Kümeleme tabanlı kablosuz algılayıcı ağların kara delik ve seçici yönlendirme saldırıları altında kayıp paket analizi

İpek Abasıkeleş Turgut[2], Cansu Canbolat[*1]

[1,2]*İskenderun Teknik Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği, Hatay*

Özet

Günümüzde Kablosuz Algılayıcı Ağlar (KAA) sağlık izlemeden askeri takip sistemlerine kadar çeşitli alanlarda sıklıkla kullanılmaktadır. Düşük güç ve kolay kurulum avantajlarının yanında çözülmesi gereken kendisine özgü problemleri bulunmaktadır. Kablosuz iletim ortamının saldırıya açık doğası ve bu ağlardaki düğümlerin kaynak kısıtları KAA'da güvenlik problemleri için özel çözümlerin üretilmesine neden olmaktadır. Ağdan başarılı bir şekilde veri toplanmasını engelleyen ve kriptolojik yöntemlerle yakalanamayan iç saldırılar en tehlikeli saldırı gruplarındandır. Bu çalışmada yönlendirme katmanı iç saldırılarına dahil olan kara delik ve seçici yönlendirme saldırılarının farklı ağ alanları altında modellenmesi çalışması yapılmıştır. Simülasyonlar sonunda elde edilen sonuçlar kara delik saldırılarının %43'e, seçici yönlendirme saldırılarının ise %28'e varan oranda ortalama paket kayıplarına neden olduğu ve ağ alanı arttıkça yaşanan kayıpların daha da arttığını göstermektedir.

Anahtar Kelimeler: Kablosuz algılayıcı ağlar, Performans değerlendirmesi, Yönlendirme atakları.

Analysis of packet loss under black hole and selective forwarding attacks for cluster-based wireless sensor networks

Abstract

Nowadays, Wireless Sensor Networks (WSNs) are widely used in various fields ranging from health monitoring to military monitoring systems. Besides the advantages of low power requirement and easy deployment, it has unique problems that have to be solved. The open nature of the wireless transmission environment and the resource constraints of the sensor nodes in WSNs results in special solutions for security problems. Insider attacks are the most dangerous types of attacks that prevent successful data collection from the network and can not be captured by traditional cryptographic methods. In this study, black hole and selective forwarding attacks, which are included in the routing layer internal attacks, is modelled and performed under different network sizes. The results obtained from the simulations show that average packet loss rates are up to 43% of black hole attacks and 28% of selective routing attacks, and that the loss rate increases as the network size increases.

Keywords: Wireless sensor networks, Performance evaluation, Routing attacks.

[*]Sorumlu yazar (Corresponding author): İpek Abasıkeleş-Turgut, *ipek.abasikeles@iste.edu.tr*

1. Giriş

Bir Kablosuz Algılayıcı Ağ(KAA), fiziksel dünya ile etkileşimde bulunmak amacıyla ortama yerleştirilmiş çok sayıda küçük boyutlu, sınırlı kapasiteli, kısa mesafeli vericiye sahip, düşük güçlü ve düşük maliyetli algılayıcı düğümden oluşur [1]. Genellikle güvenilir olmayan alanlara rastgele yerleştirilen KAA'daki düğümler, fiziksel dünyadan aldıklarını sanal dünyaya taşırlar. Çoğunlukla durağan olan algılayıcı düğümler belirli bir alana yerleştirildikten sonra çevreyi gözetler ve bir olay algıladıklarında rapor oluşturarak bu raporu kablosuz kanal aracılığı ile bir merkeze (genellikle bir baz istasyonu) iletirler. KAA 'lar askeri uygulamalardan, sağlık, ev aletleri yönetimi ve habitat izlemeye kadar oldukça geniş bir yelpazede başarı ile kullanılmaktadır.

Algılayıcı düğümlerin küçük boyutlarda olması, düşük maliyet ve az güç tüketimi gibi avantajlarının yanında KAA'larda güvenlik, kısıtlı enerjinin verimli bir şekilde kullanılması, lokalizasyon vb. birçok problemin çözülmesi gerekir [2]. KAA yapısını oluşturan düğümlerin kısıtlı kaynaklara sahip olması ve düşman sahalar gibi zorlu şartlar altında konumlandırılmaları, iletim kanalları ve algılayıcı düğümler arasındaki iletişimin çeşitli saldırılara açık olmasına neden olmaktadır. Bununla birlikte KAA'ların işlemci ve radyo kapasitelerinin düşük olması geleneksel güvenlik protokollerinin bu ağlarda uygulanmasına olanak tanımaz. Bu nedenle güvenlik alanında KAA'lara özel kapsamlı çalışmalar yapılması gerekmektedir [3].

KAA'lara yapılan saldırılar iç ve dış saldırılar olmak üzere iki temel grupta toplanır. Dış saldırıların tespiti için kriptolojik çözümler ve yetkilendirme protokolleri başarılı sonuçlar vermektedir [4]. Bununla birlikte ağda gerekli yetkileri, anahtarları veya şifreleri ele geçirmiş bir kullanıcının içeriden yapacağı bir saldırı için bu yöntemler maalesef etkili olamamaktadır [4]. Bu nedenle iç saldırılara yönelik olarak literatürde kriptolojik olmayan çeşitli çözümler önerilmiştir. En tehlikeli iç saldırılar grubuna dahil olan yönlendirme ataklarında kötü niyetli bir düğüm tarafından ele geçirilen normal düğümler, bilgilerin ağın dışına aktarılmasına, hedefe hiç aktarılmamasına veya eksik aktarılmasına neden olarak tüm ağı tehlikeye sokabilir [5]. Bu atakların önlenebilmesi/yakalanabilmesi ve uzaklaştırılabilmesi için saldırıların davranışlarının iyi bir şekilde analiz edilmesi gerekmektedir.

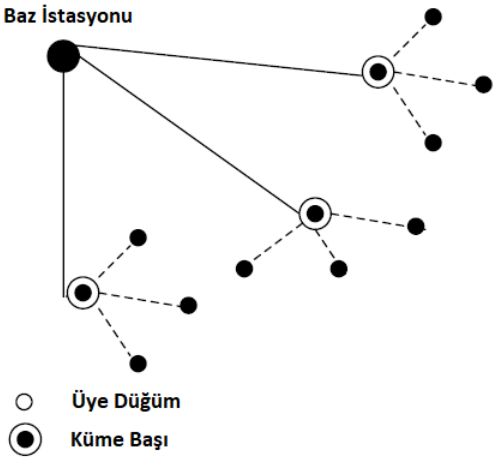
Bu çalışmada yönlendirme saldırıları grubuna dahil olan seçici yönlendirme ve kara delik saldırılarının kümeleme tabanlı bir KAA'ya verdiği zarar, paket kayıp oranları üzerinden değerlendirilmiştir. Farklı ağ büyüklükleri için yapılan simülasyonlarda önceden belirlenen bir saldırgan düğümün küme başı olarak seçilmesi ve paket iletimini sabote etmesi sağlanmıştır. Bu durumda ağ üzerinde saldırıya ve ağın büyüklüğüne bağlı olarak %8.26 ile %42.97 arasında paket kayıp oranları yaşandığı gözlemlenmiştir.

Bölüm 2'de kullanılan materyal ve yöntemler açıklanmıştır. Bölüm 3'te elde edilen sonuçlar analiz edilmiş, son bölüm olan Bölüm 4'te ise makale sonuçlandırılmıştır.

2. Materyal ve yöntem

2.1. Kümeleme mimarisi

Büyük ölçekli KAA' lar, genellikle binlerce / on binlerce algılayıcı düğümün bir araya gelmesinde oluşur. Bu ağlarda ölçeklenebilirlik problemi için kümeleme tabanlı yönlendirme mimarilerinin kullanılması etkili bir çözümdür [6]. Kümeleme yapısında komşu düğümler bir küme oluşturmak üzere birleştirilir. Bir küme başı (cluster head - CH) bu kümeyi yönetmek amacıyla belirlenen bir yönteme göre seçilir. Kümeleme tabanlı KAA'lar, Şekil 1'de görüldüğü gibi küme başı, üye düğümler ve baz istasyonu olmak üzere üç temel elemandan oluşur. Baz istasyonu, küme başının, üye düğümlerden toplayıp kendisine gönderdiği veriyi değerlendirmekle görevli iken; küme başı kendisine bağlı olan üye düğümlerden veri toplama ve bu veriyi baz istasyonuna iletmede görevlidir. Üye düğümler ise yerleştirildikleri ortamda bir olay algıladıkları zaman bağlı oldukları küme başına algılanan veriyi yollamadan sorumludur. Kümeleme yapısı sayesinde algılayıcılar, düşük enerji tüketimi ile daha kapsamlı bir algılama sağlayabilir ve aralarındaki koordinasyonu gerçekleştirebilirler [7].



Şekil 1. Küme tabanlı KAA mimarisi

Bu çalışmada kümeleme tabanlı yönlendirme mimarisi olarak literatürde çoğunlukla baz alınan LEACH [8] protokolü kullanılmıştır. Tamamen dağıtık küme oluşumunu öneren LEACH protokolü enerji tüketimini minimize etmek için küme başı rolündeki düğümlerin rasgele, ağdaki diğer düğümlerden tamamen bağımsız ve dönüşümlü olarak belirlenmesini sağlar. Böylece ağdaki yük dağıtımını paylaştırır. First Order Radio Model (FORM) olarak adlandırılan radyo modelini kullanan algoritmada, ölçeklenebilirliği artırmak amacıyla yerelleştirilmiş düğüm koordinasyonu kullanılır ve baz istasyonuna iletilen veri miktarını ve dolaylı olarak iletimde harcanacak enerjiyi minimize etmek için veri birleştirme işlemi gerçekleştirilir.

2.2. Yönlendirme saldırıları

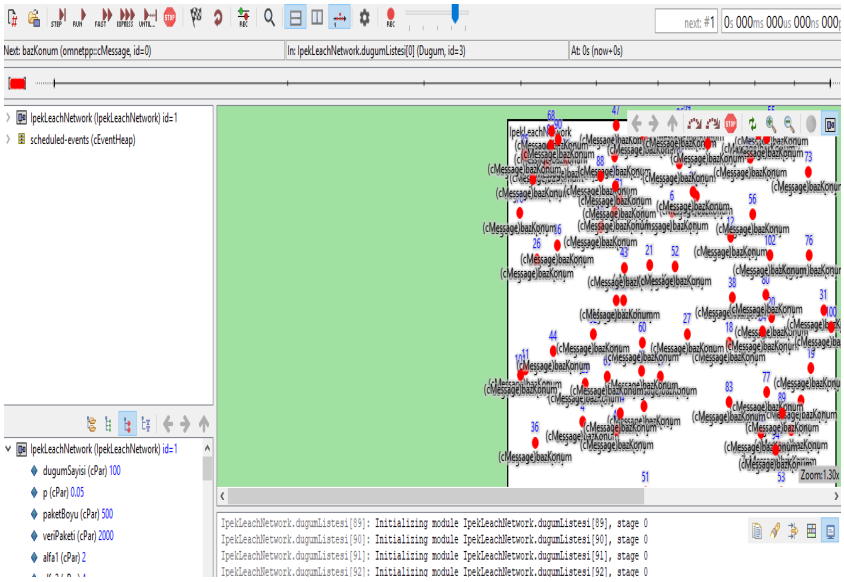
Yönlendirme saldırıları, KAA'ların ağ katmanında paket / veri iletimini sabote etmeye yönelik olarak gerçekleştirilen saldırılardır. Obruk (sinkhole), kara delik (blackhole), gri delik (gray hole), solucan deliği (wormhole), seçici yönlendirme (selective forwarding) gibi çeşitli saldırılar bu grup altında toplanır. Bu çalışmada kara delik ve seçici yönlendirme saldırıları modellenmiştir [9].

Kara delik saldırısında saldırgan düğüm, kendisine ulaşan paketlerin tamamını bloke ederek hedefe iletimini engellerken; seçici yönlendirme saldırısında paketlerin bir kısmını bloke edip, bir kısmını geçirir [10]. Her iki saldırı da baz istasyonunda veri kaybına neden olup, ağdan sağlıklı bilgi toplanamaması sonucunu doğurur. Bu saldırılara karşı literatürde çok sayıda öneri sunulmuştur [4]. Saldırılara karşı alınacak önlemleri tasarlamadan önce saldırıların davranışlarının ve ağa verdiği zararların belirlenmesi gerekmektedir.

Bu çalışmada farklı ağ alanları için kara delik ve seçici yönlendirme saldırıları modellenmiştir. Kullanılan modelde ağdaki düğümler içinden bir tanesi (id numarası 4 olan düğüm) saldırgan olarak seçilmiş ve başlangıç enerjisi diğer düğümlerin 2 katı olacak şekilde ayarlanmıştır. Bu düğüm her 5 döngüde bir kendisini küme başı olarak seçerek etrafındaki düğümlerin verilerini kendisine iletmesini sağlamış ve ardından bu verileri ya hiç iletmemiş (kara delik) ya da yarısını iletmiştir (seçici yönlendirme).

2.3. Simülasyon çatısı

Bu çalışmada modellenecek olan kümeleme tabanlı KAA yapısı ve iç saldırılar için simülasyon yöntemi kullanılacak olup; nesneye yönelik ve modüler yapıda bir ayrık olay ağ benzetim programı olan OMNeT++ [11] kullanılmıştır. Şekil 2'de görüldüğü gibi OMNeT++, çeşitli çalışmaların modellenmesi için kullanıma hazır bir takım haberleşme ağlarını içermekle birlikte kullanıcının kendi ağının simülasyonu için de temel modüller sağlar.



Şekil 2. OMNeT ağ simülasyon programı

KAA'larda güvenlik sorunlarının beraberinde enerjinin yönetimi de çözülmesi gereken önemli bir problemdir. KAA'ların yapısını oluşturan algılayıcılar, enerjilerini sınırlı bir ömre sahip olan pillerden alır. Çoğunlukla bu cihazların bataryalarının ortama yerleştirildikten ve devreye alındıktan sonra değiştirilmesi mümkün olmamaktadır. Bu da KAA'larda enerjinin verimli bir şekilde kullanılması zorunluluğunu beraberinde getirir [12]. Enerjiyi verimli bir şekilde kullanabilmek için literatürde çok sayıda yönlendirme protokolü önerilmiştir [6]. Yönlendirme mimarisi düz ve hiyerarşik olmak üzere iki gruba ayrılır. Tüm düğümlerin aynı fonksiyonellik ve sorumluluklara sahip olduğu düz mimariler, küçük ölçekli ağlarda görece olarak iyi bir performans sergilese de geniş ölçekli ağlarda kaynak kısıtlamaları nedeniyle efektif değildir. Bununla birlikte düğümlerin farklı rollere sahip olduğu hiyerarşik mimarilerde kümeleme işlemi sayesinde enerjinin verimli bir şekilde düğümler arasında dağıtılması sağlandığı için KAA'nın ömrü daha uzun süreli olmaktadır [6].

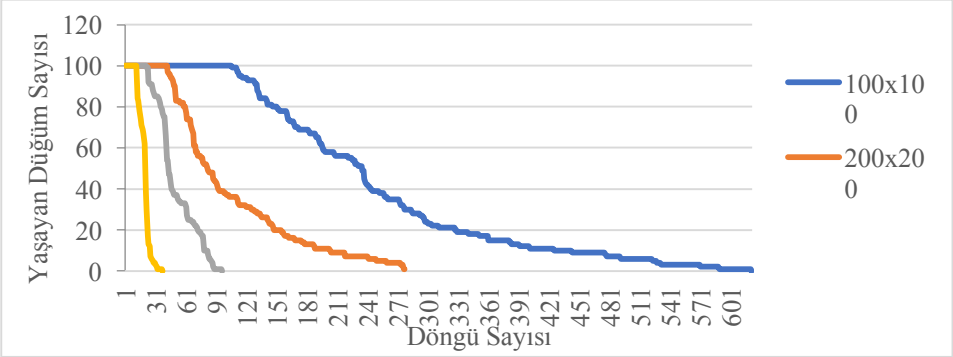
Gerçeklenen simülasyonlarda kullanılan parametreler Tablo 1'de görülmektedir. 100 x 100, 200 x 200, 300 x 300 ve 400 x 400'lük alanlarda 100 düğüm rasgele olarak dağıtılmıştır. Bir düğümün küme başı olma olasılığı %5'tir. Ancak, saldırgan düğüm 5 döngüde 1, küme başı olarak kendisini seçer. Düğümlerin başlangıç enerjileri 0.25 Joule, kontrol paket boyutu 500 bayt ve data paketi boyutu 2000 bayttır. Baz istasyonu (10, 10) konumunda yer almaktadır.

Tablo 1. Simülasyon Parametreleri

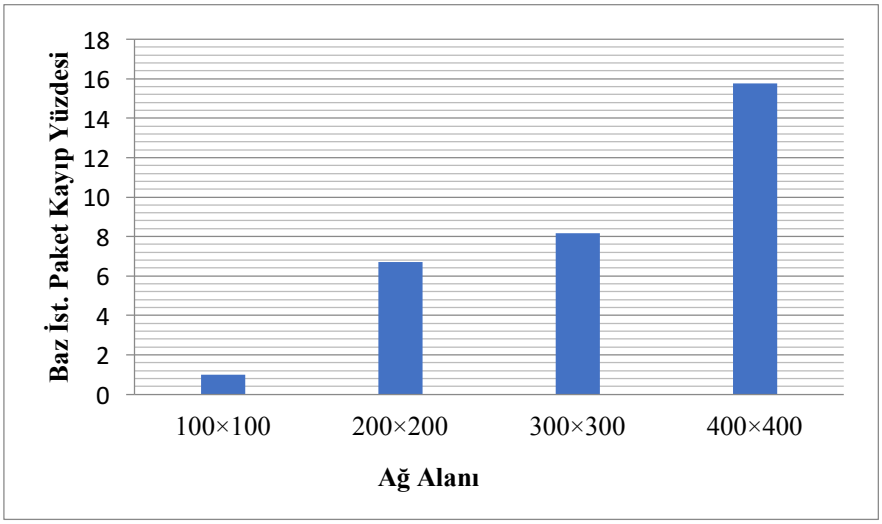
Parametre Adı	Değeri
Düğüm Sayısı	100
Küme Başı Olma Olasılığı	0.05
Veri Boyu	2000 Bayt
Kontrol Paket Boyu	500 Bayt
Düğümlerin Başlangıç Bataryası	0,25 Joule
Saldırganın Başlangıç Bataryası	0,5 Joule
Ağ Alanı	100x100, 200x200, 300x300, 400x400
Bazın Konumu	(10,10)
Saldırgan Sayısı	1
Saldırganın Görülme Sıklığı	5 döngüde 1

3. Bulgular ve tartışma

Şekil 3'te ve Şekil 4'te sırasıyla 100 x 100, 200 x 200, 300 x 300 ve 400 x 400 boyutunda ağ alanına sahip kümeleme tabanlı bir KAA üzerinde saldırının olmadığı durumda döngü başına yaşayan düğüm sayısı ve ağ yaşam süresi sonunda baz istasyonundaki ortalama paket kayıp oranları görülmektedir. Ağ yaşam süresi, sistemdeki son düğümün bataryasının tükendiği döngüdür. Baz istasyonundaki ortalama paket kaybı hesaplanırken, öncelikle her döngünün başında algılayıcı düğümler tarafından üretilen toplam paket sayısından, döngü sonunda baz istasyonuna ulaşan toplam paket sayısı çıkarılır. Ardından ağ yaşam süresi boyunca her döngü alınan bu farkların ortalaması alınır.



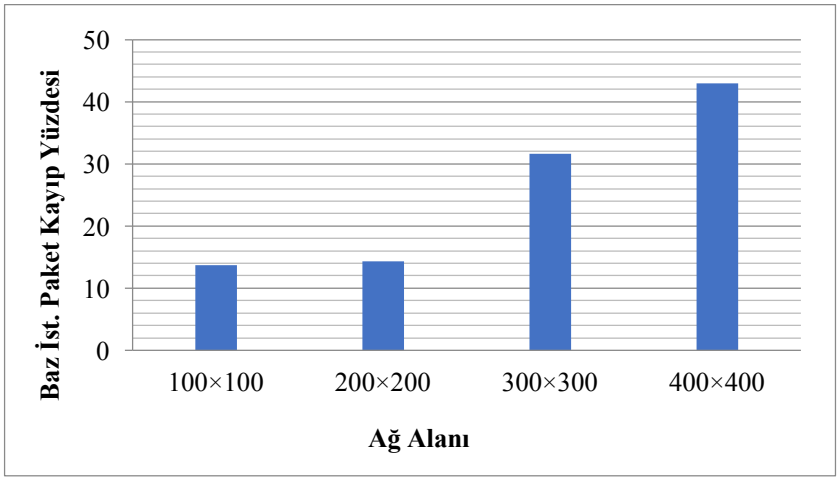
Şekil 3. Saldırının olmadığı durumda döngü başına yaşayan düğüm sayısı



Şekil 4. Saldırının olmadığı durumda ağ yaşam süresi sonunda baz istasyonundaki ortalama paket kayıp yüzdesi

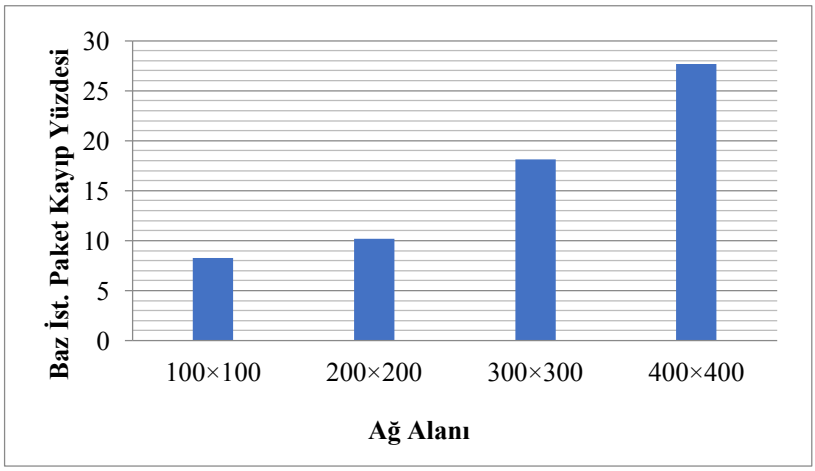
Şekil 3'te görüldüğü üzere ağ alanı arttıkça düğümlerin yaşam süreleri azalmaktadır. Bunun sebebi düğümlerin verilerini daha uzak mesafeler boyunca iletmeye çalışmaları ve bu amaçla daha yüksek oranda batarya harcamalarıdır. Sistemde saldırı olmadığı durumda dahi (Şekil 4) paket kayıpları yaşanmaktadır ve ağ alanı arttıkça paket kayıpları daha da artmaktadır. En iyi durumda (100 x 100 ağ alanında) ağda yaşanan paket kaybı önemsenmeyecek derecede az iken (%1); en kötü durumda (400 x 400) bu değer %15 seviyesini geçmektedir. Bunun nedeni düğümlerin batarya kısıtlarından dolayı verilerini başarılı bir şekilde baz istasyonuna iletememeleridir. Sadece saldırı olması durumu değil, küme başının bataryasının tükenmesi durumu da veri kayıplarına neden olan önemli faktörlerden biridir. Ağ alanı arttıkça daha uzak mesafelere iletim yapmak zorunda olan küme başlarının bataryalarının döngü tamamlanmadan bitmesi, baz istasyonuna verilerin ulaşamamasına neden olmaktadır.

Şekil 5 ve Şekil 6'da ise sırasıyla 100 x 100, 200 x 200, 300 x 300 ve 400 x 400 boyutunda ağ alanına sahip kümeleme tabanlı bir KAA üzerinde kara delik ve seçici yönlendirme ataklarının modellenmesi sonrasında elde edilen ağ yaşam süresi sonunda baz istasyonundaki ortalama paket kayıp oranları görülmektedir.



Şekil 5. Kara delik saldırısı altında ağ yaşam süresi sonunda baz istasyonundaki ortalama paket kayıp yüzdesi

Kara delik saldırısı ağ alanından bağımsız olarak her durumda, beklenildiği gibi, paket kaybına neden olmuştur. Saldırganın küme başı olarak topladığı paketleri iletmemesi baz istasyonunda verilerin eksik toplanmasına neden olmaktadır. Bununla birlikte ağ alanı arttıkça kara delik saldırısından kaynaklanan paket kayıp oranları daha da artmaktadır (Şekil 5). En iyi durumda (100 x 100) bile %13.69 oranına paket kaybı yaşanırken, en kötü durumda (400 x 400) bu sayı %42.97 değerine ulaşmıştır.



Şekil 6. Seçici yönlendirme saldırısı altında ağ yaşam süresi sonunda baz istasyonundaki ortalama paket kayıp yüzdesi

Kara delik saldırısına benzer şekilde seçici yönlendirme saldırılarında da ağ alanı arttıkça ortalama paket kayıpları artmaktadır. Bununla birlikte paket kayıp oranları en iyi durumda %8.26 iken, en kötü durumda %27.64'tür. Bu değerlerin kara delik saldırısından daha az olmasının nedeni paketlerin tamamının değil, sadece bir kısmının iletilmemesidir.

Bu çalışmanın sonunda elde edilen sonuçlar, sadece tek bir saldırganın olduğu durumda dahi hem kara delik hem de seçici yönlendirme ataklarının her durumda ağda kabul edilemeyecek seviyede yüksek oranlarda paket kayıplarına neden olduğunu göstermektedir. Bu bağlamda bu çalışma gelecekte yapılacak olan saldırı tespit, saldırı önleme veya güvenli yol oluşturma çalışmalarına ışık tutacaktır.

4. Sonuç

KAA'larda yönlendirme yolunu bozmaya yönelik olarak uygulanan ağ katmanı iç saldırıları, algılayıcıların, ortamdan algıladıkları verileri baz istasyonuna iletmesini sabote ederek ağdan sağlıklı veri toplanmasını engellerler. İç saldırıları yakalama, engelleme veya güvenli yol kurma üzerine literatürde çeşitli çalışmalar mevcuttur. Ağdaki saldırıları uzaklaştırmak ve/veya onlardan korunmak amacıyla daha başarılı önlemler alınması ve/veya çözümler sunulması için öncelikle saldırıların ağa verdiği zararın incelenmesi gerekmektedir.

Bu çalışmada kara delik ve seçici yönlendirme ataklarının ağa verdiği zararı incelemek için 1 saldırgan düğümün kümeleme tabanlı KAA mimarisinde 5 döngüde 1, küme başı olarak seçilmesi sağlanmış ve etraftan topladığı paketleri iletmeyerek veya yarısını ileterek ağa verdiği zarar izlenmiştir. Farklı ağ boyutları için tekrarlanan simülasyonlarda ağda %8 ve %43 arasında değişen oranlarda ortalama paket kayıplarının yaşandığı gözlemlenmiştir. Tek bir saldırganın dahi ağa verdiği zarar boyutu düşünüldüğünde bu saldırılara yönelik çalışmaların önemi açıkça görülmektedir. Gelecek çalışmada, güvenli yol kurulması sayesinde enerji efektif bir şekilde iç saldırılardan korunma hedeflenmektedir.

Kaynakça

[1] Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. The Journal of supercomputing, 68(1), 1-48.

[2] Sharma, S., Bansal, R. K., & Bansal, S. (2013, December). Issues and challenges in wireless sensor networks. In Machine Intelligence and Research Advancement (ICMIRA), 2013 International Conference on (pp. 58-62). IEEE.

[3] Jan, M. A. (2016). Energy-efficient routing and secure communication in wireless sensor networks (Doctoral dissertation).

[4] Singh, S. K., Singh, M. P., & Singh, D. K. (2011). A survey on network security and attack defense mechanism for wireless sensor networks. International Journal of Computer Trends and Technology, 1(2), 9-17.

[5] Sedjelmaci, H., Senouci, S. M., & Feham, M. (2012, July). Intrusion detection framework of cluster-based wireless sensor network. In Computers and Communications (ISCC), 2012 IEEE Symposium on (pp. 000857-000861). IEEE.

[6] Singh, S. P., & Sharma, S. C. (2015). A survey on cluster based routing protocols in wireless sensor networks. Procedia computer science, 45, 687-695.

[7] Tohma, K., Aydın, M. N., & Turgut, İ. A. (2015, May). Improving the LEACH protocol on wireless sensor network. In Signal Processing and Communications Applications Conference (SIU), 2015 23th (pp. 240-243). IEEE.

[8] Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on (pp. 10-pp). IEEE.

[9] Kalita, H. K., & Kar, A. (2009). Wireless sensor network security analysis. International Journal of Next-Generation Networks (IJNGN), 1(1), 1-10.

[10] Roosta, T., Shieh, S., & Sastry, S. (2006, December). Taxonomy of security attacks in sensor networks and countermeasures. In The first IEEE international conference on system integration and reliability improvements (Vol. 25, p. 94).

[11] Varga, A., & Hornig, R. (2008, March). An overview of the OMNeT++ simulation environment. In Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops (p. 60). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[12] Alippi, C., Anastasi, G., Di Francesco, M., & Roveri, M. (2009). Energy management in wireless sensor networks with energy-hungry sensors. IEEE Instrumentation & Measurement Magazine, 12(2).