DİPLOMA PROJESİ

RAPOR - 3

İSTANBUL ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

Halil Hakan Tarhan
1306010039

INSENS* ALGORİTMASININ PERFORMANS BAKIMINDAN DEĞERLENDİRİLMESİ [1]

1- Giriş

Kablosuz sensör ağlar (WSN) araştırma dünyasında önemi hızla artan yeni bir alan olarak görünmeye başlandı. Uygulama alanı olarak evden ofise , doğa-çevre gözlemlerinden askeri uygulamalara ve gömülü sistemlere kadar çok sayıda alanda kullanılmaktadır.

Askeri uygulamalarda , WSN'in düşman sahaya kurulması asker ve araçların izlenmesine olanak sağlar. Ev/ofis uygulamalarında , ev içerisindeki sensör ağ yaşlı insanların sağlık durumlarının gözlemlenmesine ve kablosuz ev güvenlik sistemleri aracılığı ile , eve girmeye çalışan kişilerin tespit edilmesinde kullanılabilir. Bu senaryoların herbirinde hayatlar dakiklik ve dağıtılmış düğümlerin elde ettiği veririn doğruluğuna bağlıdır.

Sonuç olarak , her WSN , sensör düğümlerinin elde ettiği verinin doğruluğunu bozabilecek ve verinin iletilmesini engelleyebilecek izinsiz kullanıcılara karşı korunmalıdır. Bu sorunları ortaya koymak amacıyla burada, veri iletimini engellemeye çalışan ataklara karşı dayanıklı , uçtan uca bütünlük sağlaması (checksum) , ve algılanan verinin kurcalanmasının (tampering) tespitinde kullanılabilecek kimlik doğrulama şemalarını içeren güvenli yönlendirme sistemi geliştirilmiştir.

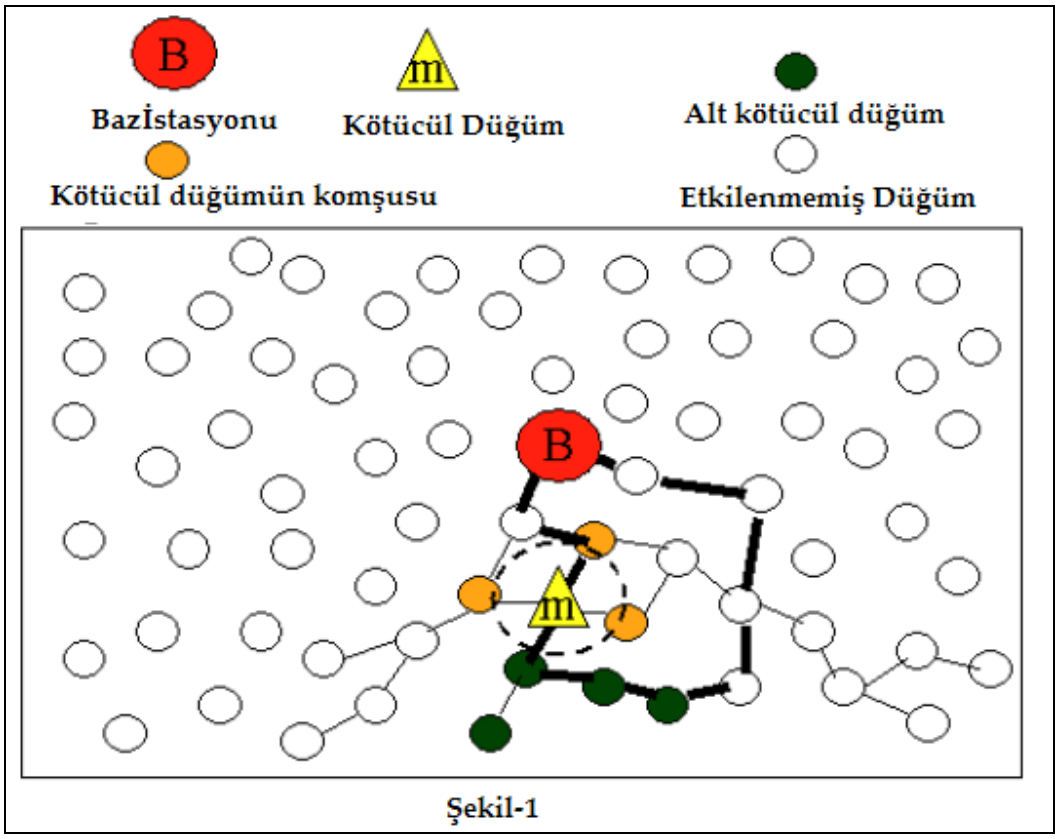
WSN lerde güvenli yönlendirmenin tasarımı ve gerçeklenmesi aynı anda üç zor problemi çözmelidir.Bunlardan birincisi ,sensör düğümler arasındaki kablosuz haberleşme gizli dinlemeye,izinsiz erişime,kandırma(spoofing), tekrarlı gönderime ve DOS saldırılarına karşı ağın güvenliğini tehlikeye atmaktadır.

İkinci problem , sensör düğümlerinin ileri derecede kaynak-sınırlı olmalarıdır ; sınırlı bellek, işlemci ,iletişim bant genişliği , ve özellikle batarya ömrü bu sınırlamalara örnek olarak verilebilir.Kaynakların sınırlılığı düğümler üzerinde gerçeklenebilecek şifreleme , deşifreleme ve kimlik doğrulama işlemlerinin seviyesini sınırlandırır, ve geleneksel güvenlik mekanizmalarının uygunluğunun tartışılmasına neden olur. Üçüncü olarak , herhangi bir alana düğümleri yayılmış olan WSN'ler fiziksel saldırıyla karşı karşıya gelebilir , ayrıca tekil düğümlerin yerlerinin tespit edilmesi ve saldırıya maruz kalmaları ya da kaybedilmeleri iyi donanımlı bir saldırgan tarafından gerçekleştirilebilir.

Başarılı bir saldırı sonrasında , kaybedilmiş düğüm art niyetli işlemlerde kullanılabilir , örnek olarak ; sensör ağın bilgisi dışında yanlış yönlendirme bilgisinin yayılması , sensör ağ içerisinden DOS saldırısı yapılması verilebilir.

* INSENS : Intrusion-Tolerant Routing in Wireless Sensor Networks

Verilen problemler ve kaynak sınırlılığı ışığında , WSN'leri güvenli hale getirmek için , iyi donanımlı bir saldırganın tekil sensör düğümlerini ele geçirebileceği kabulü yapılmıştır , bu durumda bile sensör ağın tasarımı bu kayıpları tolare edecek şekilde yapılmalı , WSN işlevselliğini muhafaza edebilmelidir. Baz istasyonlarının , olası saldırılara karşı kendisini savunmak için , mevcut kaynaklarının sensör düğümlere göre oldukça fazla olduğu varsayımı yapılmaktadır.Bu nedenle sisteme karşı yapılan saldırları en zayıf taraftan yani kaynak-sınırlı sensör düğümler tarafından gerçekleştirmemiz gerekir.



Şekil-1

Şekil-1 ; Baz istasyonunu kök olarak kullananan örnek asimetrik WSN topolojisi.Üçgen düğüm kötücül düğümdür.Yeşil düğümler kötücül düğümün alt düğümleridir.İzinsiz girişlere karşı müsamahakar yönlendirme (Intrusion-tolerant routing) çoklu yol ile sağlanır; bu sayede alt düğümler hala baz istasyonuyla iletişim kurabilecek haldedir.

Bu amaç ile tasarlanan INSENS (INtrusion-tolerant routing protocol for wireless SEnsor NetworkS-Sensör Ağlar için İzinsiz Girişlere Dayanıklı Yönlendirme Protokolü) tek bir düğümün kaybı ile sadece ağın bir bölümünün etkilenmesini sağlayacak şekilde tasarlanmıştır , bu düğüm kaybı ağın tamamını etkilemez.

INSENS güvenli yönlendirme sistemi aşağıdaki tasarım prensiplerine bağlıdır.

1-DOS tipi boğma saldırılarını önlemek için , tek bir düğümün tüm ağa tümegönderim (broadcast) yapmasına izin verilmez.

2- Sadece baz istasyonu (Bkz. Şekil-1) tümegönderim yapmaya yetkindir. Baz istasyonu kablolu ortama açılan bir ağgeçidi gibi davranır , örnek olarak yerüstü ağa yapılan uydu bağlantısı .Baz istasyonu tek yönlü ardışık numara üzerinden gevşek kimlik doğrulamalıdır , bu yüzden tek bir düğüm keyfi olarak baz istasyonunu kandıramaz (spoof) ve ağı boğamaz (flood).Sensör düğümleri sadece tekegönderim (unicast) yapma ile sınırlandırılmışlardır , ve de sadece baz istasyonuna gönderim yapabilirler , bu da DOS/DDOS tümegönderim saldırılarını önler. Direkt olarak eşten eşe (Peer-to-peer) sensör iletişimi yapılamaz , baz istasyonu üzerinden tünelleme yoluyla indirekt sensör-sensör iletişimi sağlanabilir.Yanlış yönlendirme bilgisinin yayılmasını önlemek amacıyla , yönlendirme bilgisinin kontrolü kimlik doğrulama ile sınanmalıdır.

Bu kazanımın önemli bir sonucu ; art niyetli paket yayılması durumu sonucunda bile kısmi de olsa baz istasyonu sürekli olarak doğru ağ topolojisi bilgisini alır.

3-Kaynak sınırlılığı sebebiyle ; a) Gizlilik ve kimlik doğrulama için simetrik anahtar şifreleme baz istasyonu ve düğümler arasında kullanılır , çünkü public anahtar şifreleme daha fazla hesaplama odaklıdır , b) yönlendirme tablolarının hesaplanması ve dağıtımı için kaynak sıkıntısı çekmeyen merkezi baz istasyonu görevlidir.

4- Kaybedilmiş düğümlerin bilgisini kullanarak güvenli yönlendirmenin sağlanması için , fazlalıklı çokyollu yönlendirme INSENS içerisinde yerleşik durumdadır (Bkz Şekil-1) . Buradaki amaç , ayrık yollara sahip olmak ve bu sayede , saldırgan bir düğümü ya da bir yolu ele geçirse dahi , aynı güzergah üzerindeki ikinci yol aracılığı ile doğru hedefe istenilen paketi yollayabilmektir.

2-Protokolün Tanımı

Bu bölümde kısaca INSENS in genel görünümü verilecektir. INSENS yol bulma ve veri gönderme aşamalarından oluşmuştur. Yol bulma aşaması sensör ağın topolojisini tespit eder ve her düğüm için uygun gönderim tabloları oluşturur.

Yol bulma üç devreye bölünmüştür. İlk devrede ; baz istasyonu erişilebilir tüm düğümlere bir istek mesajı yollar/salar (limited-flooding). İkinci devrede ; Her sensör düğümü , kendine ait olan komşuluk topolojisi bilgisini , baz istasyonuna geribildirim mesajı ile bildirir.Üçüncü devrede ; baz istasyonu komşuluk bilgisini doğrular ve ağın topolojik resmini oluşturur , her sensör

düğümü için gönderim tablosunu hesaplar , ve bu tabloları yönlendirme güncelleme mesajı kullanarak ilgili düğümlere yollar. Veri gönderim aşaması verinin sensör düğümlerinden baz istasyonuna ve tam tersi yönde gönderilmesini mümkün kılar.

Simetrik haberleşme kanalı varsayılmaktadır , örneğin a düğümü b düğümünden gelen bir mesajı duyabiliyorsa , a düğümü b ye mesaj yollayabilir. Her düğüm baz istasyonuyla paylaşılmış bir simetrik anahtara sahiptir. Her düğüm global olarak bilinen tek yönlü F fonksiyonu ve ilk sıra numarası K0'a sahiptir. F ve K0 bazdan gelen mesajların gevşek kimlik doğrulamaya tabi tutulmasında birlikte kullanılır. F , K0 ve paylaşılmış simetrik anahtar bilgisi önceden dağıtılır , örnek verirsek ; düğümlerin yayılmasından önce programlanır.Askeri uygulamaları göz önünde bulundurursak , sensör düğümlerinin yayılmadan önce gizli anahtarlarının programlandığını görürüz.

2.1 Yol Bulma : Yol İsteği

Baz istasyonu tüm düğümlere ait gönderim tablolarına oluşturmaya ihtiyacı oldukça , birinci devreyi ilkler .Baz istasyonu tüm komşuları tarafından alınan bir istek mesajı yayınlar. Bir x düğümü tarafından yayınlanan istek mesajı , x düğümünden baz istasyonuna giden yol bilgisini de içerir. Bir düğüm bir istek mesajını ilk kez aldığında , bu mesaja kendi kimliğini ekleyerek yayınlar(gönderir). Ayrıca mesajın kendi komşuluk kümesindeki göndericisinin kimliğini de kaydeder.

Bir düğümün aynı mesajı birden çok kez alması halinde ise , göndericinin kimliği kaydedilir fakat alınan mesaj tekrar yayınlanmaz. Bu devrede ağ içerisindeki art niyetli düğüm birden fazla saldırıya teşebbüs edebilir.Bunlardan birincisi , baz istasyonunu sahte istek mesajı yollayarak kandırmaya(spoof) teşebbüstür. İkinicisi , almış olduğu istek mesajını gönderirken sahte yol bilgisi ekleyebilir.Üçüncüsü , almış olduğu istek mesajını göndermeyebilir ya da tekrarlı bir biçimde yolladığı istek mesajları ile DOS saldırısı başlatabilir .

Bu saldırılara karşılık vermek için iki tür mekanizma kullanabiliriz. Bu iki mekanizma da sensör düğümlerinin uygun değerlerle önceden ayarlanmış olmasını gerektirir.

İlk olarak , baz istasyonu tek yönlü kriptografik hash fonksiyonu kullanır ve K_0 , K_1, ... ,K_n ardışık sayılarını üretir , bu fonksiyonu Ki = F(Ki+1) şeklinde gösterebiliriz , burada 0 <= i < n dir. Başlangıçta , her düğüm K_0 ve F değerlerini bilir . İlk yol bulma aşamasında , baz istasyonu K_1 i yayınladığı istek mesajına ekler . Genelde , baz istasyonu Ki'yi i'nci yol bulma aşamasında kullanır. Her düğüm yayınlanan sıra numarasının baz istasyonu merkezli olup olmadığını

Ki = F(Ki+1) fonksiyonunu kullanarak hesaplayabilir. Bir düğümü ele geçiren saldırgan , sıradaki tek yönlü ardışık sayıyı tahmin edemez , örnek vermek gerekirse F,K_0 ve son kullanılan K_i ye sahip olunsa da , saldırgan F ' yi sıradaki sayıyı (Ki+1) üretmekte kullanamaz. Sonuç olarak , kaybedilmiş bir düğüm baz istasyonunu sıradaki sayıyı üreterek kandırmaz. Ancak , kaybedilmiş düğüm mevcut sıra numarasını istek mesajının içerisinde alt düğümlere tekrar tekrar yollar ise , alt düğümleri kendisinin baz istasyonu olduğuna inandırabilir.

Bu durumda hasar kaybedilmiş düğümle sınırlıdır, bu da bizim tasarım hedefimizdir. Ağın geri kalanı , kimlik doğrulamayı geçmiş olan baz istasyonunun yol isteğini ilk olarak alır , ve bu yüzden kaybedilmiş düğümün yol isteklerini yoksayar. Tek yönlü fonksiyonları kullanımımız μTESLA protokolünüyle gelen kazanımları yükseltir , buradaki fark ; tek yönlü zincirdeki numaralar simetrik anahtarlar değildir , sıralı numaralardır.

Kullandığımız ikinci mekanizme anahtarlanmış MAC algoritmasıdır. Her sensör düğümü bölünmüş bir gizli anahtar ile ayarlanmıştır,bu anahtar sadece baz istasyonuyla paylaşılır. Bir x düğümü bir istek mesajını ilk kez aldığında , kendi kimliğini yol listesine ekler , ve sonrasında yeni yolun tamamının MAC'ını kendi anahtarıyla üretir.Ayrıca bu MAC istek mesajı alt düğümlere yollanmadan önce istek mesajına eklenir. Bu MAC , baz istasyonu tarafından pakette bulunan yolun bütünlüğünü sınamada kullanılır. Ayrıca bir düğüm kaybedilince , sadece bir gizli anahtar kaybedilmiş olur , saldırgan tüm ağı ele geçiremez. Tüm bu güvenlik mekanizmalarının etkisine bakarsak ; saldırgan bir düğüm birinci devrede sadece sınırlı boğma (flooding) yapabilir , çünkü istek mesajı yollanmaz ve istekte yollanan sahte yol bilgisi ikinci devrede tespit edilir.İki ataktan sonuncusu , saldırgan düğümün altındaki düğümlerde , geribesleme mesajlarını baz istasyonuna yollayamama ve istek mesajlarını alamama şeklinde etkilere sahiptir.

2.2 Yol Bulma : Yol Geribesleme

İkinci devrede , her sensör düğümü kendine ait yerel bağlanabilirlik bilgisini (komşu düğümlerine ait kimlik bilgilerinin kümesi ; baz istasyonundan kendisine olan yol bilgisi) geribesleme mesajı ile baz istasyonuna yollar. Bir x düğümü kendi istek mesajını devre birde yolladıktan (forward) sonra , belli bir zaman aşımı aralığı kadar bekler ve sonrasında geribesleme mesajı üretir. Bu zaman aralığı boyunca , aynı mesajı yollayan komşu düğümlerin yerel yayınını dinler ve bu düğümlerin kimliğini (id) ve MAC'ını istek mesajı içerisinde gömülü biçimde saklar. Zaman aşımı sonrasında , sensör düğümü kendine ait komşularının (aşağı-downstream, yukarı-upstream , aynı seviye-peer) listesini

baz istasyonuna geri yollar , her komşu kimliği ve MAC 'ıyla tamınlanır. Sensör düğümü anahtarlanmış MAC ' ını topoloji bilgisine ekler , örnek olarak ; komşularının listesi , geri besleme mesajlarının bütünlüğünü sağlamak için kullanılabilir.Baz istasyonuna ulaşan mesajlar , doğrulamadan sonra doğru olduğu ve tahrif edilmediği yönünde garantilidir. Bir x düğümünden baz istasyonuna yollanan geri besleme mesajının yönlendirilmesi , geribesleme yanıtını ilklendiren istek mesajının geriye doğru yol takibi ile sağlanır. Geri besleme mesajını yollarken saldırgan bir düğümün yanlış yol bilgisi üretmediğinden emin olmak için ; bir düğüm kendi üst (parent) kimlik bilgisini , üstün MAC'ı ile birlikte tutar , bu MAC ilk istek mesajında alınmıştır. Her düğüm bir meşru yukarı düğümü üst olarak seçecektir , bu seçim baz istasyonuna giden yoldaki düğümlerin oluşturduğu ana düğüm zincirini biçimlendirir.

Saldırganın eline geçmiş bir düğüm en fazla ,kendi üstünün baza giden zincirindeki düğümlerden birini boğma (flood) şansına sahip olur , diğer düğümleri değil . Bu saldırının etkisini sınırlandırır. İleri atakları kısıtlamak için , hız kontrolü her düğüme uygulanmıştır ; giriş trafik hızı dikkate alınmaz , çıkış trafiğinin maksimum hızı bir değerle sabitlenir , bu sayede boğma saldırıları önlenmiş olur. Ayrıca her düğüm geri besleme mesajını yollarken , uygun veriyi şifreler , şifrelenmiş halde gönderim art niyetli bir düğüm tarafından dinlemeye karşı güvenliği sağlar. Bu güvenlik mekanizmalarının toplam etkisine bakarsak ; saldırgan bir düğümün yapabileceği , DOS saldırısı ya da geri besleme mesajının yollamamak , ya da düğümlerin komşuluk bilgisinin değiştirilmesi (baz istasyonunda farkedilir) gibi saldırılarda hasar sınırlandırılır .Bu saldırılar, saldırgan düğümün aşağısındaki düğümlerin bazılarının , baz istasyonuna doğru bağlanabilirlik bilgisini sunamamasına neden olabilir.Art niyetli bir düğüm batarya tüketimine neden olmak için sürekli sahte geribesleme mesajlarını hız kontrol sınırında da olsa yollayabilir, bu tarz bir saldırı sadece sınırlı sayıda üst düğümü etkiler.

2.3 Yol Bulma : Çokyollu Yönlendirme Tablolarının Hesaplanması ve Yayılımı

Baz istasyonu ilk devrede istek mesajını yolladıktan sonra , belli bir süre geribesleme mesajlarının alımı ile tüm bağlanabilirlik bilgisini toplamak için bekler.Her düğüm kendi komşularının doğrulanmış listesini döndürür. Sonuç olarak baz istasyonu komşuluk bilgisini , geri besleme mesajları ile doğrulama ve herhangi bir tahrifi tespit etme yeteneğine sahiptir. Baz istasyonu bu doğrulanmış geribesleme mesajları aracılığı ile ağın topolojisini oluşturur, ağın bu resmi , ulaşmayan geribesleme mesajları olabileceğinden tamamlanmamış

olabilir. Bu bağlanabilirlik bilgisi üzerinden baz istasyonu her düğüm için bir yönlendirme tablosu hesaplar.INSENS , yönlendirmeye fazlalığı , birden çok fazlalık yolları oluştururarak dahil eder, bu sayede sisteme girmeye çalışan saldırgan atlatılmış (bypass) olur , Bkz. Şekil-1. Yollar birbirlerinden bağımsızdır , olabildiğince az ortak düğüm/bağlantı içerirler ; ideal olarak , tüm yol boyunca sadece kaynak ve hedef düğümler ortaktır.Bir yol boyunca bir ya da daha fazla saldırganın varlığı yollanan bazı mesaj kopyalarının hedefe ulaşmasını tehlikeye atar. Ancak , saldırgan tarafından etkilenmemiş en az bir adet yolu varlığı sayesinde, hedef en az bir adet tahrif edilmemiş mesaj kopyasını alacaktır.

INSENS çoklu yolların seçimi için kesin bir kritere sahip olmasa da , biz aşağıdaki yöntemleri INSENS gerçeklememizde çoklu yol bulmada kullanacağız.

A düğümü için , A dan baz istasyonuna giden yollardan birincisi Dijkstra'nın en kısa yol algoritmasıyla bulunur. İkinci yolu bulmak için , S_1 ,S_2 ve S_3 düğüm kümeleri oluşturulur. S_1 birinci yola ait düğümleri içeren , S_2 ise S_1 deki düğümleri ve S_1'deki düğümlere komşu tüm düğümleri içeren ve S_3 ise S_2'deki tüm düğümleri ve bu düğümlere komşu tüm düğümleri içeren kümelerdir.Bu üç küme A ya da baz istasyonunu dışlar.

İkinci yol aşağıdaki adımlar doğrultusunda hesaplanır :

1. Ağdan S_3 'deki tüm düğümler çıkarılır,sonrasında A dan baz istasyonuna giden en kısa yol bulunur.Eğer bir yol bulunursa , hesaplama sonlandırılır. Bulunan yol ikinci yoldur.
2. Eğer bir yol bulunamadı ise ; S_2' deki tüm düğümler orijinal ağdan çıkarılır,sonrasında A dan baz istasyonuna giden en kısa yol bulunur. Eğer bir yol bulunursa , hesaplama sonlandırılır. Bulunan yol ikinci yoldur.
3. Eğer bir yol bulunamadı ise ; S_1' deki tüm düğümler orijinal ağdan çıkarılır,sonrasında A dan baz istasyonuna giden en kısa yol bulunur. Eğer bir yol bulunursa , hesaplama sonlandırılır. Bulunan yol ikinci yoldur.

Aksi halde A dan baz istasyonuna giden ikinci bir yol yoktur.

Ağın durumuna göre ikinci bir yol bulunamamasının olası olduğu görülmelidir.Bu durumda INSENS in mevcut gerçeklenmesi tek bir yol ile devam eder. INSENS için daha iyi bir çoklu yol bulma algoritmasının tasarlanması gelecek çalışmalarda yapılmalıdır.Her düğüm için fazlalıklı yolların hesaplanmasından sonra , baz istasyonu her düğüm için gönderim tablolarını hesaplar.Bu gönderim tabloları her düğüme sırayla dağıtılır.Baz istasyonu ilk olarak kendine komşu olan düğüme gönderim tablolarını yollar.Ardından kendine iki adım mesafede olan düğümlere gönderim tablolarını yollar , bu işlem adım sayısı artırılarak devam eder.Bu mekanizma zekice fazlalık yönlendirme mekanizmasını kullanır , gönderim tablolarının dağıtılması için geliştirilmiştir.

2.4 Veri Gönderme/Yönlendirme

Bir düğüm birden fazla girişli gönderim tablosuna sahiptir , her kayıt düğüme ait bir yol bilgisini tutar. Her giriş 3 alandan oluşur ; < *hedef,kaynak, anlık gönderen*>.Hedef; veri paketinin gönderildiği hedef düğümün kimlik numarasıdır , kaynak , bu veri paketini oluşturan düğümün kimlik numarasıdır, ve anlık gönderen , bu veri paketini en son gönderen düğümün kimlik numarasıdır. Örnek olarak , S düğümünden D düğümüne giden bir yol şu şekilde verilsin : S > a > b > c > D . a düğümünün gönderim tablosunda < D, S, S > kaydı mevcuttur , b düğümünün tablosunda < D, S, a > , c düğümünün tablosunda <D,S,b> kaydı görülür. Bu yöntemle paket gönderimi basit bir şekilde gerçekleştirilebilir.

Düğüm bir veri paketi alırken , kendi gönderim tablosundaki kayıtlar içerisinde <*hedef,kaynak, anlık gönderen*> ile eşleşen bir kayıt arar , kayda rastlarsa , veri paketini gönderir (yayınlar).

3-Simülasyon

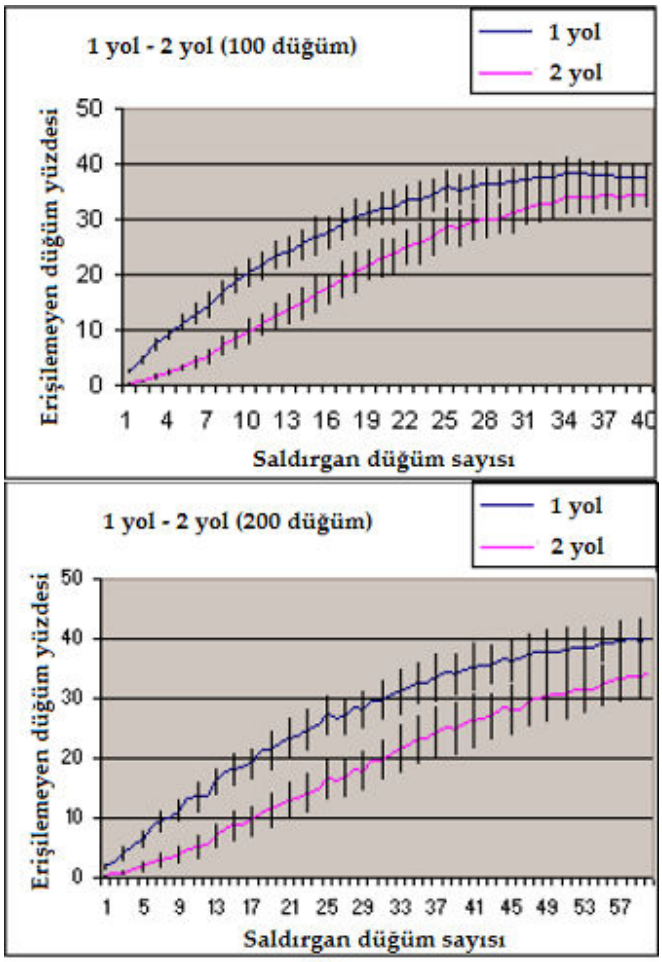
INSENS nsclick üzerinde simüle edilmiştir , nsclick , ns-2 ağ simülatörünü Click Modüler Router ile birleştirir. Bu uygulamaya özel Click elemanı geliştirilmiştir , bu sayede INSENS'in davranışları sensör düğümleri ve baz istasyonu üzerinde simüle edilmiştir.Ns-2 kablosuz ağ ortamının simüle edilmesinde kullanılmıştır , MAC protokolü , kablosuz ağın alt katmanlarını ve düğümlerin coğrafi dağılımlarını içerir.

3.1 Veri Gönderme Sırasında Kötücül Saldırı

INSENS kötücül düğümleri atlatmak için iki yol üretir.Herhangi iki düğüm ve baz istasyonu arasındaki iki bağımsız yol sayesinde , protokolün kazanımı tek bir kötücül düğümün varlığında mesajları doğru bir biçimde yönlendirebilmektir.İlginç bir şekilde şu da farkedilir, birden fazla kötücük düğümün varlığında da protokol oldukça iyi çalışmaktadır.

Birden çok düğümün kötücül düğüme dönüşmesi ve ardından veri paketlerini düşürmesi durumunda kaç adet düğümün erişilemez/engelli hale geldiğini ölçmek için testler gerçekleştirildi.Şekil-2 kötücül düğüm sayısı ile bu düğümlerin etkileri sonucu ile ortalama kaç adet düğümün erişilemez olabileceğini gösterir.Karşılaştırma amacı ile , yol sayısı bire indiğinde ortalama

erişilemeyen düğüm sayısını da hesapladık.Sonuçlar 100 ve 200 düğümden oluşan ve düğümleri 1500x1500 m^2 alana rastgele dağıtılmış 2 ağ için geçerlidir. Şekilde belirtilen sayılar kötücül düğümlerin 50 farklı kombinasyon sonucu rastgele seçilmesi ile elde edilmiştir. Örnek olarak ; 10 kötücül düğüm için, engellenmiş düğümlerin sayısını , 10 düğümü 50 farklı kombinasyon içerisinden seçip kötücül düğüme çevirip hesaplarız.Her test için 20 rastgele topoloji seçildi.



Şekil -2

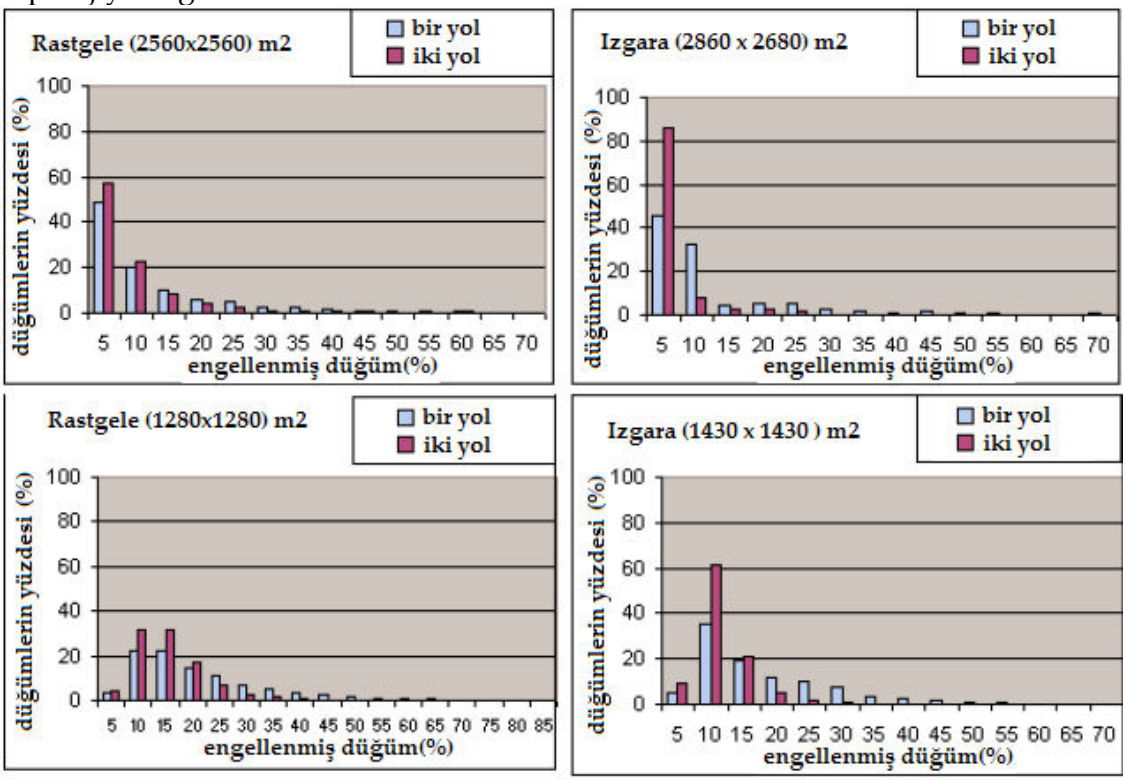
Şekil-2.Birden çok düğüm tarafından yapılan saldırı karşısında tek ve çift güvenli yola sahip olma durumu.Üst grafik 100 düğümlü , alt grafik 200 düğümlü ağı gösterir. X ekseni : Saldırgan düğümlerin sayısı , Y ekseni : Erişilemeyen (paket gönderemeyen) düğüm yüzdesi.

3.2 DOS Saldırıları

DOS saldırılarını kötücül bir düğümün gerçekleştirmesi durumunda saldırıların etkilerini analiz etmek için birçok test gerçekleştirildi.Bu testlerde kullanılan DOS saldırı tipleri ; kablosuz ortamı engellemek için ard arda baz istasyonuna paket gönderme ve diğer düğümlerin paketlerini göndermelerine engel olma şeklindedir.

DOS saldırılarının ağ katmanında tam olarak etkisiz hale getirilmesi zordur. Bu saldırılar farklı katmanlarda karşılanmalıdır. Analizimize göre , aşağıdaki adımlar varsayılmıştır:(1) Sensör düğümleri veri paketlerini gönderirken hız tabanlı bir kontrol mekanizması kullanmalıdır.Şu varsayım yapılmıştır ; kötücül bir düğüm ard arda yolladığı veri paketleri ile komşularını engelli konumuna düşürebilir , fakat başka düğümleri (üst düğümlerini) engelleyemez.(2) Baz istasyonu büyük bir band genişliğine sahiptir yani , kötücül bir düğüm kendi bölgesinde baz istasyonunu DOS saldırısı ile engelleyemez.

Şekil-3 DOS saldırısı yapan bir kötücül düğümün sebep olabileceği hasarı gösterir. DOS saldırısı sonucu oluşan hasar çoklu-yol algoritmasının verimliliğine, sensör ağın arabağlantılarının yoğunluğuna ve sahip olunan topolojiye bağlıdır.



Şekil-3: Düğümlerin seyrek ve yoğun olarak rastgele ve ızgara modelle dağıtılması sonrasında,simüle edilmiş DOS saldırılarını gösteren histogramlar.

Bu deneyde , iki farklı ağ yoğunluğu (seyrek ve yoğun) ve iki ağ topolojisi (rastgele ve ızgara model) sınanmıştır.Rastgele üretilen topolojide tüm düğümlerin yerleri rastgele seçilmiştir, baz istasyonu ortadadır.
Rastgele üretilen topolojide düğüm sayısının toplamı 200 dür.Izgara model topolojide, her sensör düğümü bir kare ızgaraya yerleştirilmiştir.Izgara boyutu 14 x 14 m lik karedir.

Şekil-3 bir düğümün DOS saldırısında bulunması sırasında INSENS'in performansını gösterir.Izgara model ya da rastgele dağılımda yapılan ilk iş , dağıtılmış düğümlerin topolojisini üretmektir.Bu topoloji için , her düğümün bir kez DOS saldırganı olmasını sağlar ve engellenen düğüm sayısını ölçeriz. Bu her topoloji için bir histogram üretilmesini sağlar.Histogramın x ekseni tek düğümden kaynaklı DOS saldırısı sonucu engellenen düğümlerin yüzdesini gösterir, y ekseni ise saldırgana dönüşen düğümlerin yüzdesini gösterir. Temiz bir görünüm için x ekseni %5 lik dilimlere bölünmüştür.Rastgele ve Izgara model topolojilerin ikisi için de , 50 topoloji üretilmiş ve ortalama histogramlar Şekil-3 de gösterilmiştir.

Bu şekilden , DOS saldırılarına karşı korunmanın değişik ağ yoğunluklarına ve topolojilere göre değiştiği gözlemlenebilir.Beklendiği gibi tüm durumlarda DOS saldırılarına karşı çok-yollu algoritma, tek yolluya göre daha iyi koruma sağlamaktadır.Çok yollu algoritma ızgara modelde çok daha iyi bir sonuç verir , çünkü ızgara yapısı neredeyse her zaman geçerli bir fazlalık ikinci yol sunar. Çok yollu algoritmanın verdiği en iyi sonuç seyrek dağılmış topolojisinde görülür (sağ-üst grafik) , saldırgan düğümlerin %85 i sadece 5 ve daha az düğümü engelleyebilmiştir.Seyreklik , saldırganın az sayıda düğümü engelleyebilmesine neden olur, aynı zamanda ızgara yapı neredeyse her zaman göndericiye geçerli bir ikinci yol sunar. Çok yollu algoritmada en kötü sonucu seyrek ve rastgele şekilde dağıtılmış topolojide görürüz (sol-üst grafik) , bu durumda düğümler az sayıda komşuya ve az sayıda alternatif yola (genelde baza giden tek yol vardır) sahiptir. Bu durumda , çok yollu algoritma tek yollu algoritmadan çok az bir farklılık (iyi yönde) gösterir.Ağ yoğunlaştıkça , grafiğin üst sıralarından alt sıralarına doğru ilerlersek , saldırganların artan sayıda düğümleri engelleyebildiğini görürüz ve histogramlar sağa kayar. Bu durum hem rastgele hemde ızgara model topolojiler için geçerlidir.

Şekiller (Şekil-3 deki) INSENS'in ortalama tepkisini gösterir, saldırgan topolojinin yapısını kullanarak ve en zayıf düğümü belirleyerek grafiği bölebilir. Bu tür bir bölme saldırısı ızgara yapıda ya da yoğun topolojilerde büyük oranda verimsiz olacaktır, çünkü bu topolojiler alternatif yolların varlığından ötürü kolayca bölünemezler.Hem seyrek hem de rastgele dağıtılmış topolojilerde bölme saldırısı daha etkilidir.Bu tür saldırılara karşı INSENS in performansı ölçülmemiştir.

4. Sonuç

Bu dökümanda , INSENS algoritmasının deneysel gözlemini sunmaktayız. INSENS'in çeşitli haberleşme tabanlı saldırılara karşı çok-yollu performansını simülasyon aracılığı ile gözlemledik.

[1].Jing Deng, Richard Han, Shivakant Mishra : A Performance Evaluation of Intrusion-Tolerant Routing in Wireless Sensor , Networks University of Colorado at Boulder, Computer Science Department