Academic Platform Journal of Engineering and Science

journal homepage: http://apjes.com/

Gerçek-Zamanlı Kablosuz Algılayıcı Ağlarda Toplama Ağacı Protokolü Üzerinde Yönlendirme Saldırılarının Modellenmesi ve Saldırı Tespit Sistemi Tasarımı

[1]Çağlar Oflazoglu, *[2]İpek Abasıkeleş-Turgut
[1]Hatay Mustafa Kemal Üni., Fen Bilimleri Enstitüsü, Enformatik Ana Bilim Dalı, Hatay, Türkiye, caglar.oflazoglu@iste.edu.tr,
[2]İskenderun Teknik Üni., Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü, Hatay, Türkiye, ipek.abasikeles@iste.edu.tr,

Araştırma Makalesi Geliş Tarihi: 10.09.2019 Kabul Tarihi: 02.03.2020

Öz

Kablosuz Algılayıcı Ağlar (KAA), günümüzde IoT sistemlerin kullanımlarının artması ile birlikte önem kazanan konulardan birisi haline gelmiştir. KAA'yı oluşturan düğümlerin sınırlı kaynaklara sahip olması ile birlikte kablosuz ortamın saldırılara açık olan doğası, bu ağlarda çeşitli güvenlik sorunlarını da beraberinde getirmektedir. Veri paketinin kaynaktan hedefe doğru yönlendirilmesi aşamasında içeriden yapılan saldırılarda kriptolojik ve/veya kimlik doğrulama tabanlı çözümler başarılı olamadıkları için bu saldırılara yönelik farklı çözümlerin üretilmesi gerekmektedir. Bu çalışmada, gerçek zamanlı KAA'da çıkış deliği, kara delik ve seçici yönlendirme saldırılarını içeren bir grup yönlendirme saldırıları test ortamı üzerinde modellenmiştir. Son yıllarda literatürde popüler bir yönlendirme mimarisi olan CTP protokolü üzerinde 3 çeşit yönlendirme saldırısının gerçek zamanlı olarak modellenmesi ve ardından komşu izleme tabanlı bir saldırı tespit sisteminin gerçek zamanlı olarak tasarlanarak test edilmesi bu çalışmanın yenilikçi yönünü oluşturmaktadır. Ayrıca bu çalışmanın, CTP üzerinde saldırıların gerçek zamanlı davranış modellerini şekillendirmesi açısından gelecekte tasarlanacak olan saldırı tespit ve saldırı yanıt sistemleri için temel oluşturacağı düşünülmektedir.

Anahtar Kelimeler: Kablosuz Algılayıcı Ağlar, Toplama Ağacı Protokolü, Yönlendirme Saldırıları, Gerçek Zamanlı Test Ortamı.

Modelling Routing Attacks on Collection Tree Protocol and Designing an Intrusion Detection System on Real-Time Wireless Sensor Networks

[1]Çağlar Oflazoglu, *[2]İpek Abasıkeleş-Turgut
[1] Hatay Mustafa Kemal University, Graduate School of Natural and Applied Sciences , Department of Informatics, Hatay, Turkey, caglar.oflazoglu@iste.edu.tr
[2] İskenderun Technical University, Faculty of Engineering and Natural Sciences, Department of Computer Engineering, Hatay, Turkey, ipek.abasikeles@iste.edu.tr

Abstract

Nowadays, Wireless Sensor Networks (WSNs) have become one of the important issues with the increasing usage of IoT systems. The nodes having limited resources in WSNs and the nature of wireless environment, which is vulnerable to attacks, bring along various security problems. Since cryptologic and / or authentication-based solutions are not successful for insider attacks during the travelling of data packet from source to destination, different solutions should be proposed. In this study, a group of routing attacks, including sinkhole, black hole and selective forwarding attacks in real time WSNs, are modelled and analysed on testbed. The contributions of this study are real-time modelling of 3 different types of routing attacks on CTP protocol, which is a popular routing architecture in literature in recent years, and the design and testing of a real time neighbour tracking-based intrusion detection system from these attacks. Besides, this study is thought to be the basis for future intrusion

*Sorumlu Yazar: İskenderun Teknik Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü, Hatay ipek.abasikeles@iste.edu.tr, +90-326-613-5600

Doi: 10.21541/apjes.617854

detection and intrusion response systems that will be designed in the future in terms of shaping real-time behaviour models of attacks on CTP.

Keywords: Wireless Sensor Networks, Collection Tree Protocol, Routing Attacks, Real Time Testbed.

1. GİRİŞ

Kablosuz Algılayıcı Ağlar (KAA), fiziksel ortamdan algıladıkları veriyi kablosuz ortam aracılığıyla genel bir merkeze ileten çok sayıda küçük algılayıcı düğümden oluşur. Düşük güçte çalışan ve düşük işlem kapasitesine sahip bu küçük düğümlerin, düşük maliyet ile uygulama kolaylığı KAA'nın bilim ve teknolojinin birçok alanında kullanılmasına olanak tanır. KAA, sağlık hizmetleri ve askeri gözetleme gibi, bireylerin aktivite ve davranışlarından bilgi toplanması; deprem, hava kirliliği, su kalitesi gibi çevresel olayların takip edilmesi; bina güvenliği, imalat makine performansı gibi endüstriyel tesislerin izlenmesini içeren oldukça geniş bir yelpazede kullanım alanına sahiptir [1]. Bununla birlikte, kablosuz kanalın tüm dinleyicilere açık olması, algılayıcı düğümlerin kısıtlı kaynaklara sahip olması ve genelde sabit bir altyapı olmaksızın zor koşullar altında konumlandırılması KAA'yı dışarıdan ve içeriden gelecek saldırılara karşı savunmasız hale getirir. Bu nedenle bu ağlarda güvenlik, çözülmesi gereken önemli bir problem halini alır [2].

KAA konusunda yapılan araştırma ve geliştirmeler kapsamlı, tekrarlanabilir ve doğrulanabilir bir değerlendirme sürecini gerektirir. KAA alanında yapılan en eski çalışmalar, değerlendirme amacıyla kullanılacak olan araç ve platformlarının eksikliğinden dolayı genellikle teorik analizler üzerine yoğunlaşmaktadır. Ancak, günümüzde KAA işletim sistemleri, geliştirme araçları, benzetim platformları ve hatta gerçek zamanlı donanımlar mevcuttur. Günümüzde KAA üzerine yapılan çalışmaların büyük bir çoğunluğu kolay bir yöntem olması nedeniyle simülasyon yöntemini tercih etmektedir. Bununla birlikte, teorik analizlerin ve simülasyon ortamının belirgin ve güvenilir olması, gerçek KAA uygulamalarının güvenilmez ve belirsiz doğası ile örtüşmemektedir. Ayrıca dağıtık uygulama mantığının, paylaşılan bir ortam üzerinden çevresel ve radyo iletişimi gibi problemlerin birebir benzetiminin yapılması oldukça zordur. Sonuç olarak teorik analizler ve simülasyonlar sadece bir bakış açısı sunan yaklaşımlar olabilirler. Bu sebeplerden dolayı son yıllarda KAA'nın gerçek zamanlı test ortamları üzerinden değerlendirilmesi popüler hale gelmiştir [3].

Gerçek zamanlı KAA'da güvenlik problemlerine karşı sunulan çözümlerin bir kısmı kriptolojik çözümlerdir [4-8]. Dışarıdan gelen saldırılara karşı ağı korumada başarılı olan kriptolojik ve kimlik doğrulama yaklaşımları, ele geçirilen ve içeriden saldırmaya başlayan düğümlerde maalesef etkili olamamaktadır. İç saldırılar, özellikle yönlendirmeyi bozmaya yönelik olduklarında verinin kaybı ve bozulması gibi zararlara neden olmaktadır [9]. İç saldırılara karşı yapılan çalışmalar temelde iki grup altında toplanır: saldırı tespit sistemleri ve güven tabanlı yol kurma. Saldırı tespit sistemlerinde amaç, saldırıların yakalanması ve ağdan uzaklaştırılması iken; güvenli yol kurulumunda**,** saldırı tespiti yerine verinin güvenilir bir yol üzerinden hedefe ulaşması amaçlanır. Zhan ve arkadaşları [10], yönlendirme mesajlarının tekrarlanması yoluyla yapılan çıkış deliği, solucan deliği ve sahte baz istasyonu ataklarına karşı güven tabanlı bir yol kurulması önerisinde bulunmuştur. Sultana ve arkadaşları [11] ise saldırıların gerçekleşmeden önce önlenmesi ve yakalanan saldırıların sistemden uzaklaştırılması için çeşitli çözümler sunmuştur. Önerdikleri algoritmaları veri değiştirme, seçici yönlendirme ve çıkış deliği saldırıları için gerçek zamanlı olarak test etmişlerdir. Bir başka çalışmada ise [12], kümeleme mimarileri için saldırı tespit mekanizması önerilmiş ve çeşitli yönlendirme ataklarına karşı gerçek zamanlı olarak test edilmiştir.

KAA'nın test ortamında gerçeklenmesinin zorluğu nedeniyle literatürde az sayıda bulunan gerçek zamanlı güvenlik çalışmaları, genellikle önerdikleri algoritmaları test etmek amacıyla literatürde tanımı yapılmış olan bir veya birkaç saldırı çeşidini modellemişlerdir [9, 10, 12]. Ancak bu çalışmalarda saldırıların ne şekilde modellendiği konusunda ayrıntılı ve açık bir bilgi yer almamaktadır. Gerçek hayattaki uygulamalarda ise savunma sistemleri, saldırıların gerçekleşmesinin ardından geliştirilir. Bu nedenle güvenlik sistemi tasarımında saldırıların ne şekilde modellendiği, davranışlarının ne olduğu oldukça önem arz eder.

Bu çalışmada son yıllarda popüler olan CTP yönlendirme protokolünü kullanan gerçek zamanlı bir KAA yapısı üzerinde çeşitli yönlendirme saldırıları modellenmiştir. Bu saldırıların tanımlarından yola çıkılarak çeşitli modeller oluşturulmuş; tasarlanan her bir model için sistemin aldığı zararlar analiz edilmiş ve bu analiz sonuçları çerçevesinde komşu tabanlı izleme sistemi üzerine kurgulanmış bir saldırı tespit sistemi önerilmiştir. Yapılan bu çalışmanın gelecekte tasarlanacak olan savunma sistemlerine ışık tutması amaçlanmaktadır.

Bölüm 2'de literatürde CTP için geliştirilen güvenlik önlemleri; Bölüm 3'te ise yönlendirme mimarisinin tanıtılması, test ortamının açıklanması ve modellenen saldırıların tanımları yer almaktadır. Deneysel çalışma ve elde edilen bulgular Bölüm 4'te tartışılmış, Bölüm 5'te ise komşu tabanlı saldırı tespit sistemi tasarımı gerçeklenmiştir. Çalışmanın son bölüm olan Bölüm 6'da makalenin sonuçları yer almaktadır.

2. BİLİMSEL YAZIN TARAMASI

Literatürde CTP üzerinde yapılan güvenlik çalışmalarının çoğu simülasyon yöntemini kullanmaktadır.

Peter vd. [13], TOSSIM simülatörü kullanarak CTP ve ısıya dayanıklı modüller içeren algılayıcı düğümler için geliştirilen güvenli-CTP protokolünün performans analizini yapmışlardır. Stetsko vd.[14], simülasyon yöntemi kullanarak CTP protokolü üzerinde modelledikleri seçici yönlendirme, taşma saldırısı ve yayın bozma saldırıları için komşu izlemeye dayalı saldırı tespit sistemi geliştirmişlerdir. Liu vd. [15], gerçek zamanlı KAA için hatalı çalışan düğümleri (ölü veya saldırgan düğümleri) ağdan izole etmeyi amaçlayan, zaman senkronizasyonuna dayalı, güvenlik iş birliği toplama ağacı protokolü (SC-CTP) adında bir model önermişlerdir. Udhayavani vd. [16] yaptıkları çalışmada enerji verimli ve güven tabanlı bir model önerisi sunmuş ve modelin simülasyon sonuçlarını paylaşmışlardır. Çalışmada yönlendirme protokolü olarak CTP'ye ilişkin sonuçlar da yer almaktadır. Almon vd. [17] , CTP üzerinde yayın bozma ve kara delik saldırılarının davranışlarını lojistik regresyon ile test etmişler ve bölgesel bir saldırı tespit sistemi geliştirmişlerdir. Cui ve Yang [18], analitik model kullanarak davranışını analiz ettikleri seçici yönlendirme atağı için reaktif bir yönlendirme şeması geliştirmişlerdir. Bu şemayı simülasyon yöntemi kullanarak CTP üzerinde modellemişlerdir. Ioannou ve Vassiliou'nun [19] yaptıkları çalışma, bu makaleye konu ve kapsam olarak en çok benzeyen çalışmadır. Ağ katman saldırılarının KAA üzerindeki etkilerini incelemek amacıyla TelosB düğümlerinin modellendiği COOJA simülatörü kullanılarak çıkış deliği, kara delik ve seçici yönlendirme saldırıları modellenmiştir. Yönlendirme alt yapısı olarak Ağırlıklandırılmış En Kısa Yol (Weighted Shortest Path (WSP)) algoritması kullanılmıştır. Yönlendirme saldırılarının davranışları ve modelleri, yönlendirme mimarisine doğrudan bağlı olduğu için bu çalışma, CTP protokolü için uygun değildir. Ayrıca COOJA simülatörü her ne kadar gerçeğe yakın bir emülatör olsa da fiziksel fenomenlerin modellenmesinde yetersiz kalmaktadır [20]. Bu nedenle ancak gerçek zamanlı uygulamalar üzerinde saldırıların modellenmesi ile doğru sonuçlar elde edilebilecektir.

3. MATERYAL VE YÖNTEM

3.1. Yönlendirme Mimarisi

Bu çalışmada, yönlendirme altyapısı olarak, literatürde son yıllarda gerçek zamanlı KAA'da popüler olan Toplama Ağacı Protokolü (Collection Tree Protocol- CTP) [21] kullanılmıştır. CTP, ağda yer alan düğümleri en düşük maliyet ile ağaç hiyerarşisi üzerinden baz istasyonuna bağlar. Ağdaki her bir düğüm Beklenen İletim Sayısı (Expected Transmission Count, ETX) olarak adlandırılan bir parametre üzerinden kendisi ve baz istasyonu arasındaki rotanın maliyetini hesaplar [22].

ETX, belirli bir sürede gönderilen ve iletilen paket sayıları ile sonraki paketler için hesaplanan bir başarı olasılık değeridir. ETX değerlerinin belirlenmesinde, öncelikle ağaç hiyerarşisinin en tepesinde yer alan baz istasyonuna Eşitlik (1)'de görüldüğü üzere sabit bir değer verildikten sonra ($ETX_{kök}$) (varsayılan olarak sıfır), baz istasyonuna komşu olan düğümler (ağacın 1.seviye yaprakları) bağlantılarının kalitesine göre kendi ETX değerlerini Eşitlik (2)'ye göre hesaplar. Ardından ağaç hiyerarşisinde yer alan diğer düğümler kendi ETX değerlerini ($ETX_{düğüm}$) hesaplarken hiyerarşide ebeveyn adı verilen bir üst seviyede yer alan komşularının ETX değeri ile ($ETX_{ebeveyn}$) kendisi ve ilgili komşusu arasındaki bağlantının maliyetini ($ETX_{bağlanti}$) toplar. Bu şekilde ETX hesaplaması ağacın alt kademelerine doğru ilerler. Bir düğümün ETX değerini hesaplayabilmesi için üst seviye komşularının ETX değerlerini bilmesi gerekir. Bu amaçla CTP, düğümlere ETX değerlerini işaret çerçevesi içerisinde kapsama alanına yayınlamasını önerir. Böylece hiyerarşide alt seviyelerde yer alan düğümler kendi ETX değerlerini hesaplayabilirler.

$$ETX_{kök}=0 \quad (1)$$

$$ETX_{düğüm}=ETX_{ebeveyn}+ ETX_{bağlanti} \quad (2)$$

Komşu sayısının fazla olması durumunda düğümler, seçecekleri güzergahları belirlerken en düşük ETX ile bağlantı kurabilecekleri komşuyu seçerek ETX değerlerini minimize etmeye çalışırlar.

3.2. Yönlendirme Saldırıları

Çıkış deliği saldırısında (sinkhole attack) saldırgan düğüm, yönlendirme paket trafiğini kendi üzerinden geçirmek için sahte kontrol paketleri yayarak etrafındaki sıradan düğümleri aldatır [23]. Saldırgan bu yöntem ile paketlerin izlenmesi, değiştirilmesi ve iletimi konularında yetki kazanmış olur.

Kara delik saldırısında (blackhole attack) saldırgan düğüm, kendisine iletilmek üzere gönderilen paketlerin tamamını bloke ederek bir sonraki düğüme iletimini engeller ve böylece ağda veri kaybına yol açar [24].

Seçici yönlendirme saldırısında (selective forwarding attack) saldırgan düğüm, kara delik saldırısından farklı olarak kendisine gelen paketlerin belli bir bölümünün sonraki düğüme iletilmesini sağlarken bir kısmını bloke eder [25]. Bu saldırıda da kara delik saldırısına benzer şekilde veri kayıpları yaşanmaktadır.

3.3. Test Ortamı

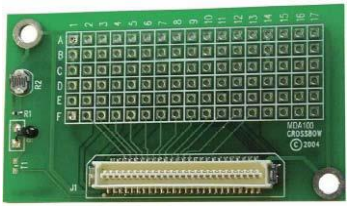
Bu çalışmada MEMSIC firması tarafından üretilen 2.4 GHz IEEE 802.15.4 IRIS algılayıcı düğümleri kullanılarak gerçek zamanlı bir KAA yapısı oluşturulmuştur. Kullanılan düğüme ait bileşenler, ana modül, algılayıcı modülü ve ağ geçidi olmak üzere 3 parçadan oluşmaktadır.

IRIS Ana Modülü, Şekil 1'de görüldüğü üzere düğümün ana bileşenlerinin üzerinde bulunduğu modüldür. Modül üzerinde Atmel ATmega 1281 8 bit mikrodenetleyici bulunmaktadır. Kullanılan düğümlerin teknik özellikleri

Tablo 1'de verilmiştir. Düşük güç tüketimine sahip olan bu modül 2.4 GHz IEEE 802.15.4 kablosuz bileşenini de kendi üzerinde barındırmaktadır. Modül, 2xAA pil haricinde farklı yöntemlerle de beslenebilmektedir.

Şekil 1. IRIS Ana Modülü

Şekil 2'de görülen algılayıcı modülü bir geliştirme modülü olup sıcaklık, ışık vb. algılayıcıların ana modüle eklenmesini sağlamaktadır.



Şekil 2. IRIS Algılayıcı Modülü

Ağ geçidi modülü (Şekil 3), ana modülün programlanması ve USB üzerinden seri haberleşme gibi ihtiyaçların karşılanması amacıyla kullanılmaktadır. Bu çalışmada Raspberry Pi 3 Model B+ Plus isimli iki mini bilgisayara Linux tabanlı Raspbian Stretch Lite işletim sistemi kurulmuş ve Java tabanlı uygulamalar ile baz istasyonu olarak kullanılan düğüm ve 1. seviye düğümden ağ geçidi modülü ile alınan veriler SQLite veri tabanında zaman bilgisi de kullanılarak depolanmıştır.

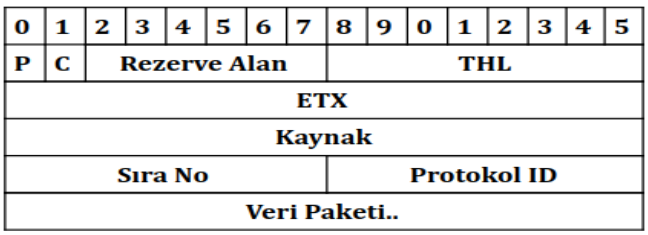
Şekil 3. IRIS Ağ Geçidi Modülü

3.4. Sistem Paketleri

CTP yönlendirme protokolünde; Şekil 4'te ve Şekil 5'te veri paketi, Şekil 6'da ise yönlendirme paketi olmak üzere iki türde paket yapısı bulunmaktadır [21].

Tablo 1. 2.4 GHz IEEE 802.15.4 IRIS Düğüm Teknik Özellikleri

İşlemci/Radyo Kartı	**XM2110CA**	**Açıklama**
İşlemci Performansı		
Program Flash Belleği	128K bayt	
Seri Flash	512K bayt	100.000 Ölçüm
RAM	8K bayt	
Konfigürasyon EEPROM	4K bayt	
Seri İletişim	UART	0-3V iletim seviyesi
ADC	10 bit ADC	8 kanal, 0-3V giriş
Diğer Arayüzler	Digital I/O,I2C,SPI	
Çekilen Akım	8 mA / 8 µA	Aktif mod / uyku modu
RF Alıcı-Verici		
Frekans Bandı	2405 MHz - 2480 MHz	ISM bandı
Veri İletim Oranı	250 kbps	
RF Gücü	3 dBm (typ)	
Alıcı Hassasiyeti	-101 dBm (typ)	
Komşu Kanal Reddi	36 dB 34 dB	+ 5 MHz kanal aralığı - 5 MHz kanal aralığı
Dış Mekan Kapsama Alanı	>300 metre	¼ dalga dipole anten, LOS
İç Mekan Kapsama Alanı	>50 metre	¼ dalga dipole anten, LOS
Çekilen Akım	16 mA 10 mA 13 mA 17 mA	Alıcı Modu TX, -17 dBm TX, -3 dBm TX, 3 dBm
Elektromekanik		
Batarya	2X AA pil	
Harici Güç	2.7 V - 3.3 V	
Kullanıcı Arayüzü	3 LED	Kırmızı, Yeşil ve Sarı
Boyut (mm)	58 x 32 x 7	
Ağırlık (gram)	18	Batarya hariç



Şekil 4. CTP Veri Paketi Çerçevesi

Veri paketi çerçevesi, verinin sonraki düğüme iletilmesi için kullanılan bir paket formudur. Bu paket formu içeriğinde; "P" adı verilen yönlendirme bitini; "C" adı verilen tıkanıklık bitini; "THL" olarak adlandırılan yaşam süresini; "ETX" olarak adlandırılan rota maliyetini; "Kaynak" adı verilen iletimi yapan düğümün kimlik bilgisini; "Sıra No" olarak adlandırılan kaynağın sıra numarasını, "Protokol ID" adı verilen protokol tanımlayıcısını ve "Veri Paketi" olarak düğümün göndermek istediği veri bloğunu içermektedir.

Veri paketi içeriği isteğe bağlı olup ihtiyaçlara uygun şekilde tasarlanabilmektedir. Bu çalışmada algılayıcı düğümün yapmış olduğu ölçüm değerlerinin yanı sıra baz istasyonuna iletilmek istenen çeşitli bilgiler de Şekil 5'te görüldüğü üzere bu paketin içeriğine eklenmiştir.

Baz istasyonuna iletilmek istenen paket içeriğinde yer alan "Hedef", iletilecek düğümün kimlik bilgisini; "Kaynak", gönderici düğümün kimlik bilgisini; "Paket No", gönderilen paketin benzersiz sıra numarasını; "ETX", gönderim için seçilen düğümün rota maliyetini; "Güç", batarya gücünü; "Sıcaklık", algılayıcı ile ölçülen ortam sıcaklık değerini ve "Işık Şiddeti" ise algılayıcı ile ölçülen ortam ışık şiddeti değerini temsil etmektedir.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
Hedef								Kaynak							
Paket No															
ETX															
Güç															
Sıcaklık															
Işık Şiddeti															

Şekil 5. Veri Paketi İçeriği

Son olarak Şekil 6'da görülen yönlendirme paketi içeriğindeki P ve C bitleri ve rezerve alan kısmı, veri paketi çerçevesi ile aynı amaçla kullanılmaktadır. ETX bilgisi ve hedef düğüm bilgisi de yönlendirme çerçevesine dahil edilmiştir.

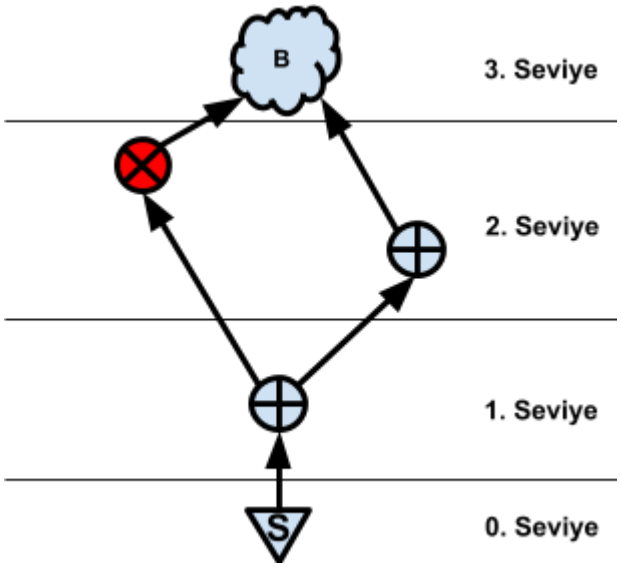
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5
P	C	Rezerve Alan						Hedef							
Hedef								ETX							
ETX															

Şekil 6. CTP Yönlendirme Paketi Çerçevesi

4. DENEYSEL SONUÇLAR

Bu makalede CTP'nin işleyişini engellemeye yönelik olarak içerisinde çıkış deliği, kara delik ve seçici yönlendirme saldırılarını da içeren bir yönlendirme saldırı kümesinin modelleme çalışması yapılmıştır. Öncelikle saldırıların literatür tanımlarından yola çıkılarak, gerçek zamanlı CTP üzerinde farklı modeller tasarlanmıştır.

Deneyde kullanılan topoloji; Şekil 7'de görüldüğü gibi 3 ara düğüm, 1 algılayıcı düğüm ve 1 baz istasyonu olmak üzere toplam 5 kablosuz algılayıcı ağ aygıtından oluşmaktadır. Bu aygıtlar, bir bina içinde farklı odalarda önceden belirlenmiş noktalarda birbirlerine 6-10 metre arası mesafe olacak şekilde konumlandırılmıştır. Konumlar belirlenirken topolojiye uygun olarak düğümlerin birbirlerinin kapsama alanı içerisinde yer alması sağlanmıştır. Tüm düğümlerin konumları sabittir ve ağ süresi boyunca değişmemektedir. Algılayıcı düğümün veri iletiminde, iki seviyeli düğüm geçişi üzerinden baz istasyonuna ulaşılması hedeflenmiştir. 1. seviyede yer alan ara düğüm, algılayıcı düğümden aldığı ve baz istasyonuna iletilmek istenen veriyi 2. seviyeye aktarmaktadır. 2. seviyede yer alan iki ara düğüm ise kendilerine iletilen veriyi baz istasyonuna ulaştırmakla görevlendirilmiştir. Her seviyede yer alan düğümler, bir önceki ve bir sonraki seviyede yer alan düğümlerin komşusudur (yani kapsama alanı içerisinde bulunmaktadır).



Şekil 7. Test Ortamı Düğüm Yerleşimi

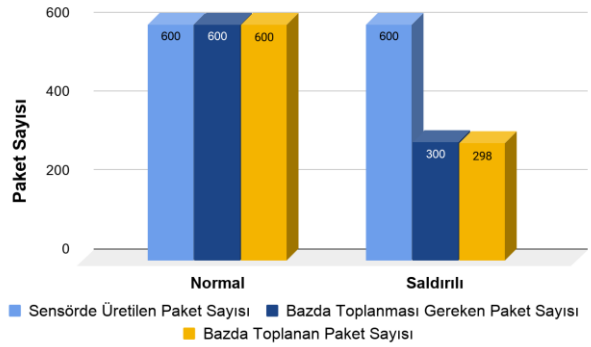
Yapılan deneylerde; temel oluşturması açısından tasarlanan saldırısız modele ait istatistikler, sistemin yaklaşık olarak 10 dakika (600 veri paketi için) çalıştırılması sonucunda elde edilmiştir. 0. seviyede yer alan algılayıcı düğüm yapmış olduğu sıcaklık, ışık şiddeti vb. ölçümleri saniyede 1 kez veri paketi olarak 1. seviyede yer alan düğüme iletmektedir. 1. seviyeye iletilen paketler veri yolu kalitesi dikkate alınarak 2. seviyeye, oradan da baz istasyonuna iletilmektedir.

4.1. Saldırı-1: Çıkış Deliği + Seçici Yönlendirme

Deneyde kullanılan topolojide 2. seviyede yer alan yönlendirici düğümlerden birinin saldırgan olarak görev yapması sağlanmıştır. Bu düğüm; ilk olarak çıkış deliği saldırısı düzenleyerek düğümün gerçek ETX değerini daha düşük bir sahte değerle değiştirir ve böylece 2. seviyeye iletilen trafiğin kendi üzerine alınmasını sağlar. CTP'de sistemde döngü oluşmaması için her seviye geçişinde ETX değeri belirli bir minimum eşik değerinin üzerinde artmaktadır. Tasarlanan sistemde bu değer 10 olmasına

rağmen, saldırgan düğüm bu sayıyı 1 göstererek trafiği kendi üzerine çekmeyi başarır. Ardından trafiği oluşturan paketler, önceden belirlenen sabit bir oranda, bir sonraki düğüme iletilerek seçici yönlendirme saldırısı planlanmıştır. Bu modellemede saldırganın iletim oranı %50 olarak belirlenmiş ve saldırgana gelen paketlerin yarısının 3. seviyeye geçişine izin verilirken, diğer yarısının bloke edilmesi sağlanmıştır.

Yapılan deneylerde sistem 20 dakika boyunca çalıştırılmıştır. Burada her 10 dakikalık süre, yaklaşık 600 adet veri paketinin baz istasyonunda toplanma süresidir. Deneyin ilk 10 dakikası saldırının olmadığı normal durumu, ikinci 10 dakikası ise saldırının eklendiği durumu temsil etmektedir. Saldırı-1'in gerçekleştirildiği deneyin sonunda elde edilen algılayıcı düğümde üretilen paket sayısı, baz istasyonunda toplanması gereken paket sayısı ve gerçekte toplanan paket sayıları Şekil 8'de görülmektedir.

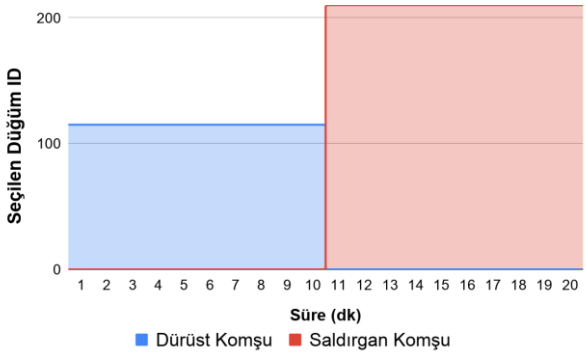


Şekil 8. Normal ve Saldırı-1 olduğu durumda algılayıcı düğüm tarafından üretilen, baz istasyonu tarafından toplanması beklenen ve baz istasyonu tarafından toplanan paket sayıları

Şekil 9'da yönlendirme protokolü tarafından seçilen 2. seviye düğümler ve aktif oldukları süreler görülmektedir. Algılayıcı düğümden iletilen 600 paketin tamamı baz istasyonuna iletilmiştir (Şekil 8). Deneyin ikinci yarısında saldırgan düğüm devreye girmiş ve yönlendirme protokolünün kendisini seçmesini sağlayarak tüm trafiği üzerine çekmiştir (Şekil 9). Algılayıcı düğümde üretilen 600 paketin tamamı saldırgan düğüme iletilmiştir. Saldırgan düğüm kendisine gelen paketlerin seçici yönlendirme saldırısı ile %50 sini baz istasyonuna iletmek üzere programlandığı için baz istasyonunda toplanan toplam paket sayısı 298 adet olmuştur (Şekil 8).

4.2. Saldırı-2: Çıkış Deliği + Kara Delik Saldırısı

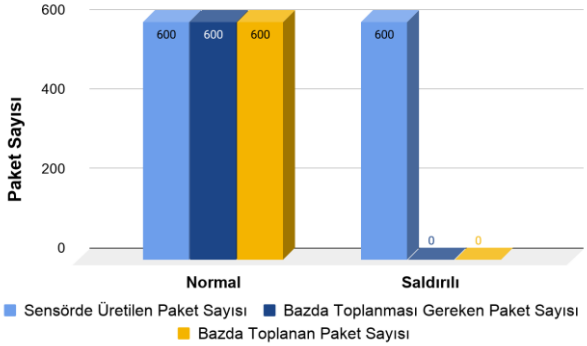
Bir önceki saldırıya benzer şekilde Saldırı-2'de saldırgan düğüm önce çıkış deliği saldırısını düzenleyerek veriyi kendisine çektikten sonra kara delik saldırısını gerçekleştirir. Kara delik saldırısı, seçici yönlendirme saldırısından farklı olarak paketlerin hiçbirisinin baz istasyonuna iletimine izin vermemektedir.



Şekil 9. Normal ve Saldırı-1 olduğu durumda yönlendirme protokolü tarafından seçilen düğüm ve aktif oldukları süre

Saldırı-2'nin gerçekleştirildiği deneyin sonunda elde edilen veriler; algılayıcı düğümde üretilen paket sayısı, baz istasyonunda toplanması gereken paket sayısı ve gerçekte toplanan paket sayıları olarak Şekil 10'da görülmektedir. Şekilde görüldüğü üzere baz istasyonu tarafında yapılan analizlerde, saldırı süresince hiçbir veri paketinin baza ulaşmadığı tespit edilmiştir. Bu süre zarfında beklenildiği gibi yönlendirme algoritması, düğüm seçimlerinin kontrolü ile ilgili herhangi bir işlem yapmamış ve trafiğin saldırgan üzerinden akmasına izin vermiştir.

Elde edilen sonuçlar, modellenen kara delik ve seçici yönlendirme saldırılarının amaçlarına ulaşarak baz istasyonunda beklenilen veri kayıplarını yaşattığını ve buna bağlı olarak bu saldırıları tespit edecek veya güvenli yollar üzerinden veriyi aktaracak algoritmalarının tasarlanmasının bu ağlar için oldukça önemli olduğunu göstermektedir.



Şekil 10. Normal ve Saldırı-2 olduğu durumda algılayıcı düğüm tarafından üretilen, baz istasyonu tarafından toplanması beklenen ve baz istasyonu tarafından toplanan paket sayıları

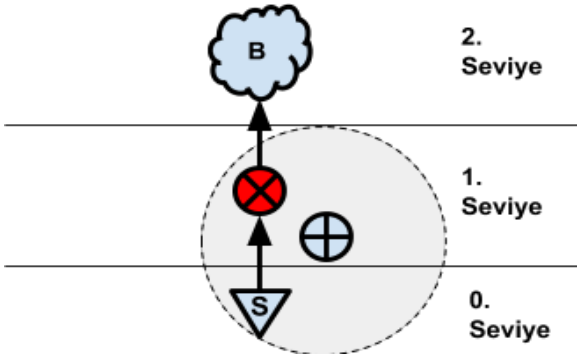
5. KOMŞU İZLEME TABANLI SALDIRI TESPİT SİSTEMİ

Bir önceki bölümde yer alan analiz sonuçları göz önüne alındığında paket iletiminin izlenmesine dayalı bir saldırgan düğüm tespit sisteminin tasarlanmasının mümkün olabileceği açıkça görülebilmektedir. Bu nedenle çalışmanın bu bölümünde komşu izleme tabanlı bir saldırı tespit sistemi gerçeklenmiştir. Şekil 11'de görüldüğü üzere 0.seviyede yer alan algılayıcı düğüm veri paketini 2.seviyede yer alan baz

istasyonuna ulaştırmak için 1. seviyede yer alan aracı düğümü (Şekilde kırmızı ile gösterilen düğüm) kullanacaktır. Bu iletişimde aracı düğümün saldırgan olması durumunda algılayıcı düğümün verisi baz istasyonuna ulaşmayacak ve sistemde paket kayıpları yaşanacaktır.

Saldırgan düğümü tespit etmek amacıyla mevcut mimari üzerinde aracı düğümün yer aldığı 1.seviyeye izleyici bir düğüm yerleştirilmiştir. İzleyici düğüm hem algılayıcı hem de 1.seviye aracı düğümü izleyebilecek şekilde konumlandırılmıştır. Bu düğüm veri iletişiminin dışındadır ve tek görevi kapsama alanındaki paket iletimini dinlemektir. Komşu düğümlerin aldıkları ve ilettikleri paketleri takip ederek kara delik ve seçici yönlendirme saldırılarının tespiti amaçlanmıştır.

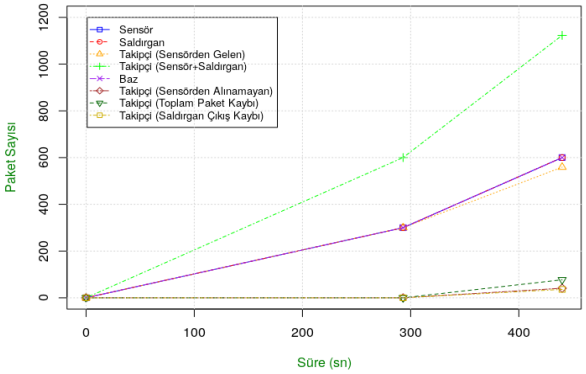
Yapılacak deneylerde gerçek zamanlı olarak algılayıcı düğüm tarafından gönderilecek olan toplam 600 adet veri paketi iki farklı süre aralığı için değerlendirilecektir. İlk 300 adet veri paket 1 sn. aralıklarla gönderilecek iken kalan veri paketleri 0.5 sn. aralıklarla gönderilecektir.



Şekil 11. Komşu İzleme Tabanlı Saldırı Tespit Sistemi İçin Test Ortamı Düğüm Yerleşimleri

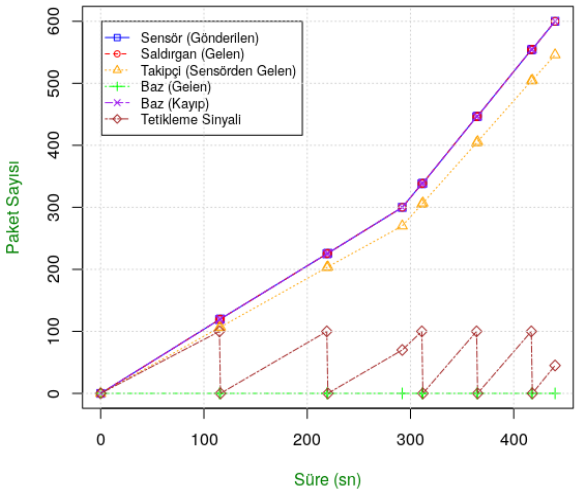
İzleyici düğüm, kapsama alanı içerisinde yer alan (baz istasyonu hariç) düğümlere gönderilen ve bu düğümlerden iletilen veri paket sayılarını (paket imzası tabanlı olarak) dikkate alarak farkın 100 olması durumunda tetikleme sinyali üretecek ve ilgili düğümün fark sayacını sıfırlayacaktır.

Şekil 12'de saldırısız durum için düğümlere ilişkin veri paket trafiği istatistikleri görülmektedir. Grafikten de anlaşılacağı üzere izleyici düğümün kapsama alanı sınırlarına yakın bir bölgede yer alması sebebi ile özellikle 0.5 saniyelik periyot içerisinde %3 lük bir paket kaybı yaşadığı görülebilmektedir. Paket kaybı miktarının belirlenen sınırlar altında olması tetikleme sinyalinin üretilmemesine neden olmuştur. 300. paket iletiminin sonrasında grafiklerde oluşan eğim, birim zamanda gönderilen paket sayısının (1 saniyeden 0.5 saniyeye düşmesi) artması sebebi ile ortaya çıkmıştır.



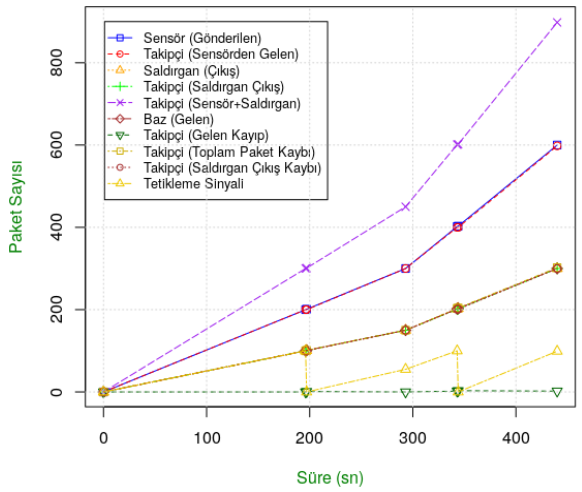
Şekil 12. Saldırının olmadığı ortamda düğümlerin ilettikleri paket sayıları

Şekil 13 'te görüldüğü üzere saldırgan düğüm veri trafiğini kendi üzerine çekerek kara delik saldırısı düzenlemiştir. Bu saldırı sonucunda saldırgana iletilen hiçbir paketin baz istasyonuna iletilmediği grafik üzerinden de görülebilmektedir. Algılayıcı düğümden gönderilen ve saldırgan düğüme gelen paket sayılarının eşit olması iletişimde paket kaybının olmadığını göstermektedir. İzleyici düğüm, gerçek zamanlı iletim ortamı sebebiyle algılayıcı düğümden gönderilen paketleri yaklaşık olarak %9 kayıp ile takip edebilmiş ve tetikleme sinyalinin daha geç aktif olmasına sebep olmuştur.



Şekil 13. Kara delik saldırısı yapılan ortamda düğümlerden iletilen paket sayıları

Şekil 14'te saldırgan düğüm veri trafiğini kendi üzerine alarak seçici yönlendirme saldırısı gerçekleştirmiştir. Bu saldırıda toplam paketlerin sadece %50'si baz istasyonuna iletilmiştir. İzleyici düğüm, gerçek zamanlı iletim ortamı sebebiyle algılayıcı düğümden gönderilen ve saldırgan düğüm tarafından iletilen paketleri yaklaşık olarak %1 kayıp ile takip edebilmiştir. Eşik değerini geçen fark sonucunda üretilen tetikleme sinyalinin, algılayıcıdan gönderilen ve baz istasyonuna iletilen paket sayıları ile doğru orantılı olduğu görülebilmektedir.



Şekil 14. Seçici yönlendirme saldırısı yapılan ortamda düğümlerden iletilen paket sayıları

İzleyici düğümün kapsama alanı içerisinde bulunan ve bu nedenle trafiklerini izlediği düğümlere ilişkin tespit edemediği/işleyemediği veri paketlerin neden olacağı tetikleme sinyali yanlış alarm üretebilmektedir. Tetikleme sinyalinin üretiminde kullanılacak olan bir eşik değeri ile (zamanlayıcı veya paket sayısına göre ile sıfırlanan) bu tür hatalar göz ardı edilebilir. Ayrıca kullanılan yönlendirme protokolünde, verilerin aktarımı sırasında iletimde olan aracı düğümler dışında geriye kalan tüm düğümler birer izleyici düğüm olarak kabul edilebilir. Böylece aynı trafiği izleyen birden fazla izleyici düğüm sistemde yer almış olacaktır. Saldırı yanıt sisteminin tasarımında birçok izleyici düğümün çoğunluk kararı dikkate alınarak gerekli süreçler yürütülebilir. Gelecekteki çalışmamızda daha fazla düğüm sayısı içeren farklı bir topoloji üzerinde önerilen sistemin test edilerek, sisteme alarm üretme mekanizmasının eklenmesi ve saldırı yanıt sisteminin tasarlanması amaçlanmaktadır.

6. TARTIŞMA

Bu çalışmada, gerçek zamanlı KAA için yaygın olarak kullanılan CTP yönlendirme protokolü üzerinde çeşitli yönlendirme atakları modellenmiş ve modellenen saldırılar için gerçek zamanlı bir saldırı tespit sistemi önerilmiştir. Öncelikle, içerisinde kara delik, seçici yönlendirme ve çıkış deliği ataklarını içeren bir atak kümesi literatürdeki tanımlarından yola çıkılarak CTP üzerinde modellenmiş ve sistemin bu saldırılara karşı verdiği tepkiler ile aldığı zararlar raporlanmıştır. Ardından bu raporlardan faydalanılarak sisteme yerleştirilen bir izleyici düğüm sayesinde komşu paket iletimleri takip edilmiş ve gerçekleştirilen saldırıların gerçek zamanlı olarak yakalanması sağlanmıştır.

Öncelikle, saldırının olmadığı sistem 10 dakika boyunca çalıştırılmış ve baz istasyonuna gelen yaklaşık 600 paket daha sonra yapılacak analizlerde kullanılmak üzere kaydedilmiştir. Saldırılar modellenirken ilk olarak çıkış deliği saldırısı kullanılmıştır. Bu saldırı sayesinde paketlerin saldırgan üzerinden akması sağlanmış ve ardından kara delik saldırısı ile tamamı; seçici yönlendirme saldırısı ile gönderilen paketlerin yarısı iletilmeyerek veri akışı engellenmiştir. Yapılan deneyler sonucunda, sistem 10 dakika boyunca çalıştırılmış ve beklenildiği gibi sistemde alternatif rotalar olmasına rağmen bunların kullanılmadığı ve buna bağlı olarak baz istasyonunda veri kayıplarının yaşandığı izlenmiştir.

Bu çalışmada önerilen komşu izleme tabanlı saldırı takip sistemi sayesinde CTP'deki güvenlik zafiyetinin giderilmesi amaçlanmıştır. Ağ trafiğine dahil olmayan bir düğümün, izleyici düğüm olarak gerçek zamanlı trafiği izlemesi ve saldırı tespiti anında tetikleme sinyali üretmesi hedeflenmiştir. Çalışmada, tekil bir izleyici düğüm ile izlenen ağ trafiği, izlenen düğümlere olan uzaklık vb. faktörler sebebi ile tolere edilebilir bir miktarda kayıplı olarak takip edilebilmiştir. Kara delik saldırısında algılayıcı düğümün göndermiş olduğu paketlere ilişkin trafik, gerçek zamanlı olarak %91 başarım ile izlenebilmiştir. Seçici yönlendirme saldırısında ise algılayıcı düğümden gönderilen paketler ile saldırgan düğümün ilettiği paketlere ilişkin trafik %99 başarı oranı ile izlenebilmiştir. Saldırgan düğümün iletmiş olduğu fakat izleyici düğümün tespit edemediği paket trafiği sebebi ile tetikleme sinyali beklenenden daha erken üretilmiştir.

Elde edilen sonuçlar ışığında yapılacak sonraki gerçek zamanlı çalışmalarda, izleyici düğüm sayısının arttırılarak ortak bir karar mekanizması ile trafiğin daha yüksek doğruluk oranlarında izlenebilmesi saldırı takip sisteminin başarımını arttıracaktır. Sonraki çalışmalarda, oluşan tetikleme sinyallerine uygun bir saldırı yanıt sisteminin modellenmesi ile saldırganın ağ trafiği dışında bırakılması amaçlanmaktadır.

KAYNAKÇA

[1] N. KhadirKumar and A. Bharathi, "Real time energy efficient data aggregation and scheduling scheme for WSN using ATL," Computer Communications, vol. 151, pp. 202-207, 2020.
[2] G. M. Borkar, et al., "A novel clustering approach and adaptive SVM classifier for intrusion detection in WSN: a data mining concept," Sustainable Computing: Informatics and Systems, vol. 23, pp. 120-135, 2019.
[3] J. Horneber and A. Hergenröder, "A Survey on Testbeds and Experimentation Environments for Wireless Sensor Networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1820-1838, Fourthquarter 2014.
[4] O. R. M. Boudia, S. M. Senouci, and M. Feham, "A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography," Ad Hoc Networks, vol. 32, pp. 98–113, 2015.
[5] J. Ryu, Y. Lee, and D. Won, "Cryptoanalysis of Lightweight and anonymous three-factor authentication and access control protocol for real-time applications in wireless sensor networks," Computational Science and Technology. Springer, Singapore, pp. 2341-349, 2020.

[6] K. Biswas, V. Muthukkumarasamy and K. Singh, "An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks," in IEEE Sensors Journal, vol. 15, no. 5, pp. 2801-2809, May 2015.
[7] Y. Tsou, C. Lu and S. Kuo, "MoteSec-Aware: A Practical Secure Mechanism for Wireless Sensor Networks," in IEEE Transactions on Wireless Communications, vol. 12, no. 6, pp. 2817-2829, June 2013.
[8] P. Gope, et al., "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," IEEE transactions on industrial informatics, Vol. 15 No. 9, pp. 4957-4968, 2019.
[9] F. Ishmanov and Y. B. Zikria, "Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues," Journal of Sensors, vol. 2017, pp. 1–16, 2017.
[10] G. Zhan, W. Shi and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197, March-April 2012.
[11] S. Sultana, D. Midi, and E. Bertino, "Kinesis: a security incident response and prevention system for wireless sensor networks" Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems - SenSys 14, 2014.
[12] H. Sedjelmaci, S. M. Senouci and M. A. Abu-Rgheff, "An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks," in IEEE Internet of Things Journal, vol. 1, no. 6, pp. 570-577, Dec. 2014.
[13] P. Peter, H. Petr and N. Jan, "Simulation and Evaluation of CTP and Secure-CTP Protocols," Radioengineering, vol. 2010, no. 1, pp. 89-98.
[14] A. Stetsko, L. Folkman and V. Matyas, "Neighbor-Based Intrusion Detection for Wireless Sensor Networks," 2010 6th International Conference on Wireless and Mobile Communications, Valencia, 2010, pp. 420-425.
[15] Z. Liu, W. Liu, Q. Ma, G. Liu, L. Zhang, L. Fang and V.S. Sheng, "Security cooperation model based on topology control and time synchronization for wireless sensor networks." Journal of Communications and Networks, 21(5), 2019 ,pp.469-480.
[16] M. Udhayavani and M. Chandrasekaran, "Design of TAREEN (trust aware routing with energy efficient network) and enactment of TARF: a trust-aware routing framework for wireless sensor networks." Cluster Computing, 22(5), 2019 , pp.11919-11927.
[17] L. Almon, M. Riecker and M. Hollick, "Lightweight Detection of Denial-of-Service Attacks on Wireless Sensor Networks Revisited," 2017 IEEE 42nd Conference on Local Computer Networks (LCN), Singapore, 2017, pp. 444-452.
[18] B. Cui and S. J. Yang, "NRE: Suppress Selective Forwarding attacks in Wireless Sensor Networks," 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, 2014, pp. 229-237.
[19] C. Ioannou and V. Vassiliou, "The Impact of Network Layer Attacks in Wireless Sensor Networks," 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, 2016, pp. 20-28.
[20] A. Dwivedi and O. Vyas, "An Exploratory Study of Experimental Tools for Wireless Sensor Networks," Wireless Sensor Network, Vol. 3 No. 7, 2011, pp. 215-240.
[21] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol," Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems - SenSys 09, 2009.
[22] S. Basagni, C. Petrioli and D. Spenza, "CTP-WUR: The collection tree protocol in wake-up radio WSNs for critical applications," 2016 International Conference on Computing, Networking and Communications (ICNC), Kauai, HI, pp. 1-6, 2016.
[23] E. C. H. Ngai, J. Liu and M. R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks," 2006 IEEE International Conference on Communications, Istanbul, 2006, pp. 3383-3389.
[23] A. Rehman, S. Rehman, and H. Raheem, "Sinkhole Attacks in Wireless Sensor Networks: A Survey," Wireless Personal Communications, Vol. 106 No.4 pp: 2291-2313, 2019.
[24] D.C. Mehetre, S. E. Roslin, and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," Cluster Computing, Vol. 22 No.1, pp: 1313-1328, 2019.
[25] H. Fu, Y. Liu, Z. Dong, Y. Wu, "A Data Clustering Algorithm for Detecting Selective Forwarding Attack in Cluster-Based Wireless Sensor Networks," Sensors, Vol. 20 No.1 pp: 23, 2020.