşenlerindeki bir parçanın sorun çıkartması ya da arızalanması durumunda, işleyişine sorunsuz devam edebilmesi gerekmektedir.

Bu gereksinimleri karşılayabilmek için, Kaliforniya (Berkeley) Üniversitesinde, mikro-görevler destekleyen küçük bir işletim sistemi, TinyOS, tasarlanmıştır. TinyOS, eklenebilir programlardan oluşan, olay güdümlü bir işletim sistemidir. Kısıtlı donanım kaynaklarına rağmen çok sayıda eş zamanlı işlemi karşılamak üzere tasarlanmış, ve C dilinde geliştirilmiştir [2].

3. TASARSIZ AĞLARDA GÜVENLİK

Dinamik olarak değişen topolojisi, belirli bir alt yapının bulunmaması ve merkezi olmayan karakteri nedeniyle, tasarsız ağlarda güvenliğin sağlanması oldukça güçtür. Güvenlik, tasarsız ağ uygulamalarının her birinde gerçekleştirilmiş bir özellik olmak zorundadır [3]. Tasarsız ağlarda çok farklı uygulamalar olduğu dikkate alınırsa, ağların çok fazla açık noktası olduğu rahatça görülebilir. Bu açıkların bazıları aşağıda açıklanmıştır.

3.1. ZAYIF FİZİKSEL KORUMA

Klasik ağ uygulamalarında, düğümlerin fiziksel koruması genellikle oldukça kolay ve tam olarak gerçekleştirilebilir. Düğümler, yetkisiz kişilerin giremeyeceği korumalı ortamlarda bulunmaktadır. Öte yandan, tasarsız ağlarda, açık arazide bulunan bir düğümün kolayca ele geçirilebileceği aşikardır. Böyle bir düşmanca ortamda mükemmel bir fiziksel koruma sağlamak mümkün değildir. Tasarsız ağ

gerçekleştirimi sırasında cihazların güvenli bir ortamda bulunmadığı dikkate alınmak zorundadır.

3.2. SINIRLI OLANAKLAR

Tasarsız ağ cihazları; işlemci gücü, pil ömrü ve aktarım bant genişliği kaynakları başta olmak üzere sınırlı olanaklara sahiptir. Bu tür kısıtlı kaynaklar servis reddi saldırısına hedef olabilmektedir. İşlemci gücü ve aktarım bant genişliğine karşı servis reddi saldırısı, klasik ağlarda da çok yakından bilinmektedir. Tasarsız ağlarda cihazlar özellikle pil ömrünün tüketilmesi yoluyla servis reddi saldırılarına açık bulunmaktadır. Bir düğümün pilinin tüketilmesi, o düğümü sürekli devre dışı bırakmak anlamına gelmektedir.

3.3. BİRLİKTE İŞLEME ZORUNLULUĞU

Tasarsız ağda bulunan bir düğüme veri iletebilmek için diğer düğümlerin katılımı zorunludur. Tek bir amaca hizmet eden tasarsız ağlarda diğer düğümlerin katılımını sağlamak zor değildir, ancak, özellikle değişik kullanıcılara hitap eden karmaşık ağlarda, kullanıcıların bencilliklerinden dolayı (örneğin pil ömrünü uzatmak, vb. amaçlarla) birlikte işletimi sağlamak sorun olabilir. Bu durumda ağın işleyebilirliği ile kaynakların korunması arasında bir ikilem ortaya çıkmaktadır. Ağın her bir düğümünün işleyişe katkıda bulunmasının sağlanması gerekmektedir.

3.4. KABLOSUZ ORTAM ZAAFLARI

Kablosuz iletişim ortamında aktarılan verilere dışarıdan erişim, verinin bozulması, verinin değiştirilmesi, kablolu ortamlara göre çok daha kolay olmaktadır.

3.5. AĞ KATMANI SALDIRILARI

Tasarsız ağların dinamik değişen topolojisi nedeniyle, yol atamanın dinamik yapılması gerekmektedir. Bu durum hatalı yönlendirme, trafik sapması, yol güncellemeleri taşması, kara delik, gri delik ve solucan yuvası saldırıları gibi sorunları ortaya çıkarmaktadır [4].

Bir düğüm, bazı nedenlerden ötürü sadece belirli paketleri ya da sadece belirli düğümlere ait paketleri yönlendirmeyi gerçekleştirirken, diğerlerini reddedebilir. Daha da ötesinde diğer düğümlerin yol taleplerine verdikleri yanıtları değiştirerek tüm ağın genel performansının da düşmesine neden olan bu durum hatalı yönlendirme olarak adlandırılmaktadır.

Trafik sapması, zararlı bir düğümün yanıltıcı şekilde çekici yol duyuruları yaparak diğer düğümlerin paketleri kendi üzerinden göndermelerini sağlamasıdır. Saldırganlar bu yöntemi, bilgi toplamak, ağ yollarını etkilemek ve bazı paketlerin aktarımını önlemek için kullanabilir.

Kısa aralıklarla ağa yol güncellemeleri göndermek ağın aşırı yüklenmesine neden olabilir. Yol güncellemeleri taşmasına neden olan bu durum, servis reddi saldırılarının bir başka yöntemidir.

Kara delik saldırıları, hatalı yönlendirme ve trafik sapması saldırılarının birleşiminden oluşur. Belirli bir düğümün paketlerini ele geçirmek isteyen bir saldırgan yanıltıcı yol duyuruları ile bu düğüme en uygun yolun kendi üzerinden geçtiğini duyurur. Bu noktada pek çok düğüm en etkin yol olarak gördükleri için paketlerini bu düğüm üzerinden göndermeye başlayacaklardır. Araya giren düğüm bundan sonra kendine gelen paketleri atar.

Gri delik saldırıları, kara delik saldırılarının özel bir biçimidir. Araya giren düğüm paketlerin bazılarını seçici bir şekilde atarken bazılarının aktarımını sağlar.

Solucan yuvası saldırılarında, aralarında özel bir bağlantı olan birden fazla düğüm işin içindedir. Düğümlerden birisi aldığı paketi yönlendirmek yerine özel bağlantı üzerinden solucan yuvasının diğer ucuna gönderir ve diğer uçtaki düğüm paketi yeniden ağa bırakır. Bu şekilde paketlerin yönlendirilmesinde kısa devre yaratılmakta ve muhtemelen oldukça yoğun bir trafik yaratılmaktadır.

4. TASARSIZ AĞLARDA GÜVENLİK SAĞLAMA YAKLAŞIMLARI

Tasarsız ağ elemanları üzerindeki fiziksel kısıtlamalar, yüksek işlem gücüne sahip cihazlar üzerinde işlemek üzere tasarlanmış olan mevcut güvenlik algoritmalarının kullanımını olanaksız kılmaktadır. Örneğin, bir mote cihazının sahip olduğu bellek miktarı şifreleme algoritmalarının gerektirdiği parametreleri tutmak için bile yeterli olamamaktadır.

Önemli bir sorun da yetkilendirilmiş verinin tüm ağa yayınlanmasıdır. Yetkilendirilmiş yayın paketleri için mevcut öngörüler, tasarsız ağlar için kullanışlı olmaktan çok uzaktır. Öncelikle bu öngörüler, yetkilendirme için simetrik sayısal imza yöntemine dayanmaktadır. Kullanışlı olmamasının nedeni, her bir paket için 50 – 1000 bayt arası ek yük getiren yüksek iletişim yükü ve sayısal imzanın yaratılması ve doğrulanması için gereken işlem yüküdür.

Yayın yetkilendirilmesi ayrı bir sorun oluşturmaktadır. Tamamen simetrik çözümler bile asgari 300 bayt gerektirmektedir [Rohatgi imza yöntemi, 5].

Tasarsız ağ elemanlarının en önemli kısıtlaması, sınırlı enerji kaynağına sahip olmaları, her bir düğümün gerçekleştirebileceği işlem ve iletişimin düzeyini belirler. Enerji kullanımını asgari tutabilmek için güvenlik alt sisteminin işlemci üzerinde mümkün olduğunca az yük oluşturması ve aktarılan her bir mesaja eklediği bilginin asgari tutulması gerekmektedir. Öte yandan düğümlerin sınırlı

ömürleri, kullanılabilir anahtarların ömrünü de kısıtlamaktadır.

Tasarsız ağlarda veri güvenliği temel olarak TinyOS işletim sisteminin bir alt parçası olan TinySEC [6] tarafından gerçekleştirilmektedir. TinySEC, bir bağlantı katmanı şifreleme mekanizması sağlamaktadır. Çekirdeğini bir blok şifreleme ve anahtarlama mekanizması oluşturmaktadır. TinySEC mevcut olarak, bir grup düğüme dağıtılmış tek bir simetrik anahtar kullanmaktadır. Paket aktarımından önce her bir düğüm paketi şifreler ve veri bütünlüğünü sağlamak üzere bir mesaj yetkilendirme kodu (MAC) ekler. Alıcı bu kodu doğrulayarak mesajın bozulmadan geldiğini anlar ve şifresini çözer. TinySEC TOSSIM [7] benzetim ortamının yanı sıra mica ve mica2 cihazlarında çalışabilmektedir. TinySEC dört hedef göz önüne alınarak geliştirilmiştir; erişim kontrolü, bütünlük, gizlilik ve kullanım kolaylığı.

4.1. ERİŞİM KONTROLÜ

Sadece yetkili düğümler ağa katılabilirler. Yetkilendirilmiş düğümler, paylaşılan anahtara sahip olduğu varsayılarak iletişime dahil edilirler.

4.2. BÜTÜNLÜK

Bir ileti sadece aktarım sırasında değiştirilmemişse kabul edilmelidir. Bu şekilde araya girme saldırıları da önlenmiş olacaktır.

4.3. GİZLİLİK.

Yetkili olmayanların ileti içeriklerine erişmelerine olanak verilmemelidir.

4.4. KULLANIM KOLAYLIĞI

Ağ kullanıcılarının farklılıkları göz önüne alındığında kullanımının zor olmaması gerekmektedir.

5. ELİPTİK EĞRİ ŞİFRELEME

Eliptik Eğriler 1890lardan bu yana incelenmiş olmasına rağmen, kripto alanında kullanımı oldukça yenidir. ECC, Eliptik Eğri ayrık logaritma problemini temel almaktadır[8]. Şifreleme, gönderilecek verinin, eliptik eğri üzerindeki noktalarla eşlenmesi ile yapılmaktadır. Belirli bir sonlu alanı ifade eden birden çok eliptik eğri denklemi bulunabileceğinden, eğri denklemini bilmeksizin gönderilen iletinin açık halinin elde edilmesi mümkün değildir.

Eliptik eğri şifreleme iki farklı sonlu alan tanımlaması kullanmaktadır: asal sonlu alan olarak adlandırılan F_p (p asal) ve karakteristik 2 olarak adlandırılan F_2m (m>1)

5.1. ELİPTİK EĞRİ DİFFİE-HELLMAN

A ve B çiftinin, iletişim için bir gizli anahtar üzerinde anlaşmak istediklerini varsayalım. İlk olarak her ikisi açık olarak bir F_p (F_2m) sonlu alanı ve bu alan üzerinde eliptik eğri E belirlerler. Yine açık olarak E üzerinde rasgele bir nokta P belirlenir. A, gizli olarak bir tamsayı a seçer ve aP'yi hesaplar. Benzer şekilde, B, gizli olarak bir tamsayı b seçer ve bP'yi hesaplar. A ve B a ve b tamsayılarını gizli tutarken, aP ve bP açıklanır. A gizli a değerine, B gizli b değerine sahiptir. Hem A, hem de B abP'yi hesaplayabilmektedirler ve bu anlaşılmış ortak gizli anahtardır. Sadece P, aP ve bP verilmişken, abP'nin hesaplanmasının eliptik eğri ayrık logaritma problemini çözmeyi gerektirdiğine inanılmaktadır [8].

6. ELİPTİK EĞRİ ŞİFRELEME KULLANILARAK ANAHTAR DAĞITIMI

Mote cihazlarının sınırlı işlem gücü ve enerjileri göz önüne alındığında, asimetrik şifreleme; yetkilendirme, bütünlük, gizlilik ve güvenlik sağlamak için kullanılamaz durumdadır. Ancak, hareketli cihazlara anahtar dağıtımı için uygun gözükmektedir. Mevcut sistemlerde, simetrik şifreleme için anahtarlar cihazlara başlangıçta yazılmakta ve cihazların ömrü boyunca bu anahtarlar kullanılmaktadır. Bir şekilde anahtarların değiştirilmesi gerektiğinde, dağıtılmış cihazların toplanarak anahtarların yazılması gerekmektedir [8].

Tasarsız ağlarda, TinyOS, erişim kontrolü, yetkilendirme, bütünlük ve gizlilik sağlayabilmek için TinySEC kullanmaktadır. İleti yetkilendirme ve bütünlük kontrolü, ileti yetkilendirme kodlarıyla, gizlilik şifrelemeyle ve erişim kontrolü paylaşılan grup anahtarlarıyla sağlanmaktadır. TinySEC, bağlantı katmanında, 80 ikil (bit) simetrik şifreleme yapan SKİPJACK algoritması kullanmaktadır. Bu şekilde şifreli bir mesajın çözülmesi ortalama 2^{79} deneme gerektirmektedir. İlave olarak TinySEC tarafından kullanılan 4 bayt ileti yetkilendirme kodu, mesajın $1/2^{32}$ ihtimalle doğru kaynaktan geldiğini garanti etmektedir. TinyOS tarafından tanımlanmış olan CRC ve Grup kimliği alanları da TinySEC tarafından kullanılmaktadır. Bu şekilde 29 bayt aktarılacak veri için; TinyOS 36 bayt aktarırken, TinySEC 41 bayt aktarım yapmakta, bu şekilde yaklaşık % 14 ek yük getirmektedir. Ölçümler göstermektedir ki, TinySEC paket aktarım süresine ortalama 2ms (%3), paketin komşu düğüme gidiş dönüş süresine ise, ortalama 5 ms (%3) ek yük getirmektedir. TinySEC paket geribildirim başarımını saniyede 0,28 paket azaltabilmektedir [9].

TinySEC işletim sırasında yaklaşık 8 KB (yaklaşık 7 KB program ve 1 KB veri) bellek alanı gerektirmektedir ki; bu bellek miktarı özellikle 4 KB RAM ve 128 KB ROM içeren mica2 cihazları için sorun yaratan bir miktar değildir.

Tasarsız ağlarda kullanılan cihazların ömrü genellikle enerji kaynaklarının ömürleriyle sınırlı olduğu için, cihazların fiziksel güvenliğini sağlamak anlamlı gözükmemektedir. Böyle bir ortamda düğümleri oluşturan cihazların birisinin ele geçirilerek bir şekilde kullandığı simetrik şifre anahtarının ele geçirilmesi, tüm ağın kullandığı anahtarın ele geçirilmesi anlamına gelmektedir. Her hangi iki düğüm arasında farklı simetrik anahtarlar kullanımı, tüm ağın güvenliğinde oldukça yükselen bir güvenlik sağlayabilmektedir, ancak bu durumda, ağı oluşturan n cihaz varsa, her bir cihaza n^2 tane 80 ikil anahtarın yazılması gerekir ki, tasarsız ağ cihazlarında bu düzeyde bir verinin tutulması olası bile değildir. Bu durumda çözüm TinySEC tarafından desteklenmekte olan anahtar değiştirebilme seçeneğinin değerlendirilmesinde yatmaktadır. Gizli simetrik anahtarların dağıtılması ise, tüm cihazları toplayıp işleme imkanının olmadığı düşünülecek olursa ancak asimetrik şifreleme yöntemleri ile olabilecektir.

Bu yöntemler arasında en uygulanabilir olanı Diffie-Hellman anahtar değişimi algoritması olarak ortaya çıkmaktadır. Diffie-Hellman anahtar değişimi protokolünün tasarsız ağlara uyarlanmış bir varyasyonu, istasyondan istasyona (STS – station to station) protokolü [10] sorunsuz bir şekilde asimetrik şifreleme kullanımına olanak sağlamaktadır. Buradaki sıkıntı, 80 ikil simetrik şifreleme tarafından sağlanan güvenlik düzeyinin altına düşmeden anahtarların dağıtılmasıdır. Bahsedilen düzeyde güvenlik ise ancak 1024 ikil asimetrik şifreleme kullanarak sağlanabilmektedir. 8 ikil işlemci kullanan cihazlarda 1024 ikil değerler üzerinde asgari 160 ikil üssel işlemler yapmak kabul edilebilir sınırların çok üzerindedir. Bu noktada 1024 ikil güvenlik düzeyini 163 ikil ile sağlayabilen ECC çok daha mantıklı bir çözüm olarak karşımıza çıkmaktadır.

7. GERÇEKLEŞTİRİM

Yukarıda açıklananlar ışığında, TOSSIM benzetim ortamında işlemek üzere NIST tarafından tavsiye edilen F_{2^p} eğrileri [11] kullanılarak Diffie-Hellman anahtar değişimi ile tasarsız ağlarda anahtar dağıtımı işlemi gerçekleştirilmiştir. F_{2^p} eğrileri kullanılmasının nedeni matematiksel işlemlerin kaydırma yoluyla yapılmasına daha yatkın olması nedeniyle, kod iyileştirmesine daha yatkın bulunmasından kaynaklanmaktadır. F_p eğrileri kullanan gerçekleştirimin kodlaması da tamamlanmış, ancak henüz en iyileştirme tamamlanmadığından kabul edilebilir sonuçlar elde edilememiştir. Gerçekleştirim; işletim esnasında yaklaşık 35 KB bellek gerektirmektedir. Bunun yanında gizli anahtar üretimi yaklaşık 400ms, ortak anahtar üretimi yaklaşık 58 saniye almaktadır. Kod üzerindeki performansa yönelik iyileştirme çalışmaları halen devam etmektedir.

8. SONUÇ

Tasarsız ağlarda eliptik eğri şifreleme kullanılarak, cihazların dağıtımı sırasında verilen simetrik anahtarların gerektiğinde değiştirilebilmesi için anahtar dağıtımının mümkün olduğu gösterilmiştir. Bu şekilde tasarsız ağ cihazlarının ömürleri boyunca tek bir anahtara tabi olarak işlemelerinin önüne geçilmesi, özellikle güvenliğin kritik olduğu uygulamalarda ihtiyaç duyulan güvenliğin olanaklı olduğu gösterilmiştir. Bundan sonraki aşamada F_p eğrileri kullanan gerçekleştirimin en iyileştirmesi tamamlanarak sonuçlar karşılaştırılacaktır.

9. KAYNAKLAR

[1] I.F. Akyıldız, W. Su, Y. Sankarasubramaniam, E. Çayırcı. Wireless Sensor Networks: A Survey. Computer Networks. Elsevier Science 38:393-422. 2002

[2] TinyOS Documantation. http://www.tinyos.net/tinyos-1.x/doc/

[3] Y. Zhou, Z. Haas. Securing ad hoc Networks. IEEE Network. 1999.

[4] E.M. Royer, C.K. Toh, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications. Nisan 1999

[5] P. Rohatgi. A Compact and Fast Hybrid Signature Scheme for Multicast Packet Authentication 6th ACM Conference on Computer and Communicaitons Security. Kasım 1999.

[6] TinySEC User Manual. http://www.tinyos.net/tinyos-1.x/doc/tinysec.pdf

[7] P. Levis, N. Lee. TOSSIM: A Simulator for TinyOS Networks. Manual. 2003.

[8] A. Menezes, P. Van Oorschot ve S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996

[9] C. Karlof, N. Sastry, D. Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. ACM Conference on Embedded Networked Sensor Systems (SenSys 2004).

[10] W. Diffie, P. C. van Oorschot, M. J. Wiener, Authentication and Authenticated Key Exchanges. Designs, Codes and Cryptography, 2, 107-125 (1992) Kluwer Academic Publishers.

[11] NIST. Recommended Elliptic Curves For Federal Government Use. http://csrs.nist.gov/CryptoToolkit/dss/ecds/NISTReCur.pdf 1999.