Using trust model to ensure reliable data acquisition in VANETs

Xuanxia Yao, Xinlei Zhang, Huansheng Ning, Pengjian Li
Ad Hoc Networks 55
2017

Özet. Araşsal tasarsız ağlar (VANET) genellikle trafik kazalarının önlenmesi, trafik verimliliğinin ve güvenliğinin arttırılması, yakıt tasarrufunun sağlanması, ticari, reklam ve eğlence odaklı uygulamaların teşvik edilmesi gibi farklı amaçlar için kullanılmaktadır. Tüm bu uygulamalar ağdaki düğümler (araçlar) arası veri iletişimine dayanmakta ve sadece verinin güvenli iletişimi değil aynı zamanda verinin doğruluğu da son derece önem taşımaktadır. Bu amaçla makalede, uygulama ve düğüm türlerine göre ağırlıklandırılmış dinamik bir varlık/araç merkezli güven modeli (entity-based trust model) öne sürülmüş ve benzetim sonuçlarına göre güven modelinin GPSR yönlendirme protokolü üzerinde düşük gecikme ve yüksek veri iletim oranıyla çalışabildiği gösterilmiştir. Bunun üzerine de basit ve gerçek-zamanda hesaplanabilecek bir veri-merkezli güven modeli (data-centrict trust model) önerilmiş ve veri iletişimi sırasında verinin güvenilirliğinin anlık olarak hesaplanabilmesinin önemine vurgu yapılmıştır. Ortaya konulan bu çalışmalarla veri güvenilirliğinin nesnel bir şekilde belirlenebildiği ve yanlış/sahte veriyle doğrusunun ayırt edilebildiği gösterilmiştir.

1 Giriş

Araçsal tasarsız ağların dağıtık ve hızla değişken yapısı onların yanlış mesaj iletme/üretme, gelen mesajın iletilmemesi ya da düşürülmesi gibi birçok sorunla karşı karşıya kalmasına neden olmaktadır. Söz konusu güvenlik problemleri daha önceden (örneğin MANET'ler için) önerilmiş yöntemler araçsal ağlara uygun olmadığı için çözülememektedir. Buna karşın ağdaki tüm uygulamalar taraflar arasında veri iletişimine dayanmakta ve verinin güvenilirliği ve doğruluğu büyük önem taşımaktadır. Tüm bu sorunların çözümü için güven modeli öne sürülmüştür. Bu bağlamda güven modelini bir düğümün başka düğümün güvenilirliğini değerlendirmek ya da dürüst olmayan/zararlı düğümleri ve sahte verileri ayırt etmeye yarayan bir sistem olarak nitelendirebiliriz. Değerlendirme türüne göre güven modeli, veri-merkezli ve varlık-merkezli olarak ikiye ayrılmaktadır. Varlık-merkezli güven modeli zararlı düğümlerin belirlenmesi ve güvenilir veri iletimini temin etmek adına araçların güvenilirliği ile ilgilenirken, veri-merkezli güven modeli ise başka araçlar tarafından rapor edilen verinin doğruluğu araştırarak uygulamaların güvenli ve etkin çalışmasını amaçlar. Bununla birlikte her ikisinin de birbiriyle etkileşim içinde olduğu söylenebilir.

En sık karşılaşılan problemlerden araçsal tasarsız ağlardaki dinamik yapının neden olduğu, bir aracın verinini ve ya başka aracın güvenilirliğini gerçek zamanda, anlık olarak değerlendirememesi olarak gösterilebilir. Bir diğer sorun ise bu açık yapının araçlar arasında yeterince bilgi toplayıp bir sonuca varmak için yetersiz olduğu. Bu bağlamda güvenilirliğin zamanında değerlendirilebilmesi ve uygulamaların güvenliğinin ve etkinliğinin arttırılması için makale boyunca iki ayrı güven modeli öne sürülmüştür. Ana iki sorun üzerinde duran araştırma, güven modelinin dinamik bir yapıya kavuşturulması ve veri kalitesi ile araç güvenilirliği arasındaki bağı inceler. Öne sürülen çözüm; makalede tanımlanan veri ve araç ağırlık değerleri ile veri türü ve araç türünü de ilişkilendirerek dinamik bir varlık-merkezli güven modeli oluşturmaktadır. Yapılan detaylı analiz ve benzetimler sonucu yönlendirme protokolündeki başarımın bir miktar düşmesine karşılık güven modelinin karadelik saldırısı (blackhole attack) ve seçimli-iletim saldırısına (selective-forwarding attack) karşı direnip, ağın güvenli ve etkin yapısını koruyabildiği gösterilmiştir. Varlık-merkezli güven modelinin yanında bir de veri, veriyi raporlayan düğüm, konum ve zaman değerlerini kullanarak hesaplanan hafif (lightweight) bir veri-merkezli güven modeli önerilmiştir. Önerilen veri-merkezli modelin güvenilirliği nesnel bir şekilde sağladığı ve güvenli veri elde edilmesini kolaylaştırdığı gösterilmiştir.

2 Literatür Özeti

İlgili çalışmalar makalede üç kategoriye ayrılmıştır. Bunlardan ilki varlık-merkezli güven modeli (entity-centric trust model) araçların davranış eğilimlerinin ölçerek güvenilirliğini hesaplamaya ve bencil ya da zararlı düğümlerin ağdan dışlanarak ağdaki taraflar arasında güvenilir mesaj iletimini amaçlar. Varlık-odaklı

(araç-odaklı) güven hem veri güveninin temelini oluşturur, hem de güvenilir veri de araç güvenini temin ederek birbirini karşılıklı besler. Bu bağlamda güvenilir yönlendirmenin sağlanabilmesi için varlık güveninin temel bileşen olduğu söylenebilir.

Literatürde var olan varlık-odaklı güven algoritmaları genellikle düğümler arası daha önceki karşılaştırmaları temel alarak güven değeri hesaplamaya dayanmaktadır. Buna ek olarak çoğunlukla söz konusu düğüme karşı komşu düğümlerin de güven değerleri toplanarak genel güven değerine ulaşılır. İlk yaklaşıma doğrudan güven (direct trust), ikincisineyse önerilen güven (recommend trust) adı verilir. Güvenin nesnel/tarafsız bir şekilde ele alınabilmesi için çoğunlukla iki güven türü (doğrudan ve önerilen) arasında sabit bir katsayı (ya da ağırlık) değeri kullanılarak son değere ulaşılır. Buna ek olarak bulanık mantık ve ya Bayesian yaklaşımlar da sıklıkla kullanılmakta ancak bunlar da daha önceki etkileşimleri temel alarak çalışmaktadır. Buna karşın, araçsal tasarsız ağların değişken yapısı düğümlerin daha önceden birbiriyle denk gelmediği durumları da karşımıza çıkarabilir. Böylesine bir senaryo, düğüm hakkında öncesinde yeterince bilgi toplayamama anlamına gelmektedir.

Makalede üstünden kısaca geçilmiş olsa da bu alanda yapılan çalışmaların ya belirli uygulamaları hedef alan ve güven değerini güncellemek için zaman çerçevesini ayarlayan ya da uygulanamayacak kadar karmaşık yöntemlerin olduğu belirtilmiştir. Makaledeyse periyodik olarak güven değerinin hesaplanması yerine düğümler arası etkileşim esnasında güven değerinin hesaplanması öngörülmüştür.

Bir diğer kategori olan veri-odaklı güven (data-centric trust) ise verinin kalitesi ve güvenilirliği ile ilgilenmekte ve sahte ya da yanlış verinin belirlenmesi için bir model öne süren algoritmaları içermektedir. Çoğu araştırma düğümden çok verinin güvenilirliğine odaklanmaktadır. Yöntem olarak ise genellikle zaman yakınlığı, konum yakınlığı, aynı olaya ilişkin rapor sayısı, olayın türü gibi farklı kıstaslar hesaba katılmaktadır. Raya et al. veri-merkezli güven için bir olaya ilişkin birden fazla mesajı topladıktan sonra ağırlıklı bir hesaplamayla genel kanıya varılan bir çözüm önermiştir. Wu et al. ise yol-kenarı birimlerin (RSU) de yardımıyla aracın olaya uzaklığı, aracın maksimum sensör menzili, araçtaki olayı belirleyebilecek sensor sayısı ve aracın ağırlıklı değeri gibi birden fazla metriği bir araya getirerek güvenilirliği hesaplama yoluna gitmiştir. Ding et al. ise düğümleri rollerine göre ayırarak verinin sahte ya da doğru olduğunu belirleyen itibar (reputation) temelli bir sistem öne sürer.

Önerilen farklı modeller farklı fikirler içerse de temelde verinin güvenilirliğinin ölçülmesini hedeflemekte, bu amaçla oy çoğunluğu (majority voting), en güvenilir rapor (most trusted report), ağırlıklı oylama (weighted voting), Bayesian çıkarım (Bayesian inference) ve Dempster-Shafer Theory (DST) gibi yöntemler kullanır. Her birinin artısı eksisi var olmakla birlikte makalede belirtilen genel eksiklik olarak hepsinin güvene dayalı kararı vermesinin uzun zaman aldığı vurgusu yapılmıştır.

Üçüncü ve son kategori olarak nitelendirilebilecek birleşik güven (combined trust) ise verinin güvenilirliği için aracın güven değerini kullanmakta ve her iki modeli bir şekilde entegre etmektedir. Genellikle yol-kenarı birimler ve ya *beacon* temelli çözümlerin olduğu belirtilmekte ancak birleşik güven alanında oldukça az çalışma olduğu ve bir çoğunun her iki modeli yeterince birbirine yediremediği öne sürülmüştür.

Son olarak ise makalede incelenen ilgili çalışmalarda ortak konu olan güven metriğinin üstünde durulmuştur. Buna göre, yaygın olarak uzaklık (araçtan olaya, gönderen ile alıcı araç, gönderen ile yol-kenarı birim, olay ile yol-kenarı birim gibi), zaman yakınlığı ve diğer araçların önerilen güvenleri kullanılmıştır. Bununla birlikte aracın hızı, pozisyonu, yönü ile aynı olayı gönderen araç sayısı, aracın türü gibi diğer metriklere de rastlanır.

3 Yöntem

Kullanılan yöntemin ayrıntılarına girmeden önce makalede kullanılan bir takım varsayımların açıklanması gerekmektedir.

3.1 Varsayımlar

Ağ modeli

Araçsal tasarsız ağlarda çoğunluğu farklı çeşitlerde araçlar olmak üzere düğümler ya araçtır ya da yol-kenarı birimlerdir. Araçlar farklı hızlarda farklı hedeflere doğru hareket halinde olduğundan ağ topolojisi sürekli değişim halindedir. Makalede genellikle sürücülerin günlük sürüş alışkanlıklarının tutarlı ve aynı olduğu ve buna bağlı olarak aynı yolda aynı saatler üzerinde çoğunlukla aynı araçların seyahat halinde olduğu ve böylelikle farklı araçların belirli bir olasılıkla birbiriyle karşılaşabileceğine vurgu yapılmıştır. Bu varsayıma göre araçların birbiriyle ilgili yeterli bilgiyi daha önceki etkileşimlerinden elde edilebileceği sonucu çıkarılmıştır.

Bununla birlikte tüm araçların akıllı sensörler, hesaplama modülleri, kablosuz haberleşme modülü, GPS gibi birimler ile donatıldığı varsayılmıştır. Bu sayede araçlar kendi konumlarını kesin bir şekilde belirleyebilmekle birlikte aynı zamanda 20m mesafedeki trafik olaylarını kesin bir şekilde algılayabilecekleri de bu varsayıma eklenmiştir. Haberleşme içinse menzil 200m olarak belirlenmiştir. Tüm araçların zaman-senkronizasyon tekniği olmadan aynı zaman diliminde aynı saate sahip oldukları buna ilaveten ulaştırma ile ilgili yetkili kurumun (transportation authority organizations/TA) araçların kayıt işlemi sırasında açık sertifikalarını (public certificates) dağıttığı, araçları ve sertifikaları periyodik olarak kontrol ettiği de belirtilmiştir. Son olarak da TA'nın açık anahtarının tüm araçlarca önceden bilindiği ve araç türünün de TA tarafından imzalanmış olduğu belirtilmiştir.

Uygulama modeli

Araçsal tasarsız ağlarda kullanılan uygulamaların işlevlerine göre üç ana kategoriye ayrıldığı (güvenlik, verimlilik ve bilgi/eğlence) belirtilmiştir. Güvenlik uygulamaları kaza uyarısı, kör nokta uyarısı, tehlikeli yol durumu gibi kamu ve birey güvenliğini arttırmaya yönelik iken, verimlilik uygulamaları trafiğin etkin bir şekilde kullanılabilmesini amaçlayacak şekilde trafik kontrol, park bilgisi gibi uygulamalardan oluşur. Son kategori, bilgi/eğlence ise reklam ve eğlence uygulamarı gibi uygulamaları kapsar. Bu kapsamda tüm uygulamalar bu kategorilere ayrılacak şekilde bir ayrıştırma yapılmıştır:

Güvenlik uygulamarı (*S*): {arka kaza, ciddi kaza, arıza, kör nokta, buzlu yol, kaygan yol, yoğun sis, keskin viraj}

Verimlilik uygulamaları (*E*): {trafik sıkışıklığı, yol bakım, kapalı yol, park yeri, gaz istasyonu}

Bilgi/eğlence uygulamaları (I): {kupon, şarkı, müzik, manzara, restoran, bar}

Ağda raporlanan herhangi bir olayın (verinin) bu kategorilerden birine ait uygulama tarafından oluşturulduğu varsayılmıştır. Gönderilen mesaj formatı ise aşağıdaki gibidir:

Olay türü	Olay konumu	Olayın gerçekleşme zamanı	Raporlayanın türü	Raporlayanın konumu	Olay tanımı	Raporlayan Hash(ID)	Raporlayanın imzası

Şekil 1. Veri formatı

Mesaj formatında *raporlayan türü* dışındaki tüm alanlar raporlayan düğüm tarafından oluşturulurken raporlayan türü ağ modelinde de belirtildiği gibi aracın kaydı sırasında TA tarafından üretilip imzalanır ve $Sign(K_M, hash(ID_K||t(v_K))$ şeklinde gösterilir. Burada ID_K, k aracının biricik (ID) değeri , $t(v_K)$ ise aracın türüne karşılık gelir.

Güvenlik modeli

Araçsal tasarsız ağlarda varlık merkezli güvenin yavaş değiştiği ve daha önceki etkileşimlerden etkilendiği söylenebilir. Bu kapsamda önerilen model; 1) Doğrudan güven değerinin iki düğüm arası etkileşimden sonra güncellendiği 2) Doğrudan güven ön-tanımlı bir eşik değerden küçük olduğundan önerilen güven ve kapsamlı güvenin hesaplandığı varsayılmıştır.

Veri güvenilirliğinin ise diğer birçok etmenin yanında raporlayan düğümün güvenliği, zaman yakınlığı, konum yakınlığı ve veri ile raporlayan arası ilişkiye dayandığı söylenebilir. Varlık-merkezli güvenin aksine veri-merkezli güvenin olaydan etkilendiği ve dinamik, uçucu (*volatile*) bir yapıya sahip olduğundan

bahsedilebilir ve bu anlamda gelen verinin güvenilirliğinin gerçek zamanlı, anlık olarak hesaplanabilmesi önem arz eder.

Son olarak da güven değeri [0, 1] arası bir değere sahip olmakla birlikte ve 1 değeri mutlak güven, 0.5 değeri belirsizlik ve 0 değeri mutlak güvensizlik anlamına gelmektedir.

3.2 Varlık-merkezli güven modeli

Varolan varlık-merkezli güven modellerine benzer şekilde makalede önerilen model de doğrudan güven ve önerilen güvene dayanmaktadır. Ancak öncekilerin aksine farklı uygulama türleri ve düğüm rollerine göre bir ağırlık değeri önerilmiştir. Bununla birlikte araçsal ağların değişken yapısını karşılamak adına doğrudan güven ile önerilen güvenin birleştirilmesi için dinamik bir katsayı da kullanılmıştır.

Ağırlık tanımları

Uygulama verisi ağırlığı

Farkı uygulamaların farklı güvenilirlik ihtiyaçları olduğu ve farklı uygulamalara dair verinin ağın, bireyin ve kamunun güvenliğini farklı şekilde etkilediği göz önünde bulundurulduğunda daha önceden anlatıldığı üzere uygulama türlerine karşın farklı ağırlıkların tanımlanması ihtiyacı doğmuştur.

$$W_D(x) = \begin{cases} 1, & x = S \\ 0.8, & x = E \\ 0.5, & x = I \end{cases} \quad (1)$$

Burada uygulama verisinin ağırlığı aslında ağda ne kadar önemli olduğunu vurgulamaktadır ve iletilen herhangi bir veri bu üç türden birine aittir.

Düğüm ağırlığı

Araçsal tasarsız ağlarda düğümlerin çeşitli ve farklı otoritelerde olduğu bellidir. Özel araçlar olarak nitelendirilebilecek (polis aracı, yol-kenarı birim gibi) araçların yüksek-seviye öneme/otoriteye (H) sahip olduğu, hizmet araçlarına (otobüs, ambulans, yol bakım araçları, çöp kamyonları gibi) ait araçların orta-seviye (M) öneme sahip olduğu, şahıs araçlarınınsa (özel araç, taksi gibi) düşük-seviye (L) öneme sahip olduğu bir kategorizasyon önerilmiştir. Bu üç kategorizasyona göre aşağıdaki çizge sunulmuştur:

$$W_N(x) = \begin{cases} 1, & x = H \\ 0.7, & x = M \\ 0.5, & x = L \end{cases} \quad (2)$$

Bu düğüm ağırlığı aracın ve bir dereceye kadar da aracın raporladığı verinin güvenilirliğine etki etmektedir. Araçsal tasarsız ağlardaki tüm düğümler bu üç seviyeden birine tabidir.

Varlık-merkezli güven modelinin tanımı

Güven modelinin çıktısı, kapsamlı güven, doğrudan güven ve önerilen güvenin bir araya gelmesinden oluştuğu için güven modeli aşağıdaki gibi üç kısımda incelenecektir. Model ve denklemlerde kullanılan gösterimlere ait tanımlar Tablo1'den incelenebilir.

Tablo 1. Gösterimler

Gösterim	Tanım
N_A^B	Düğüm A'nın düğüm B'den iletmesini istediği toplam mesaj sayısı
M_A^B	Düğüm A'nın düğüm B'den iletmesini istediği mesajlardan başarılı şekilde gönderilen sayısı

W_D^X	Uygulama verisinin ağırlığı
W_N^A	Düğüm ağırlığı
$U_W^{A,B}$	Düğüm A'nın düğüm B'den iletmesini istediği mesajların toplam ağırlığı
$S_W^{A,B}$	Düğüm B'nin düğüm A için başarılı şekilde ilettiği mesajların toplam ağırlığı
$E_{TW}^{A,B}$	Düğüm A'nın düğüm B'den iletmesini istediği mesajların ortalama ağırlığı ($E_{TW}^{A,B}=U_W^{A,B}/N_A^B$)
$E_{SW}^{A,B}$	Düğüm B'nin düğüm A için başarılı şekilde ilettiği mesajların ortalama ağırlığı ($E_{SW}^{A,B}=S_W^{A,B}/M_A^B$)
F_W^B	Düğüm B'nin zararlı eğilimi
DT_A^B	Düğüm A'nın düğüm B'ye yönelik doğrudan güven değeri
RT_A^B	Düğüm A'nın düğüm B'ye yönelik önerilen güven değeri
T_A^B	Düğüm A'nın düğüm B'ye yönelik kapsamlı değeri

Doğrudan güven

Doğrudan güven bir düğümün başka bir düğümün gelecekteki davranışına ilişkin beklentisi olarak tanımlanabilir. Araçsal tasarsız ağların değişken yapısı nedeniyle burada iki durumdan biri geçerlidir: ya iki düğüm/araç birbiriyle daha önce hiç karşılaşmamıştır ya da karşılaşmıştır yani eski etkileşimlere dair bilgisi vardır.

Daha önceden karşılaşıldığı durumda düğüm diğer düğümün başarılı bir şekilde ilettiği veri oranına bakar. Genellikle yüksek veri iletim oranına sahip düğümün güvenilirliği de yüksektir. Ancak sadece bu değere bakılarak yapılan yorum, bazı zararlı düğümlerin sadece düşük ağırlıklı, düşük öneme sahip (ve ya kendi çıkarına olan) paketleri ilettiği durumu yakalamakta başarısız olur. Örneğin sadece bilgi/eğlence türü uygulama verisini iletip güvenlik verisini iletmeyen düğümler bu sınıfa dahildir. Öyleyse bu sorunu aşmak adına, *zararlı eğilim* (malicious tendency) adı verilen bir tanım öne sürülmüştür. Aşağıdaki formül ile hesaplanan zararlı eğilim *iletimi başarısız olan ortalama veri ağırlığını* hesaplar.

$$F_W^B = \left(U_W^{A,B} - S_W^{A,B}\right)/\left(N_A^B - M_A^B\right) \tag{3}$$

Makalede belirtilene göre güvenlik (S), verimlilik (E) ve bilgi/eğlence (I) türü uygulamaların trafikte oranı sırasıyla; 0.2, 0.4, 0.4 şeklindedir. Her birinin uygulama ağırlığıyla çarpıldığında, ortalama veri ağırlığı (1 x 0.2 + 0.8 x 0.4 + 0.5 x 0.4) = 0.72 olarak bulunur. Bu da önerilen modelde zararlı eğilim için eşik değer olarak kullanılır. Yani $F_w^B < 0.72$ ise düğümün zararlı eğilimi yoktur, aksi taktirde zararlı eğilimi olan düğümdür.

Doğal bir gereksinim gereği doğrudan güven doğru davranışı daha az ödüllendirirken, zararlı davranışı daha fazla cezalandırır. Bu analiz kapsamında düğüm A'nın düğüm B'ye karşı doğrudan güven değeri aşağıdaki gibi hesaplanır:

$$DT_A^B = \begin{cases} \dfrac{W_D^x \cdot \left((Flag+1)/2 - DT_A^B\right)}{1 + E_{TW}^{A,B}/E_{SW}^{A,B}} + DT_A^B, F_W^B < 0.72 \\ W_D^x \cdot \left((Flag+1)/2 - DT_A^B\right)/4 + DT_A^B, \\ \quad (Flag = 1) and (F_W^B \geq 0.72) \\ W_D^x \cdot \left((Flag+1)/2 - DT_A^B\right) + DT_A^B, \\ \quad (Flag = -1) and (F_W^B \geq 0.72) \end{cases} \tag{4}$$

Buradaki bayrak (flag) değeri düğüm B'nin paket iletip iletmediğini (ilettiyse flag=1, değilse flag=0) gösterir. Denklem incelendiğinde zararlı eğilimi olmayan ($F_w^B < 0.72$) düğüm B söz konusu ise doğrudan güvenin başarılı paket iletim oranında (bayrak değerine göre) artıp azaldığı görülmektedir. Düğüm B'nin zararlı eğilime sahip olduğu durumda ise eğer paket başarılı bir şekilde iletildiyse doğrudan güven değeri (dörtte bir oranında) çok az arttırılırken, paket iletimi başarısız olduysa doğrudan güven veri ağırlığı oranınca (daha çok) azaltılır.

Eğer iki düğüm daha öncesinden karşılaşmadıysa doğrudan güven değeri düğüm B'nin ağırlığı olarak ilklendirilir.

Önerilen güven

Önerilen güven değeri, diğer düğümlerin düğüm B'ye karşı güven değerlerini içermektedir ve sadece doğrudan güven ile oluşturulan tek yönlülüğün/öznelliğin dengelenmesi için kullanılmaktadır. Önerilen güven değeri aşağıdaki denlemdeki haliyle düğüm A'nın komşuya olan güveni, komşu düğümün düğüm B'ye olan güveni ve komşu düğümün ağırlığı şeklinde hesaplanır.

$$RT_A^B = \frac{\sum_{i=1}^{n} DT_A^{N_i} \cdot T_{N_i}^B \cdot W_N^{N_i}}{\sum_{i=1}^{n} DT_A^{N_i}}, \quad N_i \neq B \tag{5}$$

Kapsamlı güven

Kapsamlı güven değeri, doğrudan güven ile önerilen güven değerlerinin bir araya getirilmesiyle elde edilir. Bir düğümün farklı düğümlerle farklı geçmiş etkileşimleri olduğu göz önünde bulundurulursa doğrudan güven değerinin sabit bir katsayı ile kapsamlı güvene katılmasının yanlış bir yaklaşım olacağı ve buraa dinamik bir katsayının kullanılması gerektiğine vurgu yapılmıştır. Örneğin eğer düğüm A, düğüm B'yi oldukça tanıyorsa doğrudan kendi güven değerine başvurabilirken önerilen güven değeri önem taşımaz, ancak düğüm B yabancı ise ya da düğüm A'nın doğrudan güven değeri belirli bir eşik değerin altındaysa bu durumda önerilen güven de devreye girer. Burada dengeyi sağlayabilecek dinamik bir α katsayı öne sürülmüştür:

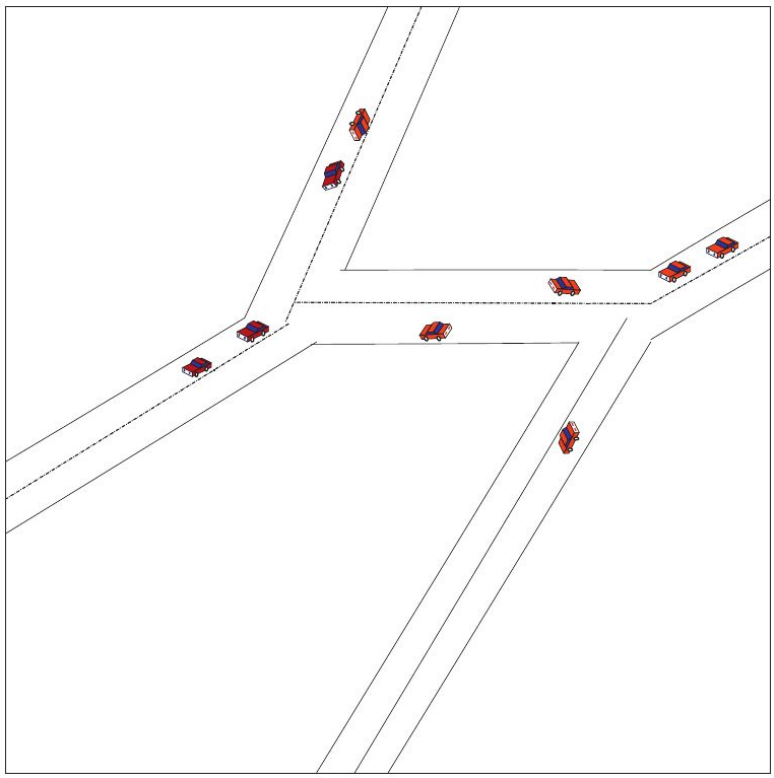
$$\alpha = \begin{cases} 1, DT_A^B \in (0.7, 1] \text{or} DT_A^B \in [0, 0.3) \text{or} W_N^B = 1 \\ DT_A^B, DT_A^B \in [0.5, 0.7) \\ W_N^B \cdot DT_A^B, DT_A^B \in [0.3, 0.5) \end{cases} \tag{6}$$

Katsayının doğrudan güven ve/ve ya düğüm B'nin ağırlığına göre değiştiği ve bu sayede doğrudan güven ile önerilen güven değerleri arasında bir denge oluşturduğu görülebilir. Katsayıyı temel alarak, dinamik varlık güven modeline ait kapsamlı güven değeri aşağıdaki gibi bulunabilir:

$$T_A{}^B = \alpha \cdot DT_A{}^B + (1 - \alpha) RT_A{}^B \tag{7}$$

3.3 Varlık-merkezli güven modeli için benzetim sonuçları

Varlık-merkezli güven modeli araçsal tasarsız ağlarda güvenilir yönlendirmedeki temel bileşenlerden biri olduğu için, benzetim sırasında da yönlendirme protokolleri üzerinden denenecektir. Bu bağlamda, GPSR algoritması hem düğümlerin konumuna doğrudan bağlı olduğu hem de güven ile yakından ilişkili olduğundan temel yönlendirme protokolü olarak seçilmiştir. Makalede önerilen model (bundan sonra T-GPSR olarak adlandırılacaktır) GPSR üzerine eklenen güven mekanizmasından oluşmaktadır.



Şekil 2. Trafik topolojisi

Benzetim ortamı

Benzetimin gerçek hayata uygun olması için MobiSim aracı seçilmiş ve ilgili trafik topolojisi aşağıdaki (Şekil 2) gibi verilmiştir. Buna ek olarak benzetim ortamının parametreleri Tablo 2'de tanımlanmıştır.

Tablo 2. Benzetim ortamı ve parametreleri

Ortam ve parametre	**Değer**
İşletim sistemi	Windows 7
Programlama dili	Java
Benzetim alanı	1000m x 1000m
Yönlendirme protokolü	GPSR, I-GPSR, T-GPSR
Düğüm sayısı	50,70,90,110,130,150,170
Bir hop menzili	200m
Bant genişliği	2 Mbit/s
Hello paketleri aralığı	Tekdüze dağılım(0.9,1.0)
Paketlerin maksimum büyüklüğü	4096 bit veya 512 Byte
Veri paketleri aralığı	Üstel dağılım (12s)
Hareket hızı	0 m/s~18m/s

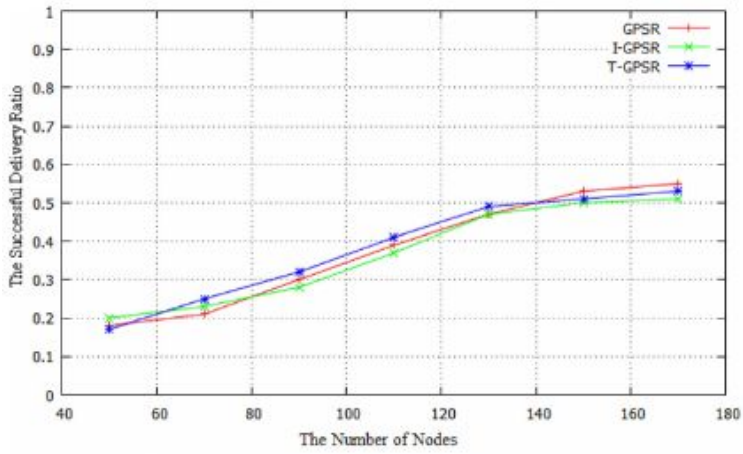
Benzetim çalıştırma süresi	1000s
Güven eşik değeri	0.6

Önerilen varlık-merkezli güven modelinin amacı zararlı, bencil düğümlerin ayırt edilip, onlardan kaçınılması olarak nitelendirilebilir. Söz konusu deneylerde saldırının olmadığı, kara delik saldırısının olduğu ve seçimli-iletim saldırısının olduğu üç ayrı senaryo ayrı ayrı denenmiştir. Karşılaştırma amacıyla GPSR, T-GPSR ve I-GPSR sırasıyla üç senaryoda de denenmiştir. Buna ek olarak; *paket iletim oranı*, *yol uzunluğu* ve *ortalama sondan sona gecikme* metrikleri de her bir protokol için ölçülmüştür.

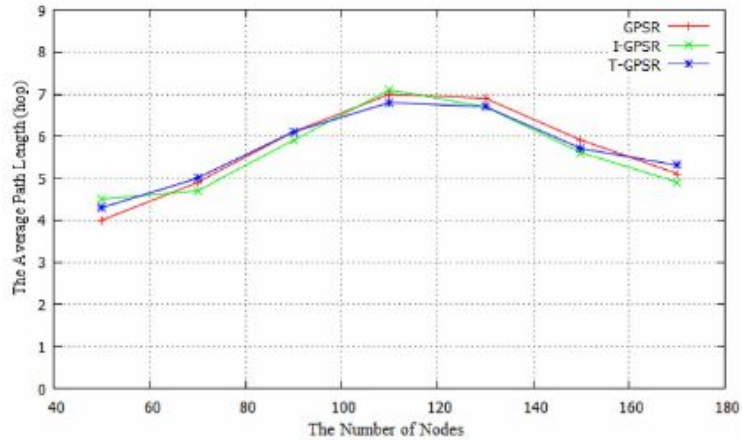
Karşılaştırmalı Analiz

Aşağıdaki şekillerde sonuçları verilen benzetimler her bir senaryo için 10 kez çalıştırılmış değerlerin ortalaması alınarak elde edilmiştir.

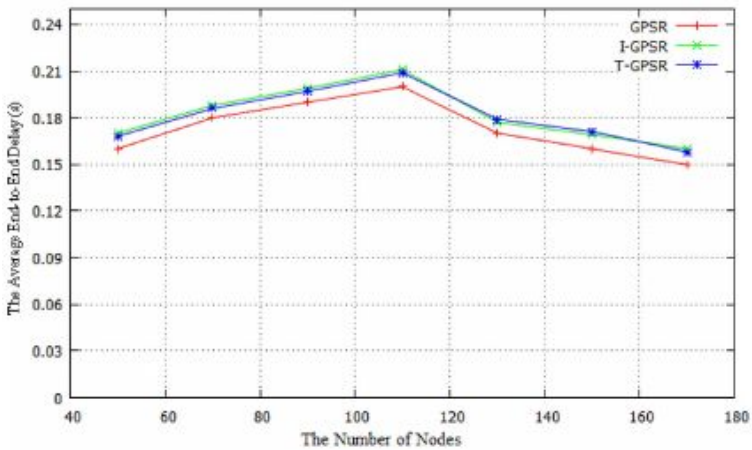
1) Saldırısız senaryo. Saldırının olmadığı senaryodaki sonuçlar Şekil 3'te görülebilir. (a) ve (b) şekillerinden de görülebileceği gibi 3 GPSR protokolünün de paket iletim oranı ve yol uzunluğu açısından değerleri aynıdır. Ancak ortalama sondan-sona gecikme değerinde I-GPSR ve T-GPSR'nın birbiriyle benzer sonuç verdiği ancak GPSR'nın daha düşük değer verdiği görülmektedir. I-GPSR ve T-GPSR'daki gecikmenin sebebi olarak GPSR'a kıyasla fazladan yapılan güven hesaplaması gösterilmektedir. Buna karşın, gecikmenin sistemin başarımını göz ardı edilemeyecek kadar etkilemediğine makalede vurgu yapılmıştır.



(a) The Data Delivery Ratio

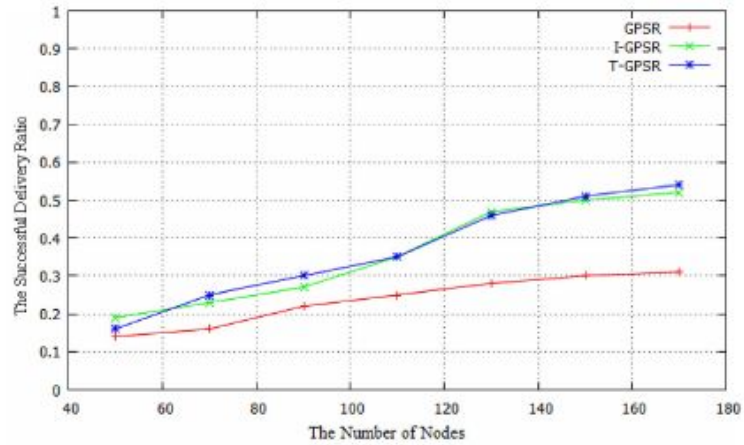


(b) The Average Path Length

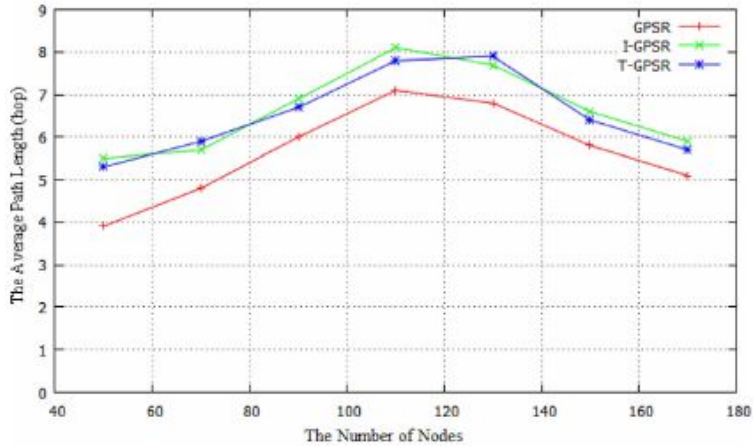


(c) The Average End-to-End Delay

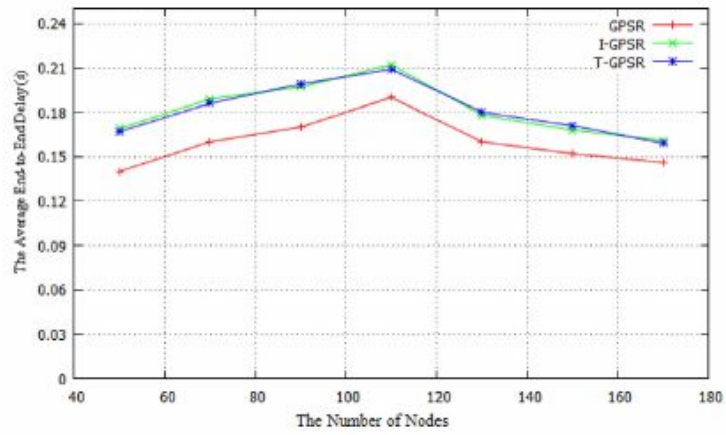
Şekil 3. Saldırısız senaryodaki benzetim sonuçları



(a) The Packet delivery Ratio



(b) The Average Path Length



(c) The Average End-to-End Delay

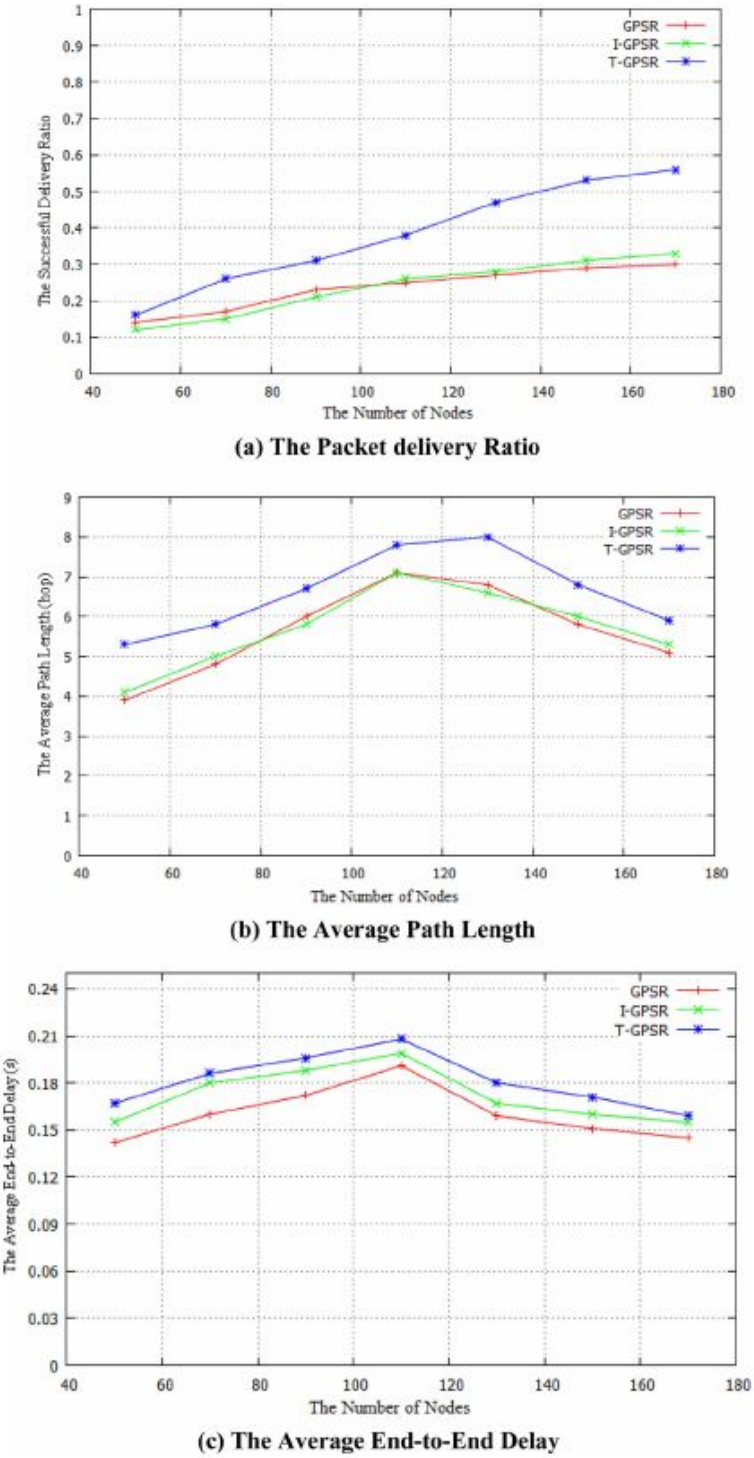
Şekil 4. Kara delik saldırının olduğu senaryodaki benzetim sonuçları

2) Kara delik saldırısının olduğu senaryo. Zararlı düğüme gelen her paketin düşürüldüğü bu senaryonun sonucu Şekil 4'te verilmiştir. Şekil 3 (a) ile Şekil 4 (a) arasında karşılaştırma yapılacak olursa I-GPSR ve T-GPSR'ın her ikisininde de neredeyse aynı olduğu ancak GPSR değerinin düştüğü görülmektedir. Nedeni olarak ise I-GPSR ve T-GPSR'ın kara delik saldırısına karşı koyabildiği ancak GPSR'ın koyamadığı ortaya sürülebilir.

Şekil 4 (b)'deki ortalama yol uzunlukları I-GPSR ve T-GPSR için Şekil 3'tekine kıyasla artmıştır, bunun nedeni ise zararlı düğümün keşfedilip daha uzun yol belirlenmesi olarak nitelendirilebilir. GPSR ise her iki durumda aynı şekilde davranmış ve makaledeki açıklamaya göre zararlı düğüme şans eseri denk gelmemiştir.

3) Seçimli-iletim saldırısının olduğu senaryo. Sadece düşük ağırlıklı, düşük öneme sahip ve ya kendi çıkarına olan paketleri ileten zararlı düğümün olduğu senaryonun sonuçları Şekil 5'te verilmiştir. Şekil 5 (a)'da görülebildiği üzere GPSR ve I-GPSR'ın veri iletim oranı neredeyse birbiriyle aynı, T-GPSR'ınki ise diğerlerinde çok daha fazla ve saldırının olmadığı durumdakiyle aynıdır. Söz konusu sonuç, I-GPSR ve GPSR'ın zararlı düğüme karşı koyamadığını ancak T-GPSR'ın başarılı bir şekilde zararlı düğümü belirleyebildiğini göstermektedir. Şekil 5 (b)'de ise T-GPSR'ın ortalama yol uzunluğunun diğer ikisinden uzun olduğu, bunun nedenininse zararlı düğümü belirleyip daha uzun yol seçmesi olarak açıklanabilir.

Ortalama sondan-sona gecikme değeri, Şekil 5 (c), ise T-GPSR'ın her ikisinden de fazla, I-GPSR'ınki ise GPSR'dan fazla olduğu görülmektedir. Burada I-GPSR'ın güven değerlendirmesi yapması nedeniyle GPSR'dan daha yüksek gecikmeye sahip olduğu, T-GPSR'ın ise zararlı düğümü belirleyerek daha fazla hesaplama yapmasına gerek olduğundan I-GPSR'dan da yüksek gecikmeye sahip olduğu anlamı çıkarılmıştır.



Şekil 5. Seçimli saldırının olduğu senaryo sonuçları

3.4 Veri-merkezli güven modeli

Araçsal tasarsız ağlarda veri iletişiminin olabildiğince hızlı olmasının gerekliliklerden biri olarak veri güvenilirliğini değerlendiren yöntemlerin de olabildiğince basit olması gerekir. Bu kapsamda varolan veri güven modellerinin aksine basit ve hafif bir model önerilmiş ve modeli oluşturan ana çarpanlar/etmenler aşağıdaki başlıklarda tanımlanmıştır.

Aşağıdaki başlıklarda kullanımlar gösterimlerin tanımları Tablo 3'te verilmiştir.

Tablo 3. Veri-merkezli modeldeki gösterimler

Gösterim	Anlamı
B_{λ}^{V}	Düğüm v tarafından üretilen λ olayının/verisinin güvenilirliği
T_{A}^{B}	Düğüm A'nın düğüm B'ye güveni
T(v)	Düğüm v'nin türü
T(λ)	Veri/olayın türü
M(T(V), T(λ))	Düğüm v ile olay λ arasındaki bağıntılı güvenilirlik
$\mu_l(V,\lambda)$	Coğrafi konum olarak yakınlık
$\mu_t(V,\lambda)$	Zaman olarak yakınlık

Çarpanların tanımı

Varolan veri-merkezli güven modellerine benzer şekilde, veri güvenilirliği; raporlayanın güvenilirliği, olay ile raporlayan arası bağıntılı güvene, raporlayının konum ve zaman olarak olaya yakınlığı gibi bir çok etmene dayanmaktadır. Makalede veri güvenilirliği için odaklanılan 4 adet ana çarpan vardır, bunlar:

1) Veriyi raporlayanın güvenilirliği

Raporlayanın güvenilirliği bir önceki kesimlerde öne sürülen T_A^B değeriyle temsil edilir. Varsayılan değeri düğümün ağırlığıdır.

2) Olay ile raporlayan arası bağıntılı güvenilirlik

Belirli bir olay/veri için, düşük otoriteye/öneme sahip bir düğümün yüksek otoriteye sahip bir düğümden daha güvenilir olması ya da aynı otorite seviyesindeki iki aracın farklı güvenilirliklerinin olması olasıdır. Bunun nedenlerinden biri olarak kabaca üçe ayrılan düğüm ağırlığı gösterilebilir. Bu bağlamda araçlar 10 ayrı kategoriye ayrılarak aşağıdaki M_T matrisi oluşturulmuştur.

Table 4. Güven matrisi

Düğüm türü	Güvenlik uyg.	Verimlilik uyg.	Bilgi/eğlence uyg.
Yol kenarı birim	1	1	1
Polis aracı	1	1	0.7
Yol bakım aracı	0.8	1	0.7
Ambulans	1	1	0.5
Otobüs	0.8	0.8	1
Mühendislik araçları	0.7	0.8	0.5
Çöp kamyonu	0.7	0.8	0.7
Taksi	0.7	0.7	1
Özel/şahsi araçlar	0.7	0.7	0.8
Nakliye aracı	0.7	0.7	0.7

3) Coğrafi konum olarak yakınlık

Olayı raporlayan olay konumuna ne kadar yakınsa olay hakkında o kadar isabetli ve doğru bilgiye sahip olur. Bu yaklaşımla yola çıkılarak olay konumuna yakın olan düğümlerin güvenilirliğinin daha yüksek olması beklenmektedir. Burada raporlayan araç v'nin konumu ile olayın yerelliği arasındaki ilişkiye bağlı olarak uzaklık tanımı aşağıdaki gibi tanımlanmıştır.

$$\mu_l(v,\lambda) = \begin{cases} 1 & d \le 10m \\ 0.9 & 10m < d \le 20m \\ 0.8 & 20m < d \le 50m \\ 0.7 & 50m < d \le 100m \\ 0.6 & 100m < d \le 200m \\ 0.4 & 200m < d \le 500m \\ 0 & d > 500m \end{cases} \quad (8)$$

4) Zaman olarak yakınlık

Raporlayanın konumu ile verininki arasındaki uzaklığa benzer şekilde, olayın oluştuğu an ile raporlandığı an arası da ne kadar kısaysa o kadar doğru, isabetli sonuç elde edilmiştir. Benzer şekilde verinin de daha güvenilir olduğuna vurgu yapılır. İstatistiksel olarak olayların (kaza, sıkışıklık gibi) genellikle 5 dakika ile 1 saat arasında çözülmesi temel alınarak aşağıdaki yakınlık tanımı yapılmıştır.

$$\mu_t(\mathrm{v},\lambda) = \begin{cases} 1 & t \le 5min \\ 0.9 & 5min < t \le 10min \\ 0.8 & 10min < t \le 20min \\ 0.7 & 20min < t \le 30min \\ 0.5 & 30min < t \le 45min \\ 0.3 & 45min < t \le 60min \\ 0 & t \ge 60min \end{cases} \quad (9)$$

Katsayıların tanımı

Tanımlanan bu dört çarpanın (raporlayanın güvenilirliği, raporlayan ile olay arasındaki bağıntı, konum olarak yakınlık, zaman olarak yakınlık) veri güvenilirliğine etkisi farklıdır ve bunlar arasındaki ilişkiyi tamamlayacak bir katsayıya ihtiyaç vardır.

Doğal olarak güvenilmez bir düğümün raporladığı verinin de güvenilmez olduğu barizdir bu nedenle veri güvenilirliğinde raporlayanın güven değerine yeterli önemin verilmesi gerekmektedir. Buna ek olarak (olay λ ile raporlayan v arasındaki) bağıntılı güven değeri *M(T(v), T(λ))* de sadece olayın ve raporlayanın değil onların bağıntılı ilişkisini de ele aldığı için aynı derecede önemlidir. Bu nedenle bu iki çarpanın katsayısı 0.7 olarak belirlenmiş, geriye kalan konuma yakınlık ve zamana yakınlık ise aynı derecede öneme sahip olduğu varsayılıp 0.15 katsayısıyla ifade edilmiştir.

Veri-merkezli güven modelinin tanımı

Yukarıdaki analize dayanarak düğüm v tarafından üretilen λ olayına ait paketi alan düğüm A ilgili veri güvenilirliğini aşağıdaki gibi hesaplar.

$$B_\lambda^v = 0.7 \cdot T_A^v \cdot M(\tau(v), \tau(\lambda)) + 0.15 \cdot \mu_l(v,\lambda) + 0.15 \cdot \mu_t(v,\lambda) \quad (10)$$

Denklemden de görülebileceği gibi veri-merkezli güven modeli hızlı bir şekilde sonuca ulaşabilecek kadar basittir, denklemi oluşturan çarpanlar ya ön-tanımlı değerler ya da veri geldiğinde anlık olarak hesaplanabilecek

değerlerden oluşur. Aynı olaya ait birden fazla raporlayandan gelen verinin güvenilirliği farklı olacağından, alıcı düğüm birden fazla güvenilirlik değerinin ortalamasına bakarak verinin sahteliği konusunda karar verebilir.

Analiz

Veri-merkezli modelinin geçerliliğini sınamak adına, 3 farklı veri türüne karşılık 10 farklı düğüm türü kullanılarak veri güvenilirlik değerleri hesaplanmıştır. Basitleştirmek adına, raporlayan düğümün güvenilirliği olarak düğüm ağırlığı alınmıştır. Zaman ve konum yakınlığı değerleri içinse üç farklı senaryo oluşturulmuştur. Burada $T1_x$ x veri türüne ait en iyi konum ve zaman yakınlığına, $T3_x$ ise en kötü konum ve zaman yakınlığına denk gelir.

Güven değerlerinin görebildiğimiz aşağıdaki tabloda verinin güvenilirliğinin genellikle raporlayan düğüm ve onun veriyle olan bağıntısından etkilendiği görülmektedir. Zaman ve konum yakınlığıysa bu değeri iyileştirmek için kullanılan çarpanlar olarak işlev görmektedir. Makalede belirtildiği üzere bu değerlerin ve veri güven modelinin daha çok tecrübeye dayalı katsayı ve ön-tanımlı değerlerle oluşturulduğu ve daha sağlam temeller üzerine oturtularak iyileştirilebileceği yorumu yapılabilir.

Tablo 5. 3 senaryonun veri güvenilirliği değerlendirmesi

Raporlayan Türü	**$T1_S$**	**$T2_E$**	**$T3_I$**	**$T1_S$**	**$T2_E$**	**$T3_I$**	**$T1_S$**	**$T2_E$**	**$T3_I$**
Yol kenarı birim	1	0.91	0.7	1	0.91	0.7	1	0.97	0.7
Polis aracı	1	0.91	0.7	1	0.91	0.7	0.79	0.7	0.49
Yol bakım aracı	0.692	0.602	0.392	0.79	0.7	0.49	0.643	0.553	0.343
Ambulans	0.79	0.7	0.49	0.79	0.7	0.49	0.545	0.455	0.245
Otobüs	0.692	0.602	0.392	0.692	0.602	0.392	0.79	0.7	0.49
Mühendislik araçları	0.643	0.553	0.343	0.692	0.602	0.392	0.643	0.553	0.343
Çöp kamyonu	0.643	0.553	0.343	0.692	0.602	0.392	0.643	0.553	0.343
Taksi	0.545	0.455	0.245	0.545	0.455	0.245	0.65	0.56	0.35
Özel araç	0.545	0.455	0.245	0.545	0.455	0.245	0.58	0.49	0.28
Nakliye aracı	0.545	0.455	0.245	0.545	0.455	0.245	0.545	0.455	0.245

4 Makalenin Katkısı

Önerilen dinamik varlık-merkezli güven modelini makalenin katkısı olarak nitelendirebiliriz. Bu bağlamda literatürdeki diğer varlık-merkezli yaklaşımların aksine uygulama türlerini ve düğüm (araç) rollerini temel alarak hesaplanan ve *doğrudan güven* ile *önerilen güven* (diğer düğümlerin değerlendirmesi) değerlerini dengelemek amacıyla dinamik bir katsayı kullanan bir model ortaya konulmuştur. Söz konusu modelin belirtilen saldırı yöntemlerinde (kara delik saldırısı ve seçimli-iletim saldırısı) GPSR yönlendirme protokolünün dayanıklılığı ve güvenliğini arttırdığı benzetimler sonucu gösterilmiştir. Bir dezavantaj olaraksa, öne sürülen uygulama türü ve düğüm rolüne ait ağırlık değerlerinin öznel olması (makalede değerlerin tecrübeye göre belirlendiği açıkça ifade edilmektedir) gösterilebilir.

Makalenin diğer bir katkısı olarak öne sürülen hafif veri-merkezli güven modeli ise odak noktası olarak gerçek-zamanlı, anlık olarak hesaplanabilmeyi hedef almaktadır ancak söz konusu güven modeli literatürdeki başka herhangi bir model ile ne bahsedildiği gibi hesaplama hızı açısından kıyaslanmış ne de detaylı bir

benzetim sonucu düğümlerin sahte veriyi doğru veriden ayırabildiği gösterilmiştir. Bununla birlikte varlık-merkezli güven modelinde olduğu gibi bu modelde de (araç-uygulama türü güven matrisinde gösterildiği gibi) kullanılan katsayıların öznelliği söz konusudur. Tüm bu nedenlerden dolayı veri-merkezli güven modelinin katkısının ne denli büyük ve gerçekçi olduğu bir soru işaretidir.

5 Gelecek Çalışmalar

Verinin iletilmesini veya işlenmesini geciktirmeyecek şekilde gerçek zamanda hızlı ve etkili bir şekilde karar verilebilmesi amaçlanarak ortaya konulan veri-odaklı güven modeli, kıyaslandığı ilişkili çalışmalara nazaran daha çok ön tanımlı değerlerle hesaplanan basit bir fonksiyona dayandığı görülebilmektedir. Veriye dair güven değerini oluşturan çarpanlar (olayı raporlayanın güven değeri, olay ile raporlayanın ilişkili güven değeri, konuma yakınlık değeri, zamana yakınlık değeri) verinin/olayın güvenilirliğini ölçmekte yeterli gözükse de bir çoğunun tanımlanmasında kullanılan sabit değerlerin neye göre seçildiği açıklanmamıştır. Bunun yerine söz konusu sabit değerlerin seçiminde sadece trafiğe dair tecrübeden faydalanıldığına değinilmiştir. Bu kapsamda sabitlerin seçimi için geçerli ve güvenilir kaynakların referans gösterilmesi yoluna gidilebilir.

Bununla birlikte veri-merkezli güven modelinin analizi esnasında sadece önerilen çözümün çıktılarına yer verilmiş, başka herhangi bir algoritma ile karşılaştırma yapılmamıştır. Bu karşılaştırma özellikle benzer araç türü ve ya veri türü için güven değerlerinin nasıl elde edildiğini karşılaştırma açısından önemli olmakla birlikte aynı zamanda güven değerinin elde edilmesi için önerilen fonksiyonun söylenildiği gibi gerçekten de hızlı ve etkin bir şekilde sonuç üretip üretemeyeceğini de gözler önüne serecektir.

Makalede de gelecek çalışma olarak veri güven modelindeki parametrelerin ve varsayılan sabit değerlerin daha iyi optimize edilebileceğine yer verilmiştir.

6 Yorum

Kara delik ve seçimli-iletim saldırısını yakalayabilen bir varlık-merkezli güven modelinin başarılı şekilde oluşturulduğu rahatlıkla söylenebilir. Buna göre, bir aracın başka araca karşı doğrudan güven değeri (değerlendirilen aracın rolü ve veri iletim oranı ile verinin türüne göre) hesaplanmakta ve elde edilen bu değer dinamik bir katsayı ile (diğer araçların değerlendirilen araca karşı güven değerlerinden hesaplanan) öneri güven değeriyle bir araya getirilip kapsamlı güven değeri elde edilmektedir. Eğer bu sonuç değer ön-tanımlı bir eşik değerden küçük ise değerlendirilen araç zararlı düğüm olarak nitelendirilip yönlendirme sırasında kaçınılmaktadır. Makalede sonuçları gösterilen benzetimlere göre bu model yönlendirme başarımındaki kabul edilebilir bir düşüşe rağmen saldırıyı başarılı bir şekilde engelleyebilmektedir ancak benzetimde kullanılan zararlı düğümlerin oranı/sayısı belirtilmemiştir.

Makalede öne sürülen diğer bir model olan veri-merkezli güven modelinde ise kullanılan katsayıların tecrübeye dayalı olarak belirlendiği ve daha iyi optimize edilmesi gerektiği söylenebilir. Bununla birlikte bu modelin detaylı bir benzetim ortamında eşleniği başka veri-merkezli modeller ile kıyaslanması da faydalı olacaktır.

7 Sonuç

Makalede düğüm/araç güvenilirliğini belirtilen saldırı yöntemleri (kara delik saldırısı ve seçimli-iletim saldırısı) altında başarılı bir şekilde değerlendirebilen bir varlık-merkezli güven modeli önerilmiştir. Benzer güven modellerine kıyasla doğrudan güven ile önerilen güven değerleri arasında dinamik bir katsayı ile denge sağlaması açısından önemli olarak nitelendirilebilir. Sunulan benzetim sonuçlarında GPSR yönlendirme protokolü üzerinde söz konusu güven modelinin başarılı bir şekilde belirtilen saldırı yöntemlerine karşı koyabildiği gösterilmiştir. Buna ilaveten anlık, gerçek zamanlı hesaplanabilme hedefi düşünülerek tanımlanmış basit bir de veri-merkezli güven modeli önerilmiştir.