
GAZİ ÜNİVERSİTESİ
Gazi
1926

AKILLI ARAÇLAR İÇİN BULANIK MANTIK TEMELLİ SİBER GÜVENLİK RİSK MODELİ

Orhan MURATOĞLU

DOKTORA TEZİ
KAZALARIN ÇEVRESEL VE TEKNİK ARAŞTIRMASI ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

OCAK 2020

Orhan MURATOĞLU tarafından hazırlanan "AKILLI ARAÇLAR İÇİN BULANIK MANTIK TEMELLİ SİBER GÜVENLİK RİSK MODELİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi KAZALARIN ÇEVRESEL VE TEKNİK ARAŞTIRMASI Ana Bilim Dalında Doktora Tezi olarak kabul edilmiştir.

Danışman: Doç. Dr. Hasan Şakir BİLGE

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Başkan: Prof. Dr. Suat ÖZDEMİR

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Prof. Dr. Oğuzhan YILMAZ

Makine Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Doç. Dr. M.Ali AYDIN

Bilgisayar Mühendisliği Ana Bilim Dalı, İstanbul Cerrahpaşa Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Dr. Öğr. Üyesi Hilal KAYA

Bilgisayar Mühendisliği, Yıldırım Beyazıt Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Doç. Dr. Hasan Şakir BİLGE

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 20/01/2020

Jüri tarafından kabul edilen bu çalışmanın Doktora Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum

……

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Orhan MURATOĞLU
20/01/2020

AKILLI ARAÇLAR İÇİN BULANIK MANTIK TEMELLİ SİBER GÜVENLİK RİSK MODELİ

(Doktora Tezi)

Orhan MURATOĞLU

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Ocak 2020

ÖZET

Siber güvenlik zafiyetleri çok sayıda akıllı sistemde artarak görünmeye devam etmektedir. Akıllı sistemlerin bir alt şubesi sayılabilecek, akıllı araçlar ise neredeyse tekerlek üzerindeki yazılımlara dönüşmüşlerdir. Araçlarda çalışan kod satırı sayısını ve siber fiziksel sistemlerin artması, beraberinde atak yüzeyinin artmasını da getirmiştir. 1990'lı yıllardan sonra üretilen araçların neredeyse tamamı akıllı araç sınıfına girmektedir. Akıllı araçlardaki siber zafiyetlerin tespit ve değerlendirilmesi için yeterli yöntem bulunmamaktadır. Başka bir zorluk ise, siber riskler genellikle arşivlenmesidir. İstatistiksel verinin az olduğu durumlarda uzmanlardan alınan görüşlerinin değerlendirilmesi daha uygun olabilmektedir. Bu tezde akıllı araçlar için, aralıklı tip-2 bulanık mantık temelli siber güvenlik risklerin değerlendirilmesi için bir model önerilmektedir. Model CORAS adı verilen şekilsel risk ilişki tekniğinin üzerine, her bir olayın olma olasılığının uzmanlardan aralıklı olarak alınan olasılık değerlerini nihai bir değere yakınsayan bir teknik olarak geliştirilmiştir. Tekniğin temelinde bir akıllı araçta istenmeyen nihai olayın gerçekleşmesine giden alt olaylar kabaca modellenmiş, CORAS tekniği ile birbirleri arasındaki ilişkiler belirlenmiştir. Daha sonra birbirini takip eden olayların, nihai olaya varan olasılıkları hesaplanabilir hale gelmiştir. Risk haritası önce sentetik değerlerle denenmiş daha sonra uzman görüşlerine dayanarak toplanan bilgiler, yeni türetilen bu yöntemde uygulanarak test edilmiştir. Sonuç olarak; risk hesaplamasını yapabilmek için, hesaplanacak istenen istenmeyen olayın oluşma olasılığı değerlerine ulaşılmıştır.

Bilim Kodu : 90317
Anahtar Kelimeler : Bulanık Mantık, Siber Güvenlik, Akıllı Araçlar, Risk Analizi
Sayfa Adedi : 112
Danışman : Doç.Dr.Hasan Şakir BİLGE

FUZZY BASED CYBER SECURITY RISK MODEL FOR SMART CAR

(Ph. D. Thesis)

Orhan MURATOĞLU

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

January 2020

ABSTRACT

Cyber security vulnerabilities continue to increase in many intelligent systems. Smart vehicles which can be considered as a sub-branch of smart systems, have become almost software on a wheel. The number of lines of code running on vehicles and the increase in cyber-physical systems have brought an increase in attack surface. Almost all of the vehicles produced after the 1990s can be classified as smart vehicles. There are not much method to detect and evaluate cyber vulnerabilities and risks in smart vehicles. Another challenge is that cyber risks are often not archived. In cases where statistical data are scarce, it may be more appropriate to evaluate the opinions of experts. In this thesis, we propose a model for smart cars to calculate the cyber security risks based on interval type-2 fuzzy sets. The model was developed on the formal risk relationship technique called CORAS, a technique that converges the probability values of the probability of each event occurring as intervals from experts to a nearest final value. Based on the technique, the sub-events leading to the undesired event occurring in smart cars are roughly modeled. Then, the fuzzy probabilities of several events to the final event became computable. The given risk map was first tested with synthetic values and then the information gathered on the basis of expert opinions was tested using this newly derived method. Finally, it became possible to calculate the probability of the occurance of the unwanted incident specified to calculate the risk value as in input.

Science Code : 90317
Key Words : Fuzzy Logic, Cyber Security, Smart Car, Risk Analysis
Page Number : 112
Supervisor : Assoc. Prof. Dr. Hasan Şakir BİLGE

TEŞEKKÜR

Desteğini esirgemeyen eşime, tezin şekillenmesinde ve doktora yolculuğunda çeşitli şekillerde katkıları bulunan, Sn.Prof. Dr. Hacı Ali MANTAR, Sn.Dr. Ahmet Dikici, Sn. Dr. Devrim ÜNAL Sn. Dr. Orkun HASEKİOĞLU, Sn. Atilla HASEKİOĞLU ve Diğer TÜBİTAK BİLGEM çalışanı akademisyen hocamız ve mesai arkadaşlarıma, Gazi Üniversitesi akademisyenlerine, Sn. Prof. Dr. Suat Özdemir'e, Sn. Dr. Hilal Kaya'ya, bulanık mantık konusundaki tecrübelerini paylaşan Sn. Doç. Dr. Emre Boran'a ve danışmanım Sn. Doç. Dr. Hasan Şakir Bilge'ye teşekkürlerimi borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu tezde kullanılmış simge kullanılmamıştır ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	**Açıklamalar**
AT2BK	Aralıklı TİP-2 Bulanık Küme
AY	Aralıklı Yaklaşım
BKA	Belirsizliğin Kapladığı Alan
BK	Bulanık Küme
BM	Bulanık Mantık
GAY	Gelişmiş aralıklı yaklaşım
GMKA	Gelişmiş Karnik Mendel Algoritmaları
SCADA	Supervisory Control and Data Acquisition
ÜF	Üyelik Fonksiyonu

1. GİRİŞ

Günümüz dünyasında siber fiziksel sistemler, bu sistemlerin siber zafiyetleri ve ataklar sonucu ortaya çıkabilecek felaketler ciddi sayılara ulaşmıştır. Donanımların adeta köle durumunda olduğu, tüm yükün yazılımlar tarafından karşılandığı, yazılım tanımlı dünyaya doğru ilerlenmektedir. Siber risklerin kayıtları, operasyonel risklere nazaran daha az tutulmaktadır. Bu alanda siber risk analizleri yapılması gerekliliği doğmuştur. Bu riskleri belirlemede kullanılacak veri tabanları kısıtlıdır. Eksik bilgi ile işleme, öğrenen sistemlerle analiz ve alternatif yöntemlerle bu riskler gözden geçirilmeli ve yönetilmelidir. Üretim aşamasına gelmeden kritik donanım ve yazılım sistemlerinin, daha tasarım aşamasında siber riskleri değerlendirilmeli ve yönetilmelidir. Üretim aşamasından sonra, örneğin bir kalp pili düşünüldüğünde, bu risklerin azaltılması veya bertaraf edilmesi çok zor ve maliyetli olacaktır. Ciddi can kayıpları, tasarım aşamasında yapılacak siber risk analizleri sayesinde, ürünler piyasada yayılmadan önce önlenebilir.

Akıllı sistemlerin bir alt şubesi sayılabilecek, akıllı araç sistemleri; son dönemde bu alandaki gelişmelerle beraber önemli hale gelmiştir. Özellikle hibrit, elektrikli ve otonom kabiliyeti olan araçlarda, milyonlarca satır kod çalıştırıyor olması, atak yüzeyi denilen "atağa maruz kalma ihtimalini" artırmaktadır. Akıllı araçlardaki siber risklerin modellenmesi amacı ile çok sayıda açık kaynak verinin olmadığı düşünülmektedir. Araç üreticilerinin ellerinde bazı atak kayıtlarının olduğu bilinmektedir. Ancak bu veriye erişim, mahremiyet ve kurumların itibar kayıpları sebebi ile akademik çalışmalar için bile olsa zordur. Bu doktora tezinde, akıllı araçların kabaca temel siber risklerin haritalarının çıkarıldıktan sonra, uzman görüşlerine dayanan ve bu görüşler arası farkların daha hassas bir şekilde modellenmesine yardımcı olan, akıllı araçlar için aralıklı tip-2 bulanık mantık temelli siber güvenlik risk analizi modeli önerilecektir. Bulanık mantık, özellikle belirsizliklerin modellenmesinde başarısı yüksek ve birçok mühendislik alanında kullanılagelmektedir. Uzman görüşlerinden alınan bilgilerin değerlendirilmesinde ve belirsizliklerin giderilmesinde faydalı olacağı düşünülmüştür. Özellikle aynı uzman kişinin kendi görüşleri arasındaki farklılıkları ve aynı soru için farklı uzman kişilerin verdiği cevaplar arasındaki belirsizliği modellemede başarılı olacağı düşünülmektedir.

Özet olarak, risk değeri gibi bir belirsizliğin tahmin edilmesinde, bulanık mantık temelli aralıklı tip-2 bulanık kümelerin kullanılmasının uygun olacağı düşünülmüştür. Bu çalışmada siber riskler akıllı araçlar için ele alınmıştır. Ancak rahatlıkla bir SCADA sistemine, nükleer enerji üretim tesisine veya bir medikal cihazın tasarım ve üretimine uygulanabilecektir. Risk yönetimi hemen hemen her alanda bulunmaktadır. Ancak siber risk yönetimi yeni bir konudur. Bu konuda yapılan çalışmalar başlangıç düzeyde ve yetersizdir. Bu çalışma ile bu alana katkı sağlanması amaçlanmıştır.

Bu tezde Lund ve arkadaşları tarafından önerilen, şematik bir risk işleme dili olan CORAS tekniği, akıllı araçların risklerini kabaca şematik olarak tahmin edilmesinde kullanılmıştır. Bu teknik, istenmeyen bir siber olayın, o olayı etkileyen tüm alt olayları ile beraber şekilsel olarak modellenmesine ve eğer mümkünse bunlara ait olan ihtimal değerlerinin matematiksel toplamlarını modellemiştir. Çalışmada ağırlıklı olarak bilgisayar ağları ortam olarak seçilmiştir. Bu doktora tezinde ise; bir siber fiziksel sistem olan, akıllı araç ortamına uygulanabilirliğini incelenmiştir. İkinci olarak, doğası gereği bulanık halde olan veriler toplanmış, Gelişmiş Aralık Yaklaşımı modeli ile aralıklı tip-2 bulanık kümeler (AT2BK) kurulmuştur. Daha sonra aritmetik işlemler uygulanmıştır, en sonunda elde edilen değerler hala bulanık durumda olduğu için, net ihtimal değerine ulaşmak için tekrar durulaştırma işlemi, Karnik ve Mendelin geliştirdikleri yöntemlere göre yapılmıştır. Sonuç olarak CORAS şemasında elde edilen ve en sonraki istenmeyen olay için beklenen risk değeri tahminlenmeye çalışılmıştır. Bu çalışmanın, şekilsel modelle matematiksel modeli birleştiren ve CORAS tekniğini genişletmesi bakımından faydalı olacağı düşünülmektedir. Aynı zamanda onlarca bulanık küme uygulama alanlarına ilave olarak akıllı araçlardaki siber güvenlik risk modelleme alanı da eklenmiş olacaktır (Lund, Solhaug, ve Stølen, 2010).

Bu doktora tezinde giriş bölümünden sonra sırası ile metot ve materyaller bölümü içerisinde tip-1 bulanık kümeler, aralıklı tip-2 bulanık kümeler, gelişmiş aralıklı yaklaşım, çoklu karar verme ve aritmetik işlemler ve durulaştırma için gelişmiş Karnik-Mendel algoritmalarından bahsedilecektir. Üçüncü bölümde konu ile ilgili literatürde önerilen çalışmalar, dördüncü bölümde tip-2 aralıklı kümeler ile CORAS tekniğinin bütünleştirmesi ve son bölümde ise örnek bir uygulama ile uzmanlardan alınan bulanık gerçek değerlerin çözümlenmesi denemesi yapılacaktır.

Tezde araştırmamıza ışık tutacak şu sorunların cevaplarını bulmaya çalışılacaktır;

- Siber Risk Hesaplama yöntemleri nelerdir?
- Siber Risk hesaplaması akıllı araçlarda nasıl yapılabilir?
- Akıllı araçlarda oluşan siber risk istatistikleri nelerdir?
- Bir akıllı araçta oluşabilecek herhangi bir siber zafiyet ve neticesindeki istenmeyen durum, bu durumu etkileyecek alt olaylar ile beraber gösterimi yapılabilir mi?
- Akıllı araçlarda veya yakın sistemlerde siber risklerle ilgili istatistik bilgileri bulunabilir mi?
- Akıllı araçlarda istatistik temelli olmayan risk hesaplama yaklaşımı geliştirilebilir mi?
- Bulanık mantık nedir? Kullanım alanları ve yöntemçeşitleri nelerdir?
- Bulanık mantık istenmeyen olayların hesaplanmasında kullanılabilir mi?
- CORAS tekniği nedir? CORAS tekniği Bulanık mantık ile birleştirilebilir mi?
- Bir siber olayın gerçekleşme olasılığı hesaplanabilir mi?
- Bu olasılık değerleri nasıl elde edilebilir?
- Nihai istenmeyen olayın toplam olasılık değeri elde edilebilir mi?
- Uzmanlara sorarak risk etki değeri ve olasılıklar hesaplanabilir mi?
- Uzmanların cevap verdikleri sorular arasındaki belirsizlik giderilebilir mi?
- Aynı siber olay için farklı uzman görüşleri arasındaki tutarsızlıklar giderilebilir mi?
- Toplam risk değeri nasıl hesaplanabilir?
- Risk değeri hesaplamada, olasılık değerleri ile risklerin etki değerleri nasıl kullanılabilir?

Doktora tezine konu olacak bu araştırma sorularını neticesinde aşağıdaki açılardan endüstriye katkısı olacağını düşünülmektedir;

- Risk yönetimi hemen hemen her çalışma içerisinde bulunmaktadır.(üretim, mühendislik, yatırım, yönetim.. gibi),
- Otomotiv endüstrisi gelişmekte ve daha fazla yazılım temelli araçlar trafikte seyir etmektedir,
- Tasarım üretim ya da satış sonrası aşamalarında bir takım siber zafiyetler kaynaklı risklerin yönetilmesi gerekmektedir,
- Bir akıllı aracın siber risklerini bulmak, ihtimallerini bulmak ve etki değerleri ile beraber toplam risk katsayısını çıkarılması birçok araştırmacı, üretici ve finans

kurumlarının işine yarayabilecektir,

- Bunun için eski istatistik verileri kullanabiliriz, ancak siber olaylar, çeşitli sebeplerle (itibar kaybı vb), kayıt edilmediği bilinmektedir,
- Araçlar için siber olayların olduğu bilinmesine rağmen veri sıkıntısı çekilmektedir,
- İstatistikten bağımsız bir şekilde, uzmanlara her bir ana olay ve alt olayın olma olasılığı sorulabilir,
- Kesin ifade edilemeyen cevapların şiddeti, farklı skalalarda nasıl yönetilebilir?

Çalışma yapılırken deneklere sorulan sorularda iki önemli nokta dikkati çekmektedir;

a. Kişilerin kendi cevapları arasındaki belirsizlikler
b. Kişiler arası belirsizlikler

Ayrıca çalışmada bahsi geçen siber atakların hepsinin sonuç doğuracağı belli bir yüzde ile farz edilmiştir. Elbette bazı siber atakların başarısız olacağı kesindir. Ancak deneklerden istenen oran içinde bu başarısız atakların oranı da yüzdesel olarak alınmış olacaktır. Bu durumda verileri istatistiksel yöntemlerle değerlendirmek için çok sayıda denek ve soru setine ihtiyaç duyulacağı düşünülmektedir. Hem durumların bulanıklığı hemde az veri ile işlem yapma yetenekleri sebebi ile bulanık mantığın daha doğru bir yaklaşım olacağı düşünülmüştür. Deneklerden belli bir yüzde ile en küçük ve en büyük değerler isteneceği için, aralıklı tip-2 bulanık kümelerin en uygun veri modelleme yöntemi olacağı düşülmüştür.

Bulanık mantık ve AT2BK yöntemi ile kişiler arası ve aynı kişinin farklı sorular arasında verdiği cevaplar arasındaki tutarsızlık da giderilmiş ve ortalama bir değere yakınsanmış olacaktır.

Bu çalışma ile; CORAS tekniği ile Bulanık Mantık (BM) teknikleri birleştirilmiştir. Aynı zamanda bir alanda sentetik ve uygulamalı olarak test edilmiş olacaktır. Bulanık kümeler alanında bir başka değerlendirme yöntemi geliştirilmiştir. Risk değerlendirme alanına katkı yapılmış ve özgün bir yöntem önerilmiş olacaktır. Siber güvenliğin bir alt dalı sayılabilecek, siber fiziksel sistemler için bir risk analiz yöntemi geliştirilmiş olacaktır.

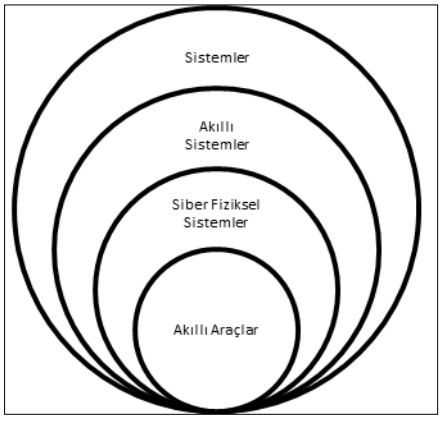
Çalışmada sırası ile birinci bölümde giriş, temel yöntemler ve literatüre katkı, ikinci bölümde literatür araştırması ve temel kavramlar, üçüncü bölümde teze temel teşkil eden aralıklı tip-2 bulanık CORAS tekniğinin önermesi, dördüncü bölümde bu tekniğin yapay olarak üretilmiş rakamlarla denenmesi, son bölümde ise sonuçların değerlendirileceği ve gelecek çalışmalara ışık tutan tartışmaların olacağı bölüm olacak şekilde bir akış izlenecektir.

2. LİTERATÜR ARAŞTIRMASI

Bu bölümde temel tanımlar, önceki akademik ve deneysel çalışmalar, alternatif risk değerlendirme yöntemleri gibi temel çalışmalar anlamına gelebilecek başlıklar işlenecektir.

2.1. Akıllı Sistemler

Günümüzde sistemler, ihtiyaçlar doğrultusunda akıllı sistemlere dönüşmektedir ve bu dönüşümün hızı her geçen gün artmaktadır. Bu trendin önümüzdeki dönemde devam etmesi beklenmektedir. Akıllı bina, Akıllı Fabrika, Akıllı Şirket, Akıllı Hastane, Akıllı Belediye, Akıllı (dijital) Devlet vs. akıllı sistemlere örnek olarak verilebilir. Nesnelerin interneti kavramı ile, önceleri internete bağlı bulunmayan elektronik cihazlar da artık internete bağlı duruma gelecektir. Bu gelişmelerin doğal sonucu olarak büyük veri kavramının daha çok gündemde olması beklenmektedir. Buna bağlı olarak yüksek hacimli verinin getirdiği risklerin değerlendirilmesi ve yönetimi ihtiyacı ortaya çıkacaktır. Bu veriler yapay zekâ ve büyük veri değerlendirme yöntemleri ile daha doğru sonuçlar çıkaracak şekilde değerlendirilebilecektir. Akıllı araçlar bir siber fiziksel sistem olarak, akıllı sistemlerin bir alt şubesi şeklinde gösterilebilir (Şekil 2.1).

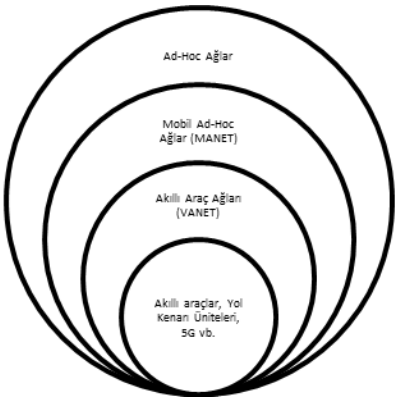


Şekil 2.1. Akıllı araçlar sistem uzayı ven şeması

2.2. Akıllı Araç ve VANET Kavramı

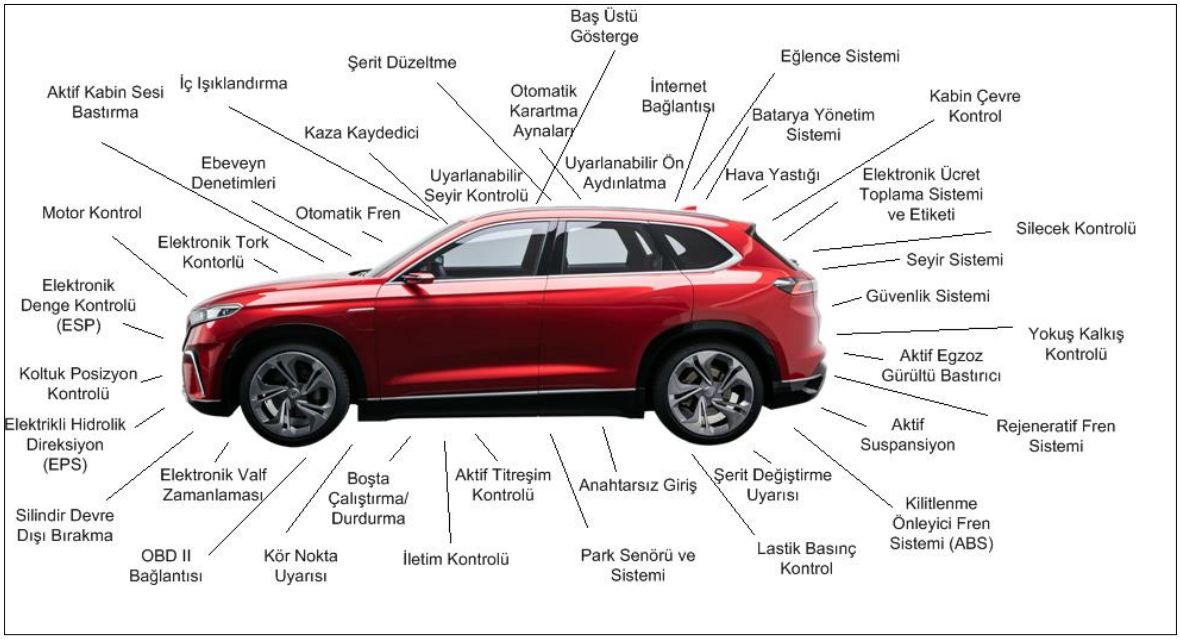
Akıllı araçlarda CAN (Controller array network) adında bir veri yolu ile 145 veya daha fazla aktuatör, 4000 çeşitten fazla sinyal veya veri, 75 ten fazla sensör bulunduğu

bilinmektedir (Technology Quarterly, 2003). Bu sensörler arasında örnek olarak radar, sonar, kamera, termometre, yağmur sensörü, lastik basınç sensörü vb. yer almaktadır. “Akıllı araç” batı ülkelerinde (ABD ve Avrupa) sürücüsüz ilerleyebilen sistemler olarak tanımlanırken, doğu ülkelerinde daha çok aracın seyrüseferinin araç içi bilgi sistemleri tarafından güvenlik ve konfor için desteklendiği teknolojiler olarak adlandırılmaktadır. Bu tezdeki yaklaşıma doğu ekolünün tarifi daha uygun olarak değerlendirilmektedir. Bu duruma her otonom araçta bir akıllı sistemdir. Dolayısıyla akıllı araç ifadesi sürücülü veya sürücüsüz tüm çağdaş araçları kapsamaktadır. Akıllı sistemlerdeki artış eğiliminden araçlar ve araç altyapıları da nasibini almıştır ve standart araçtan, tamamen sürücüsüz otonom araca doğru giden bir skalada, araçlar da akıllı hale gelmiştir/gelecektir. 2030 yılına kadar tamamen sürücüsüz bir aracın (seviye 5 otonom) trafikte seyir etemesi beklenmemektedir. Ancak bu hedefe giden yolda araçların içinde çok sayıda sistem ve bu sistemlerin birbirleri ile iletişiminden bahsedebiliriz (V2X). Mobil Ad-Hoc ağların bir alt şubesi olan araç altyapı etkileşiminin kurduğu ağlara VANET (Vehicular Ad-Hoc Networks) sistem sınıflandırması Şekil 2.2’deki ven şemasında gösterilmiştir.



Şekil 2.2. Ad-Hoc ağlar içindeki akıllı araç ve ağların sınıflandırılması

Akıllı araçlarda bulunan başlıca akıllı sistemler aşağıda verilmiştir. Bu sistemlerin daha geniş bir sınıfına Şekil 2.3’den ulaşabilmektedir. Bu özellikler esasen aracın zafiyetler bulunabilecek akıllı yüzekleri yani atak alabilecek yazılım ve donanım bulunduran parçalardır.



Şekil 2.3. Akıllı araçlar üzerindeki atak yüzeyleri

2.3. Akıllı Araçların Zafiyetleri ve Siber Ataklar

Akıllı araçlarla yapılabilecek birçok atak türü olup, bu atakların büyük çoğunluğu bilişim sistemlerine yapılan ataklara benzemektedir. Bu ataklardaki temel amaçlar; araca fiziksel erişim sağlamak, aracın ana bilgisayarına ulaşmak, aracın anahtarını kopyalamak, araca uzaktan yazılım yüklemek vb sayılabilir. En çok bilinen ataklar şunlardır;

Bilgi sistemine/ağına giriş atakları: Aracın içindeki bilgilendirme ve eğlence sistemine internet bağlantısı üzerinden yapılan ataklardır. Bu ataklar sayesinde aracın CAN veri yoluna kolayca ulaşmak mümkün olduğu için, saldırganların sıkça tercih ettiği bir yoldur. CAN veri yoluna ulaştıktan sonra araçta yapmak istedikleri eylemleri Can verisi enjeksiyonu ile devam ettirirler.

Can veri yolu atakları: CAN veri yolu araçta neredeyse her yere ulaşabilen bir ana yol gibidir. Normal şartlarda buraya okumak veya yazmak mümkün değildir. Önce saldırgan kendine bir arayüz bulur, daha sonra yetkilerini artırarak CAN veriyolu içine paket enjeksiyonu yapar. Bu sayede araç içinde ulaşamayacağı sensör verisi, ulaşamayacağı aktuatör kalmamaktadır.

Sybil atağı: Özellikle akıllı araç ağlarına, bilişim sistemlerinden miras kalan bir atak türüdür. Bu atak türünde kaçak olarak ağa dâhil olmuş habis bir düğüm, yanlış mesajlar yayarak ağın stabilitesini kendi lehine olacak şekilde bozar.

Man in the middle atağı: Yine bilişim sistemlerinden miras kalan bir atak türüdür. Burada saldırgan iki haberleşme düğümü arasına girerek, kritik bilgileri ele geçirir ve kendi amaçları için bu bilgileri kullanır.

Teşhis araçları üzerinden ataklar: Araçların servis ihtiyacı olduğunda teşhis amaçlı kullanılan ve üreticiler tarafından servislere verilen gelişmiş cihazlar, saldırganlar için iyi bir geçiş kapısı olabilir. Bu cihazlar üzerine yüklenecek bir kötücül yazılımın, servise gelen her araca ve hatta araçtan servis cihazına bulaşması mümkündür. En tehlikeli ataklardan sayılan bu atak türü, zor olmasına rağmen etki değeri en yüksektir.

OBD atağı: Araçların veriyoluna araç içinden bağlanmaya yarayan bir veriyolu ve soket türü olan OBD, on board display anlamına gelmekte ve genellikle teşhis ve sorun giderme amacı ile kullanılmaktadır. Ancak bu bağlantı kaba kuvvet atağı ile aracın bazı parametlerini ele geçirme ve aracın içindeki akıllı parçaları sömürme amacı ile kullanılabilmektedir.

Uzak bağlantı atağı: Modern araçların çoğunda, servis amaçlı yada internete bağlanmak için arayüzler bulunur. Bu arayüzler üzerinden saldırgan araca uzaktan ulaşabilir ve bir dizi atak senaryosunu deneyebilir.

Kısa mesafe bağlantı atağı: Bluetooth bağlantısı gibi bağlantı türlerini kullarak araç ağına bağlanmak, ya da bazı komutları göndermek mümkün olabilir.

Servis Durdurma Atakları (DOS): Araçta bulunun servislere çok sayıda istek göndererek, servisin doymasını ve hizmet veremez duruma düşmesine sebep olan ataklardır. Bilişim alanındaki en tehlikeli ataklardan birisi sayılan servis durdurma atakları (DOS), akıllı araçlar ve genelde akıllı sistemler için çok zararlı ataklardır.

Komut enjeksiyonu: Araç içerisindeki örneğin can veriyoluna aynı formatta ancak başka amaca hizmet eden komutların eklenmesi ve böylece yetki artırımından tüm araca zarar vermeye kadar bir dizi saldırı gerçekleştirmeye yarayan atak türüdür.

Çizelge 2.1. Akıllı araçlardaki atak türleri, etkilenen yüzeyler ve sonuçları

Atak türü	Atağın nasıl gerçekleştiği (Hangi Arayüz veya bölge üzerinden gerçekleştiği, atak vektörü)	Atak sonucu ne olduğu (Burası etkilenen araç parçaları olmalı, attack surfaces)
Hız Göstergesi için hatalı bilgi enjeksiyonu	Ana kontrol Modülü (BCM listening), Hız Paketlerini kesme,Yanlış Bilgi Gönderme	Araç hızının yanlış görünmesi
Confidentiality	TCU listening	Araç içi konuşmalar dinlenerek gizli bilgilerin tespit edilmesi
Bluetooth İle Zararlı Yazılım Enjeksiyonu	Bluetooth	Fren sistemi ile haberleşebilecek yazılımlar yükleme
Bluetooth İle Zararlı Yazılım Enjeksiyonu	Bluetooth	Hız göstergesinin manuple edilmesi
Bluetooth İle Zararlı Yazılım Enjeksiyonu	Bluetooth	Hava yastığı inaktif edilmesi
Bluetooth İle Zararlı Yazılım Enjeksiyonu	Bluetooth	Yakıt göstergesinin manuple edilmesi
Mobil Ağlar üzerinden İle Zararlı Yazılım Enjeksiyonu	Telematik Control Ünitesinin Ele geçirilmesi	Araç yazılım saldırılarına karşı savunmasız kalır
OBD-II port üzerinden İle Zararlı Yazılım Enjeksiyonu	Fiziksel Bağlantı	Yolcuların pencereleri açıp kapatmasını engellemek
OBD-II port üzerinden İle Zararlı Yazılım Enjeksiyonu	Fiziksel Bağlantı	Fren sistemine müdahale edilmesi
OBD-II port üzerinden İle Zararlı Yazılım Enjeksiyonu	Fiziksel Bağlantı	Araç hızı arttırımı ve azaltımı
OBD-II port üzerinden İle Zararlı Yazılım Enjeksiyonu	Fiziksel Bağlantı	Motor devrinin manuple edilmesi
OBD-II port üzerinden İle Zararlı Yazılım Enjeksiyonu	Fiziksel Bağlantı	Hava yastıklarının inaktif edilmesi
OBD-II port üzerinden İle Zararlı Yazılım Enjeksiyonu	Fiziksel Bağlantı	Yakıt değerlerinin manüple edilmesi
CAN Paket Eneksiyonu	Can Ağına Ulaşma	Motor devrinin arttırılması,
CAN Paket Eneksiyonu	Can Ağına Ulaşma	Motorun devre dışı bırakılması
CAN Paket Eneksiyonu	Can Ağına Ulaşma	Gaz pedalına basma oranının manuple edilmesi
CAN Paket Eneksiyonu	Can Ağına Ulaşma	Motor içindeki yakıt miktarının değiştirilmesi

Çizelge 2.1.(devam) Akıllı araçlardaki atak türleri, etkilenen yüzeyler ve sonuçları

CAN Paket Eneksiyonu	Can Ağına Ulaşma	Kullanıcıdan bağımsız hız artırılması veya azaltılması
CAN Paket Eneksiyonu	Can Ağına Ulaşma	Hava yastığı inaktif edilmesi
Tekrar saldırıları (Replay Attack)	Belirli işlevler etkinleştiğinde CAN ağını kesip aynı işlevleri yeniden etkinleştirmek için gönderme	İç ve Dış ışıkların devre dışı bırakılması
Tekrar saldırıları (Replay Attack)	Belirli işlevler etkinleştiğinde CAN ağını kesip aynı işlevleri yeniden etkinleştirmek için gönderme	Araç kapılarının kilitlerinin inaktif edilmesi
Uzaktan saldırı (Remote Attack)	Ağ keşif ve bilgi toplama	Bu saldırı türü, tipik olarak aracın davranışını değiştirmek için CAN veriyolunda mesajlar üretme girişimlerini içerir.
Kalıcı Değişiklik Atağı (Persistent vehicle alteration)	Kötü amaçlı yazılım	Aracın hızlandırılması ve yavaşlatılması
Kalıcı Değişiklik Atağı (Persistent vehicle alteration)	Yetkisiz yazılım yükleme	Aracın hızlandırılması ve yavaşlatılması
Çalınma	Ortadaki Adam Saldırısı (Man In The Middle Attack)	Anahtarsız uzaktan aracın çalıştırılabilmesi
Çalınma	Yetersiz Tasarım Planlama ve Adaptasyon sonucu	Anahtarsız uzaktan aracın çalıştırılabilmesi
Çalınma	Yönetim cihaz ve sistemlerinin yetkisiz olarak kullanımı	Anahtarsız uzaktan aracın çalıştırılabilmesi
Gözetim	Bilgi Sızması	Araç içi dinleme
Gözetim	Sızan Bilginin Kötüye kullanılması	Araç içi dinleme
Uzaktan saldırı (Remote Attack) araç fonksiyonlarından	Bu saldırı, telematik ya da bilgi-eğlence ile ilgili harici fonksiyonel arayüzlerdeki güvenlik açıklarından yararlanır.	Fren sistemine müdahale edebiilme
Uzaktan saldırı (Remote Attack) araç fonksiyonlarından	Bu saldırı, telematik ya da bilgi-eğlence ile ilgili harici fonksiyonel arayüzlerdeki güvenlik açıklarından yararlanır.	Araç içi göstergelerde manuplasyon
Yerel saldırı (Remote Attack) araç fonksiyonlarından ve teşhis arayüzlerinden	Araç içindeki donanımların firmware updatelerindeki açıklar kullanılarak yapılan saldırı türüdür.	Fren sistemine müdahale edebiilme

Çizelge 2.1.(devam) Akıllı araçlardaki atak türleri, etkilenen yüzeyler ve sonuçları

Yerel saldırı (Remote Attack) araç fonksiyonlarından ve teşhis arayüzlerinden	Araç içindeki donanımların firmware updatelerindeki açıklar kullanılarak yapılan saldırı türüdür.	Araç içi göstergelerde manuplasyon
Kalıcı Değişiklik Atağı (Persistent vehicle alteration)	Donanım Manipülasyonu	Aracın yakıt ve hız göstergesinin değiştirilebilmesi
Kalıcı Değişiklik Atağı (Persistent vehicle alteration)	Ortadaki Adam Saldırısı (Man In The Middle Attack)	Aracın yakıt ve hız göstergesinin değiştirilebilmesi
Kalıcı Değişiklik Atağı (Persistent vehicle alteration)	Mesajların Tekrar Gönderilmesi (Reply attack)	Aracın yakıt ve hız göstergesinin değiştirilebilmesi
Kalıcı Değişiklik Atağı (Persistent vehicle alteration)	Donanım Manipülasyonu	Arabanın kilit sisteminin devre dışı kalması
Kalıcı Değişiklik Atağı (Persistent vehicle alteration)	Ortadaki Adam Saldırısı (Man In The Middle Attack)	Arabanın kilit sisteminin devre dışı kalması
Kalıcı Değişiklik Atağı (Persistent vehicle alteration)	Mesajların Tekrar Gönderilmesi (Reply attack)	Arabanın kilit sisteminin devre dışı kalması

Akıllı araçlara uygulanan bazı atak türleri Çizelge 2.1'de verilmiştir. Bu çizelgede ikinci sütunda daha önce bahsedilen atak yüzeyi ya da atak vektörleri verilmiştir. Son sütunda ise bu atak gerçekleştiğinde muhtemel olabilecek sonuçlar ve araçtaki değişiklikler ifade edilmeye çalışmıştır. Daha geniş bir liste yapılabilir, ancak ataklar, atak vektörleri ve sonuçlar bu tezin konusu olmadığından bu kadarı ile yetinilmiştir.

2.4. Akıllı Araçlardaki Güvenlik Teknolojileri Üzerine Yapılan Analiz Çalışmaları

Rhim ve arkadaşları (2011), araç-altyapı ağlarında güvenlik mekanizmalarını çalışmışlar ve özellikle yol kenarı ünitesi ile araçlar arasındaki iletişim güvenliğini geliştirmeye yönelik çalışmalar yapmışlardır. Raya ve Huabaux (2007) yılında bir makalelerinde bazı kripto uygulamalarını denemişlerdir. Wolf ve Gendrullis (2012), Hossain ve Mahmud (2012) ana yazılım (firmware) güncelleme güvenliği üzerine çalışmışlar Wolf ve Gendrullis, (2012). Nilsson ve Larson (2008) yaptıkları bir çalışmada güvenlik modülü geliştirme konusuna odaklanmışlardır. Bununla beraber, siber zafiyet analizi ve riskleri ile doğrudan ilgisi olmayan, ancak zafiyetlerin görülebileceği teknolojilerden olan PKE (Pasif

Anahtarsız Giriş Sistemi) (Francillon ve arkadaşları 2011) ve TPM (Lastik Basıncını Yöneten sistem) gibi (Ishtiaq Roufa ve arkadaşları (2010) araçları "akıllı" yapan özellikler üzerine çok sayıda çalışma vardır (Francillon ve arkadaşları 2011) Ishtiaq Roufa ve arkadaşları 2010). Bu teknolojilerin her birisi zafiyetlerin oluşmasında ilave bir vektör olarak karşımıza çıkmakta ve değerlendirilmesi gerekmektedir.

Bu çalışmalar; bir başka bakış açısı ile araç içi ve araç dışı olarak iki sınıfta değerlendirebilir. Her iki sınıfta da birer alt sınıf olarak, yazılım ve donanım teknolojileri, iç ve dış ağlar, veri iletim yolları ve sensör teknolojileri üzerindeki zafiyetler ve atak vektörlerinin incelenmesi şeklinde ön plana çıkmıştır.

2.5. Akıllı Araçlar Üzerindeki Deneysel Faaliyetler

Checkoway yaptığı bir araştırmada modern otomobilin atak yüzeyini analiz etmiştir. Araştırmaya göre modern otomobiller genel olarak bilgisayarlıdır ve bu nedenle saldırıya karşı potansiyel olarak savunmasızdır. Önceden fiziksel olarak araç içi erişimi gerektiren tehdit modeli haklı olarak gerçekçi görülmüyordu. Ancak erken dönem sayılabilecek bu çalışmada yazar, siber ataklara dikkat çekmiş, içeriden ya da dışarıdan olmasını önemsememiştir. Bir başka deyişle, aracın içine nasıl erişildiğini önemsemeyerek zafiyetlere odaklanmıştır. Makale bu bakımdan çok kez eleştirilse de deneysel olarak ilk örneklerden sayılabilir. Bu makalede amaç, sistematik olarak dış saldırıları analiz ederek bu açıklıkların kapatılmaya çalışılmasıdır. Modern bir otomobilde ataklar geniş bir vektörel perspektifte olabilir (servis esnasında kullanılan araçlar, CD çalarlar, Bluetooth ve hücresel radyo dâhil). Ayrıca Checkoway, kablosuz iletişim kanalları, uzak mesafe araç kontrolü, konum takibi, kabin içi ses sızıntısına izin verme ve hırsızlık gibi faaliyetlerin gerçekleşme ihtimalini artırdığını yapılan çalışmada tartışmıştır. Ek olarak makalede, otomotiv ekosisteminin bu tür sorunlara yol açan yapısal özellikleri ve bunları hafifletmede pratik zorluklar vurgulanmıştır (Checkoway ve arkadaşları 2011).

Teknikler ortalama bir sedan üzerinde denenerek, bir otomotiv tehdit modeli çerçevesinde, nasıl atak yapılabileceği örneklerle anlatılmıştır. Gelecekteki otomotiv güvenliği için somut, pragmatik tavsiyeler sentezlemiş ve temel zorluklar gösterilmeye çalışılmıştır.

Akıllı araçların en önemli parçalarından olan ECU ve CAN parçaları üzerinde Kim ve Arkadaşları bazı deneysel faaliyetler yürütmüşler ve RSU (yol kenarı ünitesi) ile araç arasındaki iletişimi daha güvenli hale getirmek için, rastsal sayı üreteci ile kriptolu onaylama protokolü/mekanizması geliştirmişlerdir (Kim ve arkadaşları 2013).

Modern otomobillerin artık sadece mekanik cihazlar olmadığını dâhili araç şebekeleri vasıtasıyla koordine edilen düzinelerce dijital bilgisayar tarafından yaygın bir şekilde izlenip kontrol edildiğini, bir makalesinde Karl Koscher ifade etmiştir. Bu çalışmada deneysel olarak bu sorunları modern bir otomobil üzerinde değerlendirilmekte ve altta yatan sistem yapısının ne denli kırılgan olduğunu göstermektedir. Ayrıca bu çalışmada, hemen hemen her Elektronik Kontrol Birimine (ECU) sızabilen bir saldırganın, kolayca bu fonksiyonu nasıl devre dışı bırakacağını da göstermektedir. Ek olarak hem laboratuvarda hem de yol testlerinde bir dizi deney yaparak, çok çeşitli otomotiv işlevlerini düşman olarak kontrol edebilme ve sürücü girişini tamamen yok sayabilme yeteneğini sergilemiştir. Örneğin; frenleri devre dışı bırakma, motoru durdurma vb. Ayrıca, bir aracın telematik biriminde kötü amaçlı kodu yerleştiren ve kazadan sonra varlığının kanıtlarını tamamen silecek bir saldırı da dâhil olmak üzere, bireysel zayıflıklardan etkilenen bütünleşik saldırılar da yazıda sunulmaktadır. Bu güvenlik açıklarına karşı karmaşık önlemlerle beraber, mevcut otomotiv ekosistemi hakkında da ilave bilgiler vermiştir (Koscher ve arkadaşları 2010).

Cho ve arkadaşları CAN veri yolu ataklarına karşı güvenli anahtar değişim algoritması geliştirerek, sistemin savunmasına yönelik bir çalışma gerçekleştirmişlerdir (Cho ve arkadaşları 2012).

Vanet'lerdeki çeşitli atak senaryolarını ise Sharma çalışmış ve özellikle en meşhur ataklardan birisi olan Sybil atak tipini ve muhtemel sonuçlarını tartışmıştır. Sharma bu atak tipinin önlenmesine yönelik birkaç çalışma yapmıştır (Sharma, 2016). Bu çalışmanın öne çıkanlarından İranlı bilim adamları Pouyan ve Alimohammadi, sertifika servislerini ve zaman damgalarını kullanarak kişiden kişiye (peer-to-peer) ağlarda düğümlerin birden çok kimlik bilgisi yaymasını engellemeye çalışmıştır (Pouyan ve Alimohammadi, 2014).

Kong’un bir makalesinde benzer bir literatür taraması tablo halinde özetlenmiştir. Yukarıda bahsedilen bazı literatür taraması kısa özet bir tablo halinde Çizelge 2.2’de tartışılmıştır(Kong ve arkadaşları 2006).

Çizelge 2.2. Kong'un makalesinde özetlenen literatür özeti

Teknoloji	Konusu	Araştırmacı
VANET	Güvenlik Mekanizması, Kripto Uygulaması	(Rhim vd., 2011) , (Raya ve Hubaux, 2007)
ECU/CAN Ağları	Ecu ve Can içine sızma, mesaj enjekte etme ve hak yükseltme	(Kim vd., 2013),(Koscher vd., 2010),(Cho vd., 2012)
Yazılım/Donanım	Anayazılım güncelleme, yazılım yükleme, güvenlik modülü geliştirme	(Wolf ve Gendrullis, 2012),(Hossain ve Mahmud, 2007),(Nilsson ve Larson, 2008)
Diğer Çalışmalar	TMPS (Lastik basınç yönetim sistemi)	(Ishtiaq Roufa vd., 2010)
Diğer Çalışmalar	PKES (Pasif anahtarsız giriş sistemi)	(Francillon vd., 2011)
Risk çalışmaları	Araç ağına göre risk karakterizasyonu	(Studnia vd., 2013)
Risk çalışmaları	Atak senaryosuna göre risk karakterizasyonu	(Brooks, Sander, Deng, ve Taiber, 2009),(Checkoway vd., 2011)
Risk çalışmaları	Otomotiv Mühendislik Standartlarına göre risk değerlendirme çalışşması	(Wolf, Scheibel, ve Gmbh, 2012a)
Risk çalışmaları	VANET güvenliği risk değerlendirmesi	(Ren, Du, ve Zhu, 2011)

Kong’un makaledeki ilk çalışmasında hatalı olarak Lim ve arkadaşları şeklinde yazılmıştır, ancak başlığa bakıldığında bu çalışmanı Rhim ve arkadaşlarına ait olduğu anlaşılmaktadır. Küçük bir maddi hatadan kaynaklandığı düşünülen bu referansın doğrusu burada kullanılmıştır.

2.6. Siber Riskler

Üretilen verinin artması aynı zamanda sistemlerin akıllı hale gelmesi, yazılım ve donanım teknolojilerinde bu gelişme ile aynı oranla gerçekleşmektedir. Bu noktada üretilen verinin taşınırken ve depolanırken ele geçirilmesi, değiştirilmesi ya da hizmet sunumunun sekteye uğratılması gibi riskler söz konusudur.

Siber olaylar ve ataklar internet öncesi kişisel bilgisayarların tarihi kadar eskidir. Ancak son birkaç yılda gerçekleşen siber olaylar ve verdiği zararlar, tüm siber olaylar tarihinden fazladır.

Siber güvenlik uzmanları bu olaylara karşı tedbir almaya çalışırken, siber suçlular daha yeni teknikler ve zafiyetler bulmakta ve bu zafiyetleri kullanarak sistemlere zarar vermeye devam etmektedir.

Enerji altyapısı, su dağıtım şebekesi, iletişim omurgası gibi kritik sistemler söz konusu olduğunda, operasyonel risklerin yanında çok ciddi sonuçlar doğurabilecek siber riskler de artık, risk değerlendirmelerine girmiştir.

Yukarıda bahsedilen, atak yüzeyinin geometrik artışı ile, akıllı araçların siber riskleri, sonuçları itibari kişilerin can ve mal güvenliğini ciddi derecede zafiyete uğratabilecek riskler olarak değerlendirilmektedir.

2.7. Risk Analizi ve Değerlendirmeleri

Operasyonel güvenlik risk analizi ve kalite sistemlerinin bir kısmı, standartlarını güncelleyerek, siber riskleri de değerlendirme süreçlerine eklemişlerdir.

Literatür araştırması yapıldığında, operasyonel risk analiz yöntemlerini derinlemesine çalışıldığı anlaşılmıştır. Siber risklerle ilgili de farklı çalışmalar mevcuttur. Ancak akıllı araç mimarisi nispeten yeni bir mimari olduğu için, az sayıda akademik ve deneysel çalışmaya rastlanmıştır. Akıllı araçların siber risklerine dair sadece birkaç makale ve konferans bildirisinden başka bir çalışma bulunmamaktadır.

Araçların siber risklerinin tespiti; örneğin SCADA alanına göre, araçların mobilitesi ve dinamik bir alan olması bakımından daha karmaşık bir problem olarak ortaya çıkmaktadır. Çünkü modern araçlar bir kısmı yakın zamanda otonom araçlar dönüşmekle beraber, bir çoğunun içinde eğlence sistemleri, cep telefonlarına benzer yazılım ekleme çıkarma, yazılım pazarından hareket halinde iken yeni özellikler eklemeye ve eğlence için kullanılanlara benzer bir çok yazılım paketi indirilebilmesi, daima mobil internet

bağlantısının bulunması, akıllı araç ağları ve yol kenarı üniteleri ile etkileşim halinde bulunmaları, bu araçları çok daha karmaşık yapmaktadır.

2.8. Siber Risk Yönetimi

Cebula ve Young 2010 yılında yaptıkları bir taksonomi çalışmasında, siber risklerin tanımını tanımlamışlardır (Cebula ve Young, 2010). Siber risklerle ilgili çoğu çalışmaya temel teşkil eden bu çalışma sonucunda yazar dört ana risk sınıfını önermiştir; bunlar insan faktörü, sistem veya teknolojinin arıza yapması, dâhili bir işlemin hata yapması ve harici olaydır. Daha sonra araştırmacılar bu risklerin sigortalanıp sigortalanamayacağını araştırmışlardır (Biener ve arkadaşları 2015). Yine bu riskler üzerine Eling, başka bir makalesinde siber riskleri modelleyip yönetebilecek bir yöntem önermiştir. Bu makaleye göre, günümüzde siber riskler, her şirketin ana gündemine girmiştir. Ancak güvenilir verilerin ve derin analizlerin bulunmaması nedeniyle, gerekli önlemleri almak zordur. Bu durumu iyileştirmek için, operasyonel bir risk veri tabanından siber kayıpları tespit etmiş bunları aktüerya bilimi tekniklerini kullanmış ve analiz etmiştir. Özellikle, ülkeye, endüstriye, büyüklüğe ve diğer değişkenlere bağlı olarak tutarlı risk tahminleri üretmek için operasyonel risk modellerini uygulayabileceği iddia edilmiştir. Ayrıca, siber risklerin yapısal olarak diğer operasyonel risklerle özdeş olup olmadığı veya farklı özellikler sergileyip olup olmadığını test edilebilir. Makalede tüm bunların uygulamaları ile elde edilmiş sonuçlar, insan davranışının siber riskin ana kaynağı olduğunu ve siber risklerin diğer operasyonel riske kıyasla çok farklı olacağını göstermektedir. Raporun sonuçları, uygulayıcılar, politika yapıcılar ve düzenleyiciler için bu yeni ve önemli risk türünün daha iyi anlaşılabilmesi için yararlı olabileceği değerlendirilmiştir (Eling ve Wirfs, 2015).

Macher bir makalesinde siber riskleri de değerlendiren bir HARA-tehlike analizi ve risk değerlendirmesi- yapmış ve bunu kendi bulduğu isimle tehditlerin farkında olan anlamında Secure Aware Hazard Analysis and Risk Management SAHARA adında bir yöntem önermiştir (Macher, Sporer, Berlach, Armengaud, ve Kreiner, 2015).

Klimov ve Kotyashev'in bir çalışmasında risk yönetim yöntemi çalışılmış, dinamik kontrol ve bilgi kaynağı ihlallerinin risk en aza indirgenmesine dayanan siber saldırılar koşulları altında otomatik sistemlerin risklerini yönetmek için bir yöntem geliştirmek hedeflemiştir. Yöntem, hedeflenen işlevsellik için analitik ifadeler ve otomatik sistemlerin risk yönetimi

üzerinde makul kararlar vermeyi sağlayan risk faktörlerinin toleranslarını sunmaktadır. Makalede aşağıda belirtilen formül temel alarak bu risk hesaplamasını geliştirmişlerdir (Klimov ve Kotyashev, 2013).

Otomatik sistemlerin risk yönetimi yönteminin özü,

$$R = P \times Y \rightarrow min$$

formundaki riskleri en aza indirmektir. Burada P, bir saldırganın algılama süresi içinde bir siber saldırı gerçekleştirmesi ihtimalidir; Y, bir siber saldırının etkisiyle oluşacak hasarın matematiksel beklentisidir. Elde edilen bir risk düzeyi; risk yönetimi kapsamında, risk faktörlerini, olası iki kritere göre işlevselliğini gerçekleştirmesine imkân veren risklerden oluşur. Sonuç olarak bir riski istenen değerlere düşürmek veya mevcut bilgi kaynakları sınırları altındaki bir riski en aza indirmenin mümkün olabildiğini ve makul kararlar alarak riskin yönetilebileceğini göstermişlerdir (Klimov ve Kotyashev, 2013).

Kong bir makalesinde risk değerlendirme için ana çerçeve geliştirmeye çalışmış ve

$$R = A \times T \times V$$

Formülünü önermiştir. Formül ISO/IEC 1998 ve ISO 13335 standartlarının risk yönetimi bölümlerinden uyarlanmıştır (H.-K. Kong, Kim, ve Hong, 2016).

RSU (Yol Kenarı Üniteleri) bilgilerine bağımlılığı azaltarak, ele geçirilme, dolayısıyla atak risklerini azaltmaya yönelik Rhim ve arkadaşlar bir başka makale yayınlamışlardır (Rhim ve arkadaşları 2011).

Bir başka çalışmada Studnia ve arkadaşları, araç ağlarına göre risk sınıflandırması yapmışlar, benzer bir çalışmayı Ren ve arkadaşları, 2011 yılında risk değerlendirmesi olarak çalışmıştır (Ren ve arkadaşları 2011; Studnia ve arkadaşları 2013). Bu çalışmada Ren ve arkadaşları atak ağaçlarını kullanarak risk analizi geliştirmişler. Atak Ağacı adı verilen yöntem ise ilk defa Weiss tarafından 1991 yılında önerilmiştir (Ren ve akadaşları 2011; Weiss, 1991).

Güvenlik değerlendirme yöntemleri üzerine Wolf ve Scheibel'in Otomotiv mühendisliği standartlarını kullanarak değerlendirme yöntemi çalışması gibi çok sayıda bilimsel araştırma mevcuttur. Risk analizi ve değerlendirme çalışmaları bölümümüzle doğrudan alakalı olmakla beraber hedeflediğimiz tez konumuz ile dolaylı bağlantısı vardır (Wolf, Scheibel, ve Gmbh, 2012b).

2.9. Siber Risk Yönetimi Yöntemleri

Risk yönetimi bu tezin konusu değildir. Ancak risk analizi konusuna kısaca değinilecektir. Bölüm 3'te bazı siber risk analiz yöntemleri üzerinde kısaca durulduktan sonra, bu tezin konusu da olan CORAS yöntemi üzerinde tez geliştirilecektir.

3. METOT VE MATERYALLER

3.1. Taksonomi ve Tanımlar (Temel Tanımlar ve Terimler)

Tez içerisinde geçen ve sıkça kullanılan kelime ve kavramları bu bölümde tanımlanacaktır. Bu tanımlamaların çoğunda Lund ve arkadaşlarının yaptığı çalışma esas alınmıştır (Lund ve arkadaşları 2010). Başka kaynaklardan da yararlanmak ve listeyi genişletmek mümkündür.

Varlık: Lund ve arkadaşlarının hazırladığı makalede kişilerin ve kuruluşların üzerine değer atfettiği ve korumak durumunda hissettikleri her türlü varlığa verilen isimdir. Siber uzayda ise bu tanım üzerinde yazılım ve/veya donanım içeren her türlü değerli varlık olarak tanılandırılabilir. Bu tezin konusu *Siber Fiziksel* varlıklardır. Tehdidin doğrudan etkilediği birincil varlıklar *doğrudan varlık*, ikincil olarak etkilediği varlıklar *dolaylı varlık* olarak adlandırılmaktadır.

Tehdit ve Tehdit Senaryosu: Tehdit bir istenmeyen olayın potansiyel sebebi olarak tanımlanırken, bu tehdit sebebi ile oluşan ve istenmeyen bir olaya sebep olan, zincirleme olay ve olaylar silsilesine Tehdit Senaryosu denilir.

Zafiyet: Bir tehdidin, tehdit senaryosuna girmesini sağlayan zayıflık, boşluk ya da kısa yoldur.

İstenmeyen Olay: Bir siber varlık üzerinde olduğunda zarar getirebileceği düşünen olay ya da olaylar zinciridir.

Olasılık: Bir istenmeyen olayın oluşma ihtimali ya da frekansıdır.

Risk: Bir istenmeyen olayın olasılığı ve bir varlık için getirdiği sonuçlardır.

Risk Değerlendirmesi: Riskleri tanımlama, tahmin etme, hesaplama ve değerlendirme sürecidir.

Risk Analizi: Riskin içeriğini tanımlama, tahmin etme, değerlendirme ve riski hafifletmek için gereken süreçlerin tamamına denir.

Etki Değeri: Bir riskin oluştuğunda oluşturacağı maddi veya gayri maddi zararın katsayısıdır.

Zarar/Kayıp: Risk hafifletilmediği ya da ortadan kaldırılmadığı durumda oluşan maddi veya gayrı maddi kayıpların tamamıdır.

Bulanık Mantık: Aristo mantığını genişleten ve ifadeleri iki değil de çoklu olarak ifade etmeye yarayan felsefi ve matematiksel bilimdir.

Üyelik Fonksiyonu: Bir bulanık mantık kümesinde, küme üyesinin aldığı değerlerin hepsine denir.

Bulanıklaştırma: Nümerik olarak alınan alt ve üst değerleri olan veri setinin bulanık veri kümesine dönüştürme işlemidir.

Durulaştırma: Bulanık olarak işlemleri yapılmış küme üyelik fonksiyonlarının belli yöntemlerle tek bir nümerik rakama indirilmesidir.

3.2. Araştırma Yöntemi ve Stratejisi

Ida Solheim yaptığı bir çalışmada bir araştırma tezinin nasıl yapılması gerektiği ve içermesi gereken önemli özellikleri sıralamıştır (Solheim ve Stølen, 2007). Doktora tezinin önemli bir bölümü de araştırma yöntemi ve stratejisidir. Bu çalışmadaki kullanılan yöntem ve prensipler kısaca aşağıda özetlenmiştir.

3.2.1. Paydaşlar

Araştırmaya paydaş olan tüm tarafları ifade eder. Burada araştırma takımı ve üyeleri, danışmanlar, denekler, anket hazırlayıcılar ve doktora konusu özelinde riskleri tanımlayan ve sahiplenenlerle beraber yazarın kendisi kast edilmektedir.

3.2.2. Genelleştirme ve genellik

Çalışma önceki etkilendiği çalışmalar ve yöntemlerin tamamının özelliklerini içermeli ve çıktıları sonucu oluşan yeni yöntem ise yine bu özellikte olmalıdır.

3.2.3. Sağlamlık ve doğruluk

Bir araştırma sonuçları ve önerdiği yöntem bakımından en doğru sonuçları vermeli. Bu yöntem önerdiği matematiksel formüller dolayısıyla her durumda uygulanabilir ve benzer sonuçları elde etmelidir.

3.2.4. Anlaşılabilir ve uygulanabilir olmak

Teori ve hipotezler olabildiğince basit ve anlaşılabilir olmalı, benzer durumların hepsi için uygulanabilir olmalıdır. Yöntem risk analizcileri ve diğer paydaşlar tarafından kolay anlaşılabilir ve pratik olarak uygulanabilir olmalıdır.

3.2.5. Yöntemin efektif olması

Efektif olmasından kastedilen, yöntemin bir risk analiz problemini çözebilmesi, uygulanabilir olması ve önerdiği alanda sonuç elde edebilmesidir.

3.2.6. Araç kullanımını desteklemesi

Yöntem; araç kullanımına uygun olması ve desteklemesi, çıktıları araçlar için girdi olabilmesi, araştırma esnasında araçların kullanımına uygun olması gerekmektedir. Çalışmamızda başta Matlab olmak üzere, CORAS aracı, Haritalama Aracı (mind map tool), Microsoft Visio ve diğer kelime işlemciler kullanılmıştır.

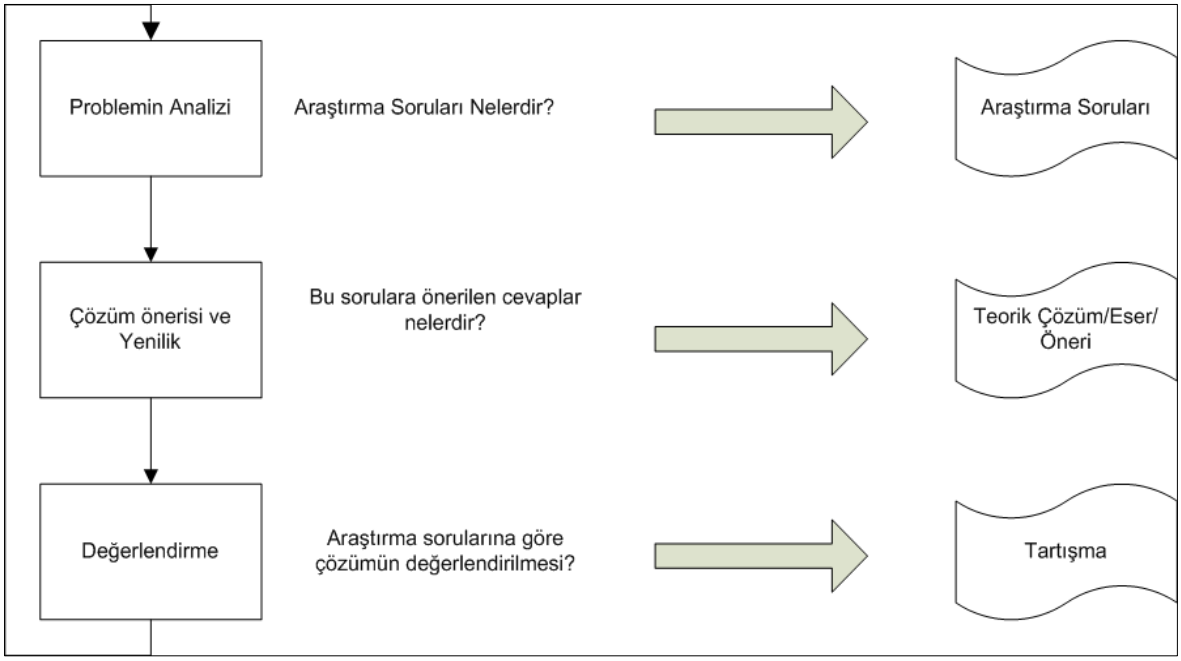
3.3. Araştırma Süreci ve Stratejisi

3.3.1. Teknolojik eksikliğin belirlenmesi

Alanda yapılmış çalışmaların literatür araştırması ile belirlenmesi ve eksikliğin belirlenmesi gerekmektedir. Teze girilmeden önce Ek-6'da bulunan haritalar oluşturulmuş ve siber risk analizi alanında çalışmanın çok fazla olmadığı anlaşılmıştır. CORAS yöntemine ulaşılmış, yöntemin içinde sentetik rakamlar kullanıldığını ve doğrudan veri kullanımı görülmüştür. Daha sonra bu alan Bulanık Mantık ile genişletilmeye çalışılmıştır. Zaman içerisinde Tran tarafından bir yüksek lisans tezinde Tip -1 bulanık kümelerin kullanıldığı ancak çalışmanın, Lund ve Stolenin çalışmasının genişletilmiş bir sürümü olduğu anlaşılmıştır (Tran, 2017). Çalışma incelendiğinde Lund ve Stolenin çalışmasındaki kelime aralıklarının biraz daha detaylandırıldığı ve iki model arasında yorum yapmadan bir karşılaştırma yapıldığı anlaşılmıştır. Hem Stolen ve hem de Tran'ın çalışmasının, önerdiğimiz yöntemin yenilikçi ve mevcut yapılan çalışmalardan tamamen farklı olduğu anlaşılmıştır (21.05.2009, Sintef, Oslo, Noveç).

3.3.2. Araştırma stratejisi

Solheim'e göre, çoğu klasik araştırma yöntemlerinde süreç, Şekil 3.1'de gösterildiği gibi, problemin analizi ile başlayan ve sürekli değerlendirme ile devam eden ve tekrarlayan bir süreçtir. Analiz safhasında problem tanımlanır ve bu problem için ya yeni bir teori ihtiyacı olup olmadığı, ya da mevcut teori ile gerçek dünya arasındaki sorun tartışılmaktadır (Solheim ve Stølen, 2007).



Şekil 3.1. Klasik araştırma süreci (Solheim ve Stølen, 2007'den adapte edilmiştir)

McGrath'a göre araştırma delilleri toplanırken şu üç faktörün göz önünde bulundurulması gerekmektedir. Bunlar; yaygınlık, hassasiyet ve gerçekçilik olarak sayılabilir (McGrath, 1984);

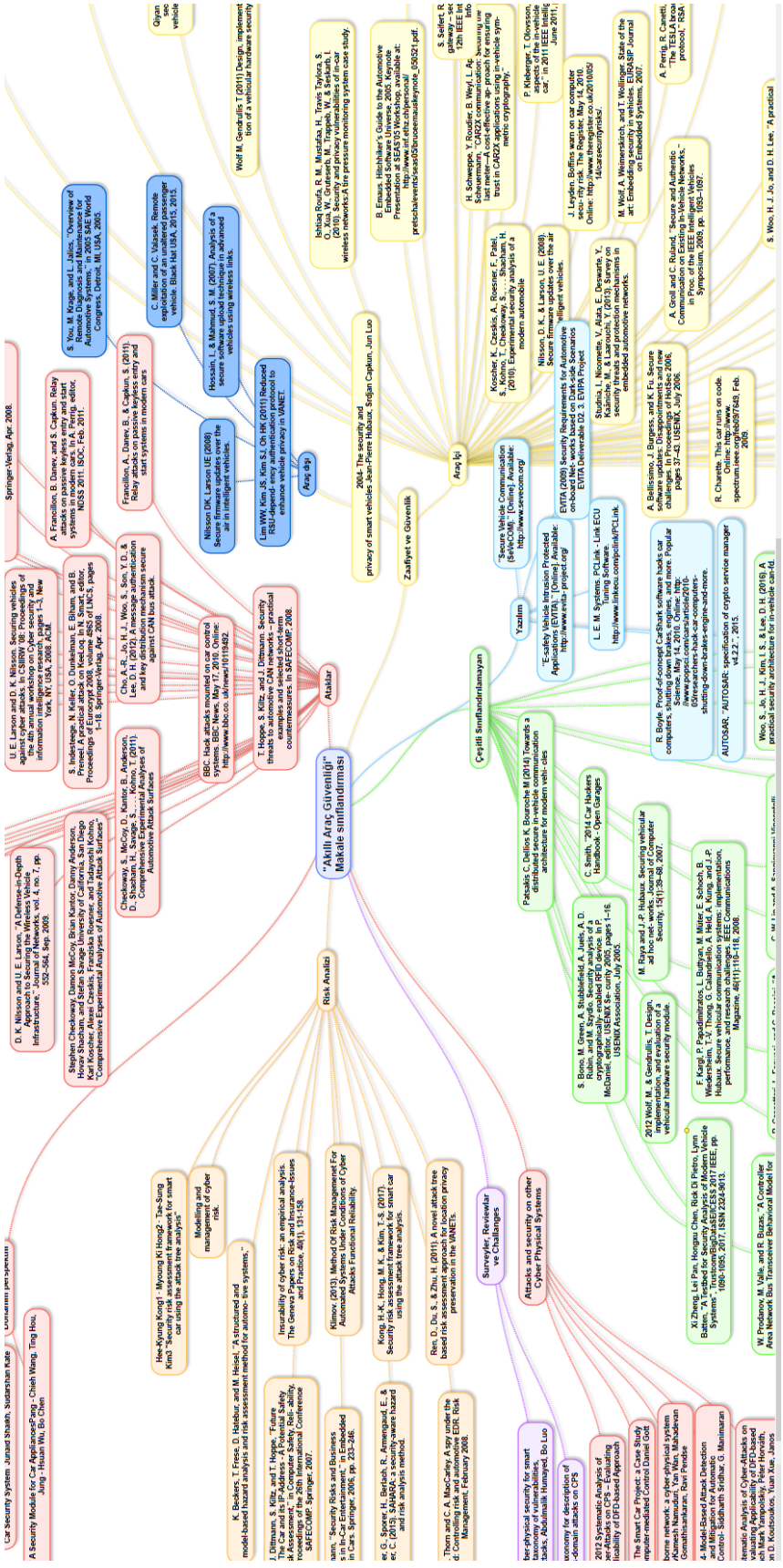
- Yaygınlık- Sonuçlar yaygın bir kitle için geçerli olmalı
- Hassasiyet- Ölçümler hassas yapılmalı
- Gerçekçilik- Sonuç bizim istediğimiz gerçek durumla, ya da içerikle doğrudan alakalı olmalı

3.3.3. Teori

Zima teoriyi tanımlarken, mantıksal gerekçelendirme ve matematiksel ifadelerle problem çözümünü öneren yöntem olarak tanımlanmıştır. Zima'ya göre teori, ilgili önermelerin sistemidir ve üç ana özelliği sağlanmalıdır; (a) tutarlı ve çelişkilerden uzak, (b) gerçek dünya hakkında bilgi verici cümle ve formüllerle ifade edilmiş ve gerçeklerle test edilmiş (c) hipotezde kullanılan varsayım ve kavramların birer tercümesi sayılabilecek, bazı yazışma kuralları içermelidir. Bu tezde bu tanımlara uygun bir model oluşturmaya çalışılacaktır (Zima, 2007).

3.3.4. Literatür araştırması

Literatür araştırması konunun evvelinde çalışmış diğer çalışmaları anlamak ve teorinin şekillenmesi için gereken boşlukları bulmak için gereklidir. Literatür araştırması daha konu belirlenmeden yapılmış olup, tez yazılırken buradan istifade edilmiştir. Konu belirlendikten sonra zaman zaman geriye dönülerek literatür araştırması tekrar yapılmıştır. Buna göre çalışma başlığı ve hedefleri tekrar güncellenerek, tekrarlayan bir süreç izlenmiştir. Ek-6'de gösterilen zihin haritaları ile hangi konunun kimin tarafından çalıştığı tespit edilerek, haritada ilgili yerlere konmuştur. Böylece siber risk analizi konusunda çok derinlemesine çalışmaların olmadığı sonucuna varılmıştır. CORAS şematik ve matematiksel bir risk analiz yöntemidir. Genellikle bilişim sistemleri ekseninde örneklendirilmiştir. Ancak çalışmalarda kullandıkları verilerin yapay olması sebebi ile, tamamlayıcı bir değerlendirme yöntemine daha ihtiyaç duyulmuştur.Bu noktada yaygın bir uygulama alanı olan ve çok sayıda sistemde kendini ispatlamış bulanık mantık teorisine başvurulmuştur. Belirsizlikleri modellemede özellikle aralıklı tip-2 bulanık mantık yöntemlerinin ve kütüphanelerinin olgunlaştığı anlaşılmıştır. Aralıklı Tip-2 Bulanık kümeler ise benzer şekilde kontrol mühendisliği ve diğer alanlarda kullanılmıştır. Sonuç olarak literatür araştırması, her ikisinin de temel teorilerini ve matematiksel modellerini içerecek şekilde yapılmıştır. IOS tabanlı Macintosh bilgisayara kurulabilen, SimpleMind Lite yazılımı ile literatürdeki çalışmalar sınıflandırılmaya çalışılmış ve araştırmaya muhtaç alan tespit edilmiştir.



Şekil 3.2. SimpleMind Lite yazılımı ile akıllı araç güvenliği komşuluğunda yazılmış makale ve bildirilerin ekran görüntüsü (EK-6'da yüksek çözünürlüklü sürümü bu teze ek olarak verilecektir.)

3.3.5. Mantıksal akıl yürütme

Bilindiği gibi iki tür akıl yürütme mantığı vardır; (a) tümden gelim, (b) tüme varım. Tümden gelim yukarıdan aşağıya doğru olur. Yani kurulan hipotezler ve teoriler, sonuçlar doğru çıktığı takdirde, doğru kabul edilmektedir. Tüme varım ise, önce deney ve gözlemlerin yapılması sonucunda hipotezlerin ve sonuç olarak teorinin kurgulanması anlamına gelir (Trifts, 2019). Bu çalışmada tümdengelim yöntemi ile kurulan aralıklı tip-2 bulanık CORAS ihtimal (risk) hesaplama yönteminin, önce sentetik, daha sonra bir uygulama ile doğrulanması esas alınmıştır.

3.3.6. Anket çalışması ve deney

Anket çalışması 34 adet deneğe, bir web uygulaması üzerinden soru seti hazırlanarak sorulmuştur. Evvela sistem deneme cevaplarla test edilmiş, dokümantasyona uygun olduğu anlaşıldığında çevrim içine açılmıştır. Çalışmada kullanılan sorular EK-1'de, cevaplar ve kişilerin anonimleştirilmiş isimleri EK-2'de verilmiştir.

3.4. Siber Risk Analizi Yöntemleri

Siber riskleri tespit edebilmek için belli başlı risk analiz yöntemleri geliştirilmiştir. Çoğunluğu bir model öneren bu risk analiz yöntemleri genellikle tehdit ile istenmeyen olayların arasındaki kritik noktalar ve sonuçları incelerler. Kısaca bu modeller; Bilgi Güvenliği Yönetim Sitemi, STS aracı yöntemi, Atak Ağacı Yönetimi, Atak Savunma Ağacı yöntemi, DREAD Risk Hesaplama yöntemi ve bu teze konu olan CORAS Siber Risk modelleme yöntemidir. CORAS yöntemi kapsamlıca diğerleri ise kısaca tanımlanarak geçilecektir.

3.4.1. BGYS (ISO 27001) bilgi güvenliği yönetim sistemi

Uluslararası Standart Organizasyonu tarafından oluşturulmuş ve kurumlar içerisindeki kıymetli bilginin gizliliğini ve yaşam döngüsünü yönetmeye çalışan bir kalite yönetim sistemidir. Bu standardın "planlama" safhasındaki risk analizi bölümü, bir siber fiziksel sitemin siber risk analizi söz konusu olduğunda uygulanabilir. Bu tezin temel

tekniklerinden olan CORAS tekniği, ISO27001'de kabul edilmiş, Planla, Uygula, Kontrol Et, Önlem Al aşamalarının planlama safhasına tekabül etmektedir.

3.4.2. STS aracı

Sosyo-teknik sistemler için aktör ve hedef odaklı bir güvenlik gereksinimi modelleme dili olan STS-Modelleme Dili, modelleme ve analiz destek aracıdır. İnsan ve organizasyon arasındaki riskler modellemeyi amaçlar. STS-Aracı (a) sosyo-teknik sistemleri etkileşimleri konusunda güvenlik ihtiyacı olan etkileşimli aktörler kümesi olarak modellemesi ve (b) sistem için güvenlik gereklilikleri türetmesi konusundaki gereksinim analistlerini ve güvenlik tasarımcılarını nasıl desteklediğini gösterir. Bu araç, belirli bir STS- modelleme dilinin iyi oluşturulmuş olup olmadığını kontrol etmeye, güvenlik gereklilikleri arasında herhangi bir uyuşmazlık olup olmadığını kontrol etmeye ve aktörlerin varlığını tehdit eden olayların tehdit izini hesaplamayı kolaylaştıran bir dizi otomatik akıl yürütme tekniğini bütünleştirir. Önce STS-ML tarafından desteklenen modelleme ve akıl yürütme faaliyetlerini, ardından e-Devlvd.anından güvenli bir sosyo-teknik sistemin tasarımını bir dizi egzersizle göstermektedir. Daha çok ilişkiler, roller ve varlıklar arasındaki etkileşimi göstermeyi amaçlamaktadır (Paja, Dalpiaz, ve Giorgini, 2014).

3.4.3. Atak yüzeyi

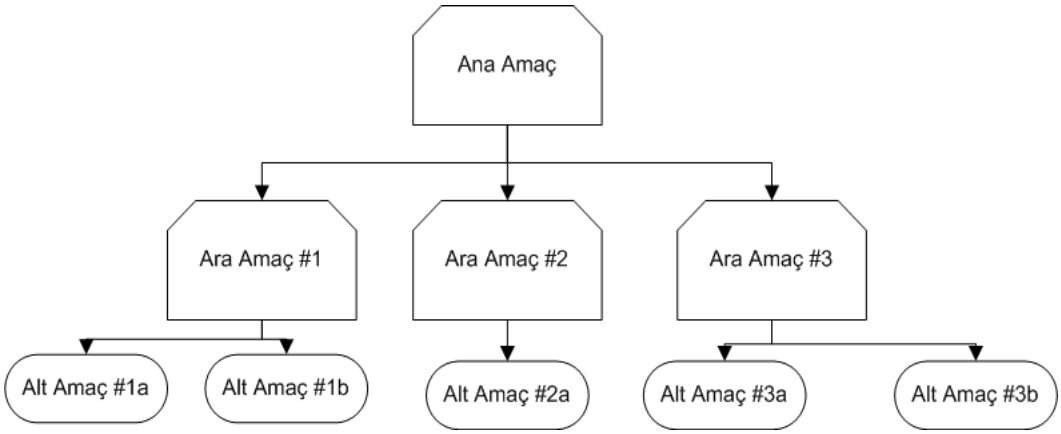
Bir bilgisayar ya da ağ ortamındaki zafiyet vektörlerinin tamamının toplamı o sistemin atak yüzeyini belirlemektedir. Bir bakıma sistemlerin siber saldırılara maruz kalma ihtimalini gösteren bir ifadedir. Yazılım kullanımının arttığı sistemlerde atak yüzeyi de artış göstermektedir.

Modern sistemlerin çoğu artık "yazılım tanımlı" sistemlere doğru kaymaktadır. Donanım elemanları birer köle kaynağa dönüşmekte ve tüm iş süreçleri yazılım üzerinden dönmektedir. Örneğin; ağlardaki anahtarlama işlemleri önceleri devre anahtarlama yolu ile daha donanım ağırlıklı çalışırken, artık aynı donanımın üzerinde farklı etki alanları oluşturmaya olanak verebilecek, paket anahtarlamaya geçilmiştir. Aynı şekilde radyo iletişiminde, sayısal telsiz sitemlerine geçilmiş, yazılım tanımlı sistemlere geçilmiş, neredeyse görevler yazılım seviyesinde yapılmaya başlanmıştır.

Akıllı araçlarda da ciddi derecede yazılım ve kod artışı yaşanması sebebi ile artık araçlar "tekerlek üzerindeki bilgisayarlar" olarak adlandırılmaya başlanmış ve zafiyetler bakımından siber risklere karşı çok daha açık bir duruma gelmiştir.

3.4.4. Atak Ağacı ve Atak-Savunma ağacı

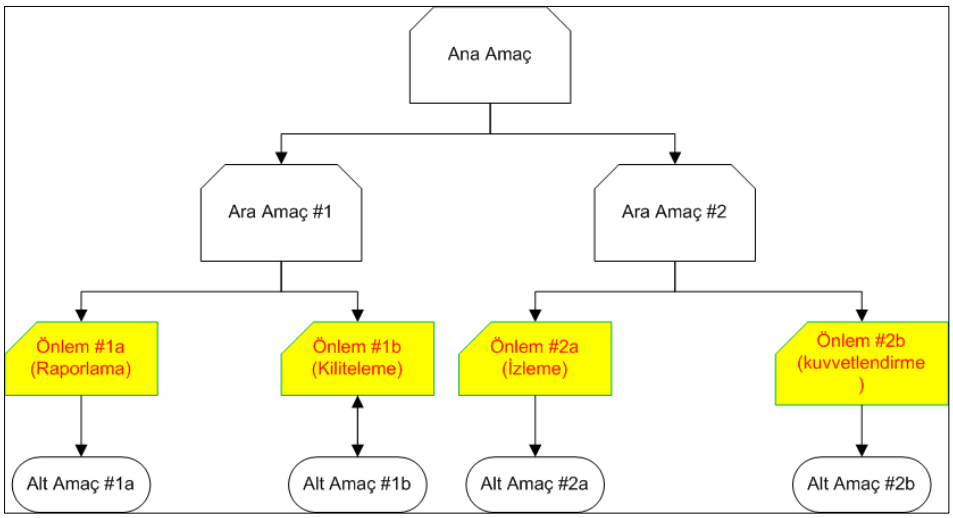
Atak ağacı analizi, 20 yıldan fazladır bilinen ve gerçeği modellemek için olayın aşamalarının kırılımını yapmaya yarayan bir tekniktir (Ingoldsby, 2013). Mühendislik çalışmalarına uygunluğu bu alanda çok kullanılmasına sebep olmuştur. Atak ağacı denilen grafiksel, matematiksel bir karar destek sistemidir. Şekil 3.3'de en basit hali ile bir atak ağacının hedef temelli olarak gösterimi görülmektedir (Ingoldsby, 2013).



Şekil 3.3. Hedef temelli basit atak ağacı yapısı (Kordy, Mauw, Radomirović, ve Schweitzer, 2014)

Atak ağaçlarına istenirse VE ya da VEYA mantıksal kapıları ile istenen şartların sağlandığı durumların analizi de yapılabilmektedir.

Atak-Savunma ağacı, atak ağacı yöntemine ilave olarak, savunma noktalarını da risk ağacında gösteren bir yöntem olarak Kordy tarafından önerilmiştir (Kordy ve arkadaşları 2014). Buradaki en temel iki özellik; ayrıntılandırma ve karşı tedbirlerin gösterimidir (Şekil 3.4).



Şekil 3.4. Atak-Savunma ağacı ve karşı tedbirlerin gösterimi (Kordy ve arkadaşları 2014)

3.4.5. DREAD risk hesaplama yöntemi

Microsoft tarafından geliştirilen bu yöntem ingilizce; Damage Potential (zarar potansiyeli), Reproducability (tekrarlanabilirlik), Exploitability (sömürülebilirlik), Affected User (etkilenen kullanıcılar) ve Discoverabilitiy (açığa çıkma kolaylığı) kelimelerinin baş harflerinden oluşmuştur. Bu yöntemrisk hesaplamasında bilişim sistemleri ve güvenlik cihazları için nümerik bir risk rakamını oluşturmayı hedeflemiştir. Teknik daha gelişmiş teknikler sebebi ile yine Microsoft tarafından 2008'den sonra kullanımı terk edilmiştir (Microsoft, 2007).

3.4.6. STIX yöntemi

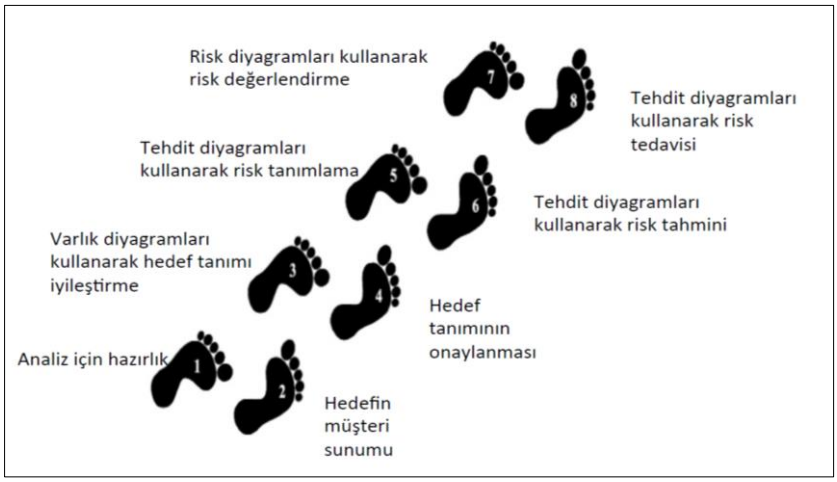
Bir açık kaynak projesi olarak Github.io içerisinde başlayan proje, çok sayıda paydaşın katılımı ile genişlemiş ve şekilsel bir tehdit analiz yöntemine dönüşmüştür. Kurum ve tüm paydaşları için standartlaştırılmış ve yapısal bir tehdit analiz yöntemini önermektedir. "Ölüm zinciri" adını verdikleri ve atakların çoklu adımlarını anlayıp yönetmeye yarayan bir yöntemdir (Standardizing Cyber Threat Intelligence, 2019).

3.4.7. CORAS yöntemi

İlk olarak Ketil Stölen ve arkadaşları tarafından ortaya atılan bu teknik, istenmeyen siber olayların olasılıklarını hesaplama üzerine hem şematik hem de matematiksel bir çalışma

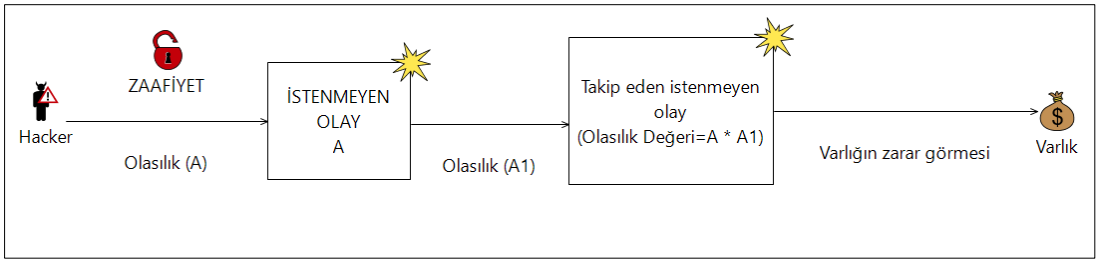
ortaya koymuştur. CORAS dili, özelde yazılımsal ve donanımsal siber risklerin modellenmesi için kurgulanmıştır. ISO 31000 Risk Yönetim Standarları ile bunun kökeni sayılan AS/NZS 4360 standartlarının bilişim sistemleri için modellenmiş halidir. Temelde bir istenmeyen olayın üzerine etki eden tüm olaylar ağının ve bunların olasılıklarının matematiksel toplamı olduğunu iddia etmektedir. Varlık, zayıflık, tehdit, etkilenen faktör, etki, olasılık, istenmeyen olay, risk ve önlem gibi siber risk yönetiminin taksonomisine katkıda bulunur ve aynı zamanda bu kavramları kullanmaktedır. Ayrıca ISO 27001 ve diğer kalite standartlarında, PUKÖ (planla-uygula-kontrol et- önlem al) döngüsünün planlama safhasına denk gelmektedir (Lund ve arkadaşları 2010).

CORAS 8 adımdan oluşan bir değerlendirme yöntemi ile varlık tabanlı tehdit analizini yapmayı hedefler. Bu adımlar Şekil 3.5'te gösterilmiştir.



Şekil 3.5. CORAS yönteminin 8 adımı (Lund ve arkadaşları 2010)

Varlık tehdit ve zafiyet tabanlı ve genel olarak savunmaya yönelik üretilmiş olan yöntemin basit bir risk haritası aşağıdaki şekilde gösterilmiştir.



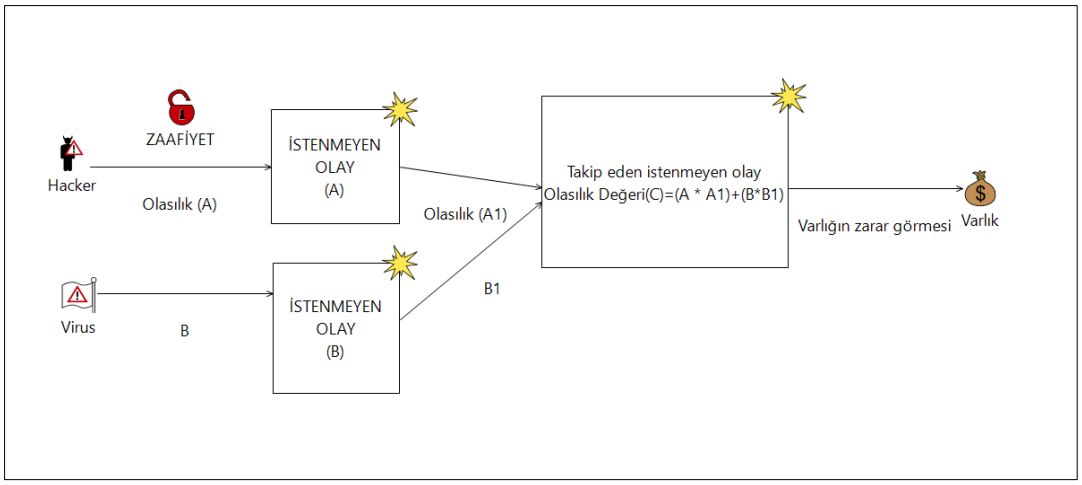
Şekil 3.6. Basit CORAS diyagramı

Şekil 3.6'daki Takip eden istenmeyen olayın olma olasılığı, İlk İstenmeyen olayın olma olasılığı ile bu olay gerçekleştiğinde diğer olayın olma olasılığı ile çarpımıdır.

$olasılık = A \times A1$

olarak ifade edilebilir.

Başka bir ifadeyle CORAS, istenmeyen bir nihai olayın üzerine etki eden tüm olayların toplamı, alt olayların olasılıklarının toplamına eşit olduğunu iddia etmiş ve şematik bir dil ile gösterme yöntemidir.



Şekil 3.7. İstenmeyen olaya etki eden iki alt olay ve olasılık hesabı

CORAS diyagramlarında birbirini takip eden olayların ihtimal hesabı üç şekilde etkileşime girebilir; (a) hariç tutan (birbirini dışlayan) (b) bağımsız (c) dâhil tutan. Birbirini takip eden olaylar eğer nihai istenmeyen olay üzerinde azaltıcı bir etki yapıyorsa "hariç tutan" diye tarif edilir. Aksi halde artırıcı etki yapıyorsa, yani destekliyorsa, "dâhil tutan" olarak adlandırılır. İstatistiksel olarak bağımsız ilişkiler için ise "bağımsız" ifadesi kullanılabiliriz. Teorinin kolay anlaşılabilmesi ve tezin karmaşıklığını azaltmak için oluşturduğumuz modellerde "bağımsız" yani birbiri üzerine etkisi olmayan olaylar zinciri olduğunu var sayılmıştır (Lund ve arkadaşaları 2010).

CORAS dilinde ayrıca, "sebep olan" ve "zarar veren" iki ana etkileşim bulunmaktadır. Tezin önerdiği yöntemi basitleştirmek adına, sebep olan etkileşimi kullanılacak ve nihai olaya giden alt olayların istatistiksel olarak bağımsız oldukları varsayılacaktır (Lund ve

arkadaşaları 2010). Ayrıca bağımlı değişkenler veya durumlarda söz konusu olabilir. Bu durumda; "içleyen" veya "dışlayan" iki tip bağımlı değişkenden bahsedilebilir. İki olay arasında, eğer birinin gerçekleşmesi diğerinin oluşma ihtimalini azaltıyorsa içleyen, diğerinin oluşma ihtimalini dışlayan bağımlı değişkenler söz konusudur. İçleyen bağımlı değişkende iki olayın çözüm kümesinin kesişimi söz konusu olduğundan, bu farkın olasılık hesaplamasında düşürülmesi gerekmektedir. Benzer şekilde dışlayan bağımlı değişkeninin bulunması durumunda bu farkın olasılık hesabına eklenmesi gerekmektedir. Bu tezin konusu model oluşturmak üzerine odaklandığı için, teorinin ispatında hesaplama kolaylığı sağladığı için, bağımsız değişkenler olduğu faz edilecektir.

Şekil 3.7 de risk haritası gösterilen basit CORAS diyagramı için;

- Bir *A* istenmeyen olayının olma olasılığı P_A olsun,
- Herhangi bir *B* olayının olma olasılığı da P_B olsun,

A ve *B* olayları olduğunda, bir sonrası istenmeyen olayın (C) olasılık hesabı, "bağımlı içleyen" olarak hesaplandığında gösterim aşağıdaki şekilde sağlanacaktır;

$$P_C = P_A \times P_{A1} + P_B \times P_{B1} - \left(P_A \times P_{A1} \times P_B \times P_{B1}\right)$$

A ve B olaylarının birbirinden bağımsız olduğu varsayılırsa;

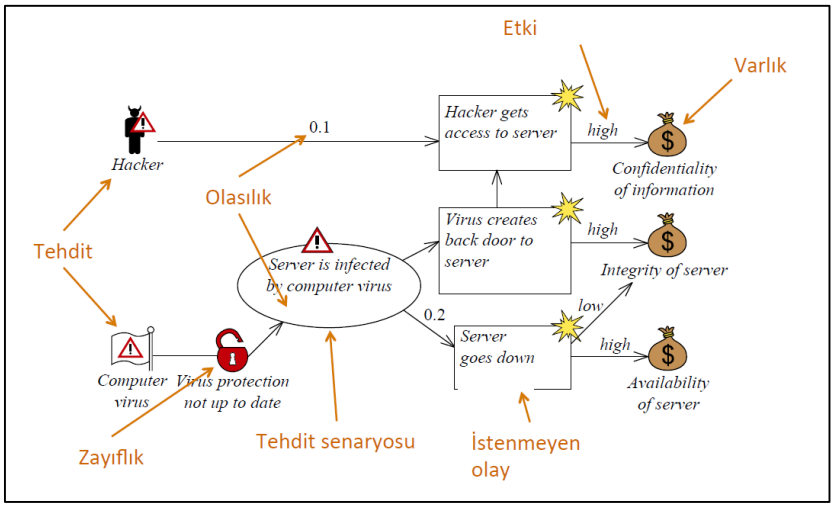
$$\left(P_A \times P_{A1} \times P_B \times P_{B1}\right) = 0$$

ifade edilebilir. Sonuç olarak ;

$$P_C = P_A.P_{A1} + P_B.P_{B1}$$

şeklinde ifade edilebilir.

Tezin temelini teşkil edecek ihtimal hesapları, yönteme odaklanmak ve kolaylık sağlamak için tümü bağımsız değişken olduğu varsayılarak çalışmalar yapılmıştır.



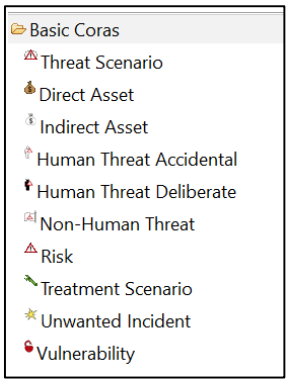
Şekil 3.8. Örnek CORAS tehdit diyagramı (Lund ve arkadaşları 2010)

Şekil 3.8 de CORAS tekniği ile oluşturulmuş bir tehdit ve istenmeyen olaylar zinciri ve bunların arasındaki ilişki gösterilmiştir. Linkler arasındaki olasılık değerleri, "bağlayan olay" olduğunda "bağlanan olayın" olma olasılığını gösteren nümerik ihtimal değerleridir. Genellikle 0 ile 1 arasında bir değerdir. Yüzdesel olarak hesaplamalar yapıldığında % 0'a yakın bir değerle % 100'e yakın bir değerde hesaplamaların yapılması uygun olmaktadır. Şematik bir anotasyon ile Tehdit Diyagramları kurar ve toplam olasılığı tahmin etmeyi amaçlar.

Coras Tasarım aracı: Şekil 3.8'de CORAS kitabından alınmış bir tehdit diyagramı vardır. Burada bahsedilen işaretlemelerin birçoğu kullanılmıştır.

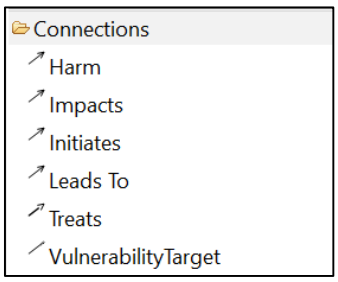
CORAS tekniğinin pekiştirilmesi amacı ile CORAS tasarım aracı geliştirilmiştir (EK-5). Bu araç ile tüm varlık, zafiyet ve istenmeyen olaylar, ihtimal değerleri ile birlikte (eğer biliniyorsa) modellenebilmektedir. Farklı alanlarda risk analizinin yapılabilmesi için, risk analizinin tüm bileşenlerini barındırır.

Basit CORAS risk haritaları için aşağıdaki hazır anotasyonlar kullanılabilir;



Şekil 3.9. CORAS aracı içinde kullanılan şekil alemanları

Varlıkları ve istenmeyen olayları aşağıdaki link tipleri ile birbirine bağlayarak basit CORAS haritaları oluşturulmaktadır (Şekil 3.10);



Şekil 3.10. CORAS aracı içinde kullanılan link elemanları

3.5. Bulanık Kümeler

Aristo Mantığına göre durum iki değişkenle ya varlık ya da var olmama durumu ile ifade edilebilir. İkili (Binary) adı da verilen bu mantıkta, durumlar ya 0 ya da 1 dir. Bazı durumlarda bu sıfır ve bir arasında çok sayıda farklı durum gruplanmaları olabilir. Örneğin "Hava Nasıl?" sorusunun cevabı, sıcak veya soğuk olabilir (Aristo Mantığı). Ancak bazı durumlarda bu anlatımı daha detaylandırmak ve ara kademeler koymak istenebilir. Ya da durumun kendisi doğal olarak ara durumlar üretmiş olabilir. Bu durumda sorunun cevabı, çok soğuk, soğuk, normal, sıcak ve çok sıcak olarak 5 kademeleri olarak ifade edilebilir. Buna benzer kişilere özgü kanaatlerin farklılaştığı durumlar "bulanık durumlar" ve ifade türüne "bulanık mantık" denir. Bu durum cevabın minimum ve maksimum değerleri

olduğu durumlarda da geçerlidir. Örneğin yapılacak bir ankette ; “orta yaş nedir?” diye sorulacak olunsa cevaplar aşağıdaki şekilde olacaktır Örnek 3.1.

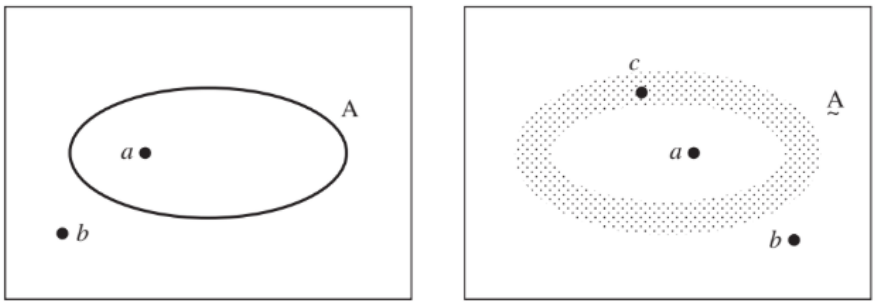
Çizelge 3.1. Örnek bulanık küme

Orta yaş nedir?	Cevap
Denek1	30-60 yaş aralığıdır.
Denek2	35-55 yaş aralığıdır.
Denek3	35-45 yaş aralığıdır.
Denek4	40-60 yaş aralığıdır.
Denek5	45-55 yaş aralığıdır.

Görüldüğü gibi, sorunun cevabı farklı aralıklarda ve farklı odaklarda öbekleşmektedir ve kesin bir cevap yoktur. Ancak istatistiksel ve bulanık mantık durulaştırma yöntemleri ile bu aralık değerleri nümerik sabit rakamlara indirgenmesi mümkün olabileceği düşünülmektedir. Bu doktora çalışmasının temel çıktısı bu olacaktır.

Bir çeşit çok değerli küme kuramı olan bulanık küme kuramında, kümedeki her bir birey, klasik çift değerli küme kuramlarında olduğu gibi üye ya da üye değil olarak değil, bir dereceye kadar üye olarak görülmektedir. Bulanık küme değişik üyelik derecesinde öğeleri olan bir topluluktur.

Zadeh, bulanık küme elemanlarının üyelik derecelerini göstermek için [0.0, 1.0] Aralığındaki gerçel sayıların kullanılmasını önermiştir (Zadeh, 1965).



Şekil 3.11. (a) Basit küme üyeliği (b) Bulanık küme üyeliği

Şekil 3.11-a’da *a*; A kümesinin bir üyesi iken, *b* üyesi değildir. Şekil 3.11-b’de ise A bulanık kümesinin a üyesi iken, *b* üyesi değildir. *c* üyesi ise belli bir dereceye kadar üyedir.

Bu üyelik derecesi bulanıklığın temel sebebidir. *c*'nin üyeliği *a* ve *b* elemanlarının durumu gibi net değildir. *c*'nin belli bir derecede üye olma durumuna Üyelik Fonksiyonu (ÜF) denir.

3.5.1. Tip-1 bulanık kümeler

Klasik küme teorisinde, elemanların evrensel kümenin alt kümesi olan *A* gibi bir kümeye ait olmaları veya ait olmamaları kesin sınırlarla belirlidir. Bir elemanın *A* kümesine ait olması 0-1 üyelik fonksiyonuyla gösterilir. Eğer bir eleman *A* kümesinin elemanıysa üyelik fonksiyonu değeri 1'e eşittir. Fakat belirsizliğin ve kesinsizliğin olduğu dünyamızda olayların iki değerli 0-1 mantıkla açıklanması tam olarak doğru bir yaklaşım değildir. Bu nedenle Zadeh klasik küme kavramının gerçek dünyada, özellikle insanları içeren kısmen karmaşık sistemlerle uğraşırken yetersiz kalmasından yola çıkarak, niteliklerin (küme elemanlarının) ikili üyelik fonksiyonuyla ifade edilen klasik kümeler yerine, dereceli üyelik fonksiyonlarıyla ifade edildiği bulanık kümeler tanımlamasını önermiştir (Zadeh, 1965). Belirsizliği daha iyi ele alabilmek için bulanık kümeler Zadeh tarafından önerilen tip-n bulanık kümeler kavramıyla genelleştirilmiştir. Bulanık kümeler tip-n bulanık kümelerin özel bir hali olup (n=1) tip-1 BK'ler olarak da adlandırılmaktadırlar (Zadeh, 1965).

Şekil 3.15'te, orta yaş için girilen her bir cevapta normal bir dağılım görülmektedir, bu gibi durumlarda "Birinci Dereceden Bulanık Küme" denir. Zadeh bu durumu dereceli üyelik fonksiyonları ile ifade ederek tek bir cevap yerine, dereceli bir cevap skalası önermiştir. Her bir cevap yine kendi içinde, kendisini oluşturan bir bulanık cevaplar manzumesi içermesi durumunda bu durum sonsuz sayıda üyelik derecesine doğru gitmekte yani n'ince dereceden bulanık kümelere dönüşmektedir. Bu durumda kümeler üyelik derecelerinin derinliğine göre Tip-N bulanık küme diye ifade edilir.

"Temel Küme Teorisine" dayanan bu durumları gösterebilmemiz için bazı tanımlamalar ve varsayımlar yapılması gerekecektir.

Tanımların matematiksel ifadeleri aşağıdaki şekilde olacaktır.

Tanım 3.1: X evrensel kümesindeki bir bulanık A kümesinin üyelik fonksiyonu $\forall x \in X$ $\mu_A(x): X \to [0,1]$ şeklinde tanımlanır. Evrensel küme kesikli ise A bulanık kümesi Eş. 3.1'deki gibi gösterilir.

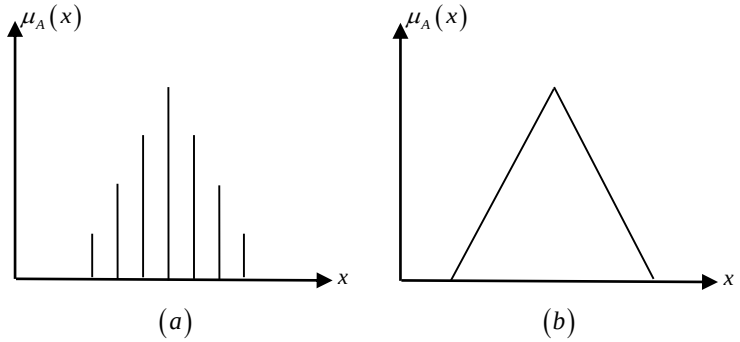
$$A = \left\{ \frac{\mu_A(x_1)}{x_1} + \frac{\mu_A(x_2)}{x_2} + \ldots + \frac{\mu_A(x_i)}{x_n} \right\} = \left\{ \sum_{i=1}^{n} \frac{\mu_A(x_i)}{x_i} \right\} \tag{3.1}$$

$\mu_A(x_i)$, x_i elemanın A kümesine aitlik derecesini ifade etmektedir. Eğer evrensel küme sürekli ve sonsuz ise A bulanık kümesi Eş. 3.2'deki gibi gösterilir.

$$A = \left\{ \int_X \frac{\mu_A(x)}{x} \right\} \tag{3.2}$$

Eş. 3.1'de gösterilen "+" işareti cebirsel toplam işareti değildir, küme elemanların birleşimini göstermektedir. Aynı şekilde Eş. 3.2'de gösterilen integral işareti de sürekli değer alan elemanların birleşimini göstermektedir.

Şekil 3.12'de bir kümeye ait elemanların üyelik fonksiyonlarının kesikli ve sürekli formda gösterimi verilmiştir.



Şekil 3.12. (a) Kesikli bulanık küme (b) Sürekli bulanık küme

Tanım 3.2: Bulanık kümelerde önemli kavramlardan iki tanesi alfa (α) kesmesi ve güçlü alfa (α^+) kesmesidir. X evrensel kümesinde bir bulanık küme A ve $\alpha \in [0,1]$ olmak üzere

α kesmesi ve α^+ kesmesi sırasıyla Eş. 3.3 ve Eş. 3.4'te gösterilmiştir (Klir ve Yuan, 1995; Ross, 2010).

$$A_\alpha = \left\{ x \in X \,\middle|\, \mu_A(x) \geq \alpha \right\} \tag{3.3}$$

$$A_{\alpha^+} = \left\{ x \in X \,\middle|\, \mu_A(x) > \alpha \right\} \tag{3.4}$$

α kesmesiyle (güçlü kesmesiyle (α^+)) A bulanık kümesi elemanlarının üyelik dereceleri α ya eşit yada büyük (α'dan büyük) olan A_α (A_{α^+}) kesin kümesine dönüşmektedir.

Tanım 3.3 : X evrensel kümesindeki bir bulanık A kümesinin özü, desteği, sınırı, geçiş noktaları ve yüksekliği Eş. 3.5-Eş. 3.9 ve Şekil 3.9'da gösterilmiştir (Klir ve Yuan, 1995; Ross, 2010).

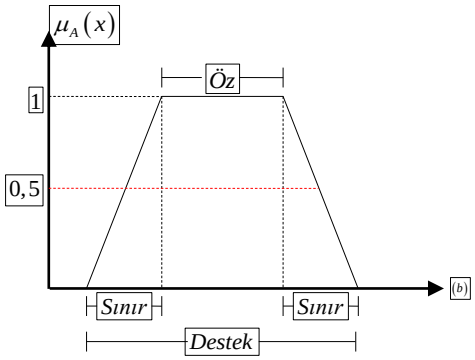
$$\text{Öz}(A) = \left\{ x \in X \,\middle|\, \mu_A(x) = 1 \right\} \tag{3.5}$$

$$\text{Destek}(A) = \left\{ x \in X \,\middle|\, \mu_A(x) > 0 \right\} \tag{3.6}$$

$$\text{Sınır}(A) = \left\{ x \in X \,\middle|\, 0 < \mu_A(x) < 1 \right\} \tag{3.7}$$

$$\text{Geçiş Noktaları}(A) = \left\{ x \in X \,\middle|\, \mu_A(x) = 0{,}5 \right\} \tag{3.8}$$

$$\text{Yükseklik}(A) = \sup_{x \in X} \left\{ \mu_A(x) \right\} \tag{3.9}$$



Şekil 3.13. Bulanık kümelerde öz, destek, sınır, geçiş noktaları ve yükseklik

Tanım 3.4 : X evrensel kümesinde bir bulanık A kümesinin konveks olması için Eş. 3.10'da verilen şartı sağlaması gerekir (Klir ve Yuan, 1995; Ross, 2010).

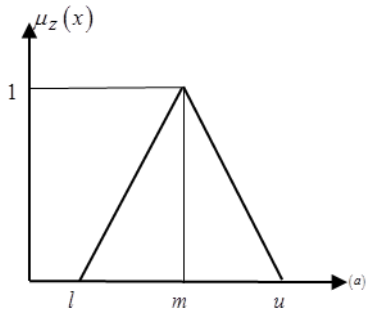
$$\mu_A\left(\lambda x_1+(1-\lambda)x_2\right)\geq \min\left(\mu_A(x_1),\mu_A(x_2)\right)\quad \forall x_1,x_2\in X,\ \lambda\in[0,1] \tag{3.10}$$

Tanım 3.5: X evrensel kümesinde bir bulanık A kümesinin normal olması için Eş. 3.11'de verilen şartı sağlaması gerekir (Klir ve Yuan, 1995; Ross, 2010).

$$\sup \mu_A(x)=1 \tag{3.11}$$

Supremum değeri, fonksiyonun maksimum değerini gösteremediğimiz durumlarda kullanılır. 1 değeri fonksiyonun bir üyesi olmadığı durumlarda, maksimum ifadesi yerine supremum (sup) değeri kullanılabilir.

Tanım 3.6: Z bulanık sayısının X evrensel kümesinde bir bulanık alt küme olabilmesi için konveks ve normal olması gerekir. Gerçek sayılar kümesinde tanımlanan bulanık sayılar çeşitli bulanık küme tipleri içerisinde özel öneme sahip altkümelerdir. Bulanık sayılar, verilen gerçek sayıya yaklaşık sayıların kümesi olduğu için belirsizliğin olduğu mühendislik uygulamalarında ve karar vermede sıklıkla kullanılmaktadır. Bulanık sayılar üyelik fonksiyonlarının şekillerine göre isimlendirilmektedir. Literatürde çok sayıda üyelik fonksiyonu tanımlanmakla birlikte işlem yükünün az olması nedeniyle en fazla kesikli, üçgen, gauss ve yamuk fonksiyonlar kullanılmaktadır. (Şekil 3.14)'de üçgensel bulanık sayının gösterimi verilmiştir. Üçgensel bulanık sayı için üyelik fonksiyonu Eş. 3.12'de tanımlanmıştır (Ross, 2010).

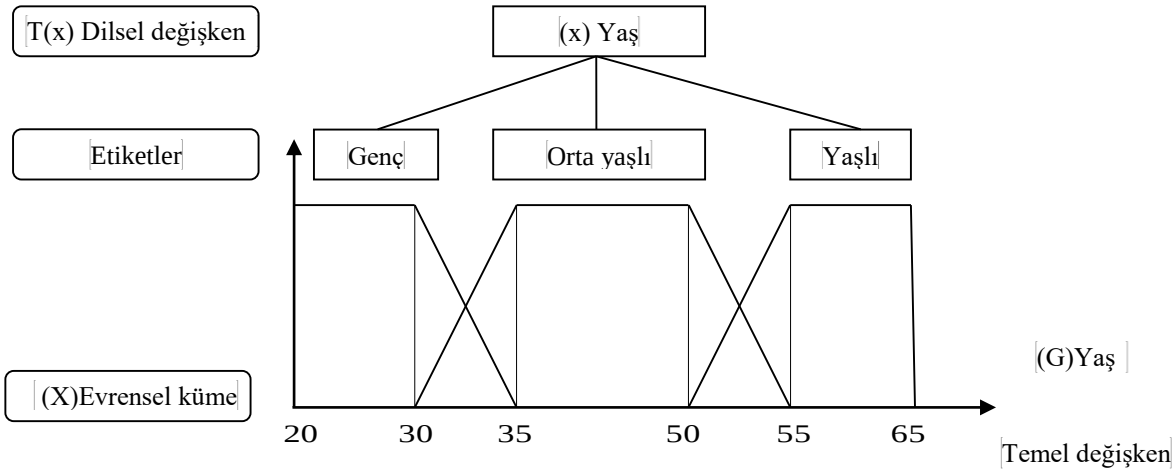


Şekil 3.14. Üçgensel bulanık küme

$$\mu_Z(x)=\begin{cases}0 & x<l\\ (x-l)/(m-l) & l\le x\le m\\ (u-x)/(u-m) & m\le x\le u\\ 0 & x>u\end{cases} \tag{3.12}$$

Tanım 3.7: İnsanların kararlarından, hislerinden ve algılarından etkilenen sistemlerin sayısal değerlerle modellenmesi oldukça zordur. Bu nedenle çok karmaşık olan düşünme ve karar verme süreçlerinde, kesin değerler yerine insan düşünce sistemine çok yakın olan dilsel değişkenler ve dilsel etiketlerin kullanılması gerekmektedir. Dilsel değişkenler, değerleri kesin sayı yerine kelimeler, doğal veya yapay dilde cümleler olan değişkenlerdir. Kesin sayılar yerine kelimeler ya da cümlelerin kullanılmasıyla daha az kesinliğin içerilmesi sağlanmaktadır. Örneğin yaş değişkenini ele aldığımızda "Ali gençtir" ifadesi "Ali 25 yaşındadır" ifadesine göre daha az kesindir. "Ali gençtir" ifadesinde "genç" yaş dilsel değişkenin dilsel etiketidir (Klir ve Yuan, 1995; Zadeh, 1975).

Bir dilsel değişken (x, T(x), X, G, M) fonksiyonuyla tanımlanabilir. Burada x dilsel değişkenin adını; T(x), x değişkeninin etiket kümesini ve X evrensel kümeyi göstermektedir. G sözdizimsel kuraldır ve T(x) kümesinde yer alan etiketleri üretir. M anlamsal kuraldır ve her A etiketin (bulanık küme) anlamını gösterir. M(A) ise X uzayındaki bir bulanık kümeyi gösterir. Örneğin x = "yaş" değişkeni olsun. Bu değişkenin T(x) etiket kümesi ise "genç", "orta yaşlı" ve "yaşlı" dilsel etiketlerinden oluşabilir. Dilsel terimler temel değişken olan yaşa göre atanan bulanık sayılarla ifade edilirler. Yaş için tanımlanan "genç" "orta yaşlı" ve yaşlı" etiketlerinin gösterimi Şekil 3.15'de verilmiştir.



Şekil 3.15. Yaş dilsel değişkeni için, alt ve üst sınırlarının gösterimi (Klir ve Yuan, 1995)

Tanım 3.8: Bulanık kümelerde dilsel etiketler üyelik dereceli dilsel eşiklerle değiştirilebilir. Dilsel atom $\Theta = \int_X \mu_\Theta(x)/x$ ile ilgili dilsel eşikler Eş. 3.13-Eş. 3.17'de verilmiştir (Klir ve Yuan, 1995; Ross, 2010).

$$"çok"\,\Theta = \Theta^2 = \int \frac{\left[\mu_\Theta(x)\right]^2}{x} \tag{3.13}$$

$$"çok\ çok"\,\Theta = \Theta^4 = \int \frac{\left[\mu_\Theta(x)\right]^4}{x} \tag{3.14}$$

$$"\ fazla"\,\Theta = \Theta^{1,25} = \int \frac{\left[\mu_\Theta(x)\right]^{1,25}}{x} \tag{3.15}$$

$$"çok\ az"\,\Theta = \sqrt{\Theta} = \int \frac{\left[\mu_\Theta(x)\right]^{0,5}}{x} \tag{3.16}$$

$$"oldukça\ az"\,\Theta = \Theta^{0,75} \tag{3.17}$$

Eş. 3.13-Eş. 3.15 verilen dilsel eşikler daraltma olarak adlandırılır. Daraltma elemanın kümeye ait olma derecesini azaltmaktadır. Üyelik derecesi 0,9 olan bir eleman "çok" dilsel eşiğiyle değiştirilse üyelik derecesi 0,81'e eşit olmaktadır. Bu durumda %10'luk bir azalma vardır. Üyelik derecesi 0,1 olan bir eleman "çok" dilsel eşiğiyle değiştirilse üyelik derecesi 0,01'e eşit olmaktadır. Bu durumda azalma %90'dır. Eş. 3.16-Eş. 3.17 verilen

dilsel eşikler genişletme olarak adlandırılır. Genişletme elemanın kümeye ait olma derecesini arttırmaktadır. Üyelik derecesi 0,81'e eşit bir eleman "çok az" dilsel eşiğiyle değiştirilirse üyelik derecesi 0,9'a eşit olmaktadır. Bu durumda üyelik derecesinde %11'lik bir artış olur. Bulanık kümelerde tanımlanan bir diğer operasyonda yoğunlaştırma operasyonudur. Yoğunlaştırma operasyonu üyelik derecesi 0,5'den küçük olan elemanın üyelik derecesini azaltmakta, üyelik derecesi 0,5'den büyük olan elemanın üyelik derecesini attırmaktadır. Eş. 3.18'de yoğunlaştırma operasyonunun tanımı verilmiştir. Bu operasyon, ÜF'ları arasında bir nevi ayrıştırma yapmayı sağlamaktadır.

$$\text{"}Yoğunlaşma\text{"}\ \Theta = \begin{cases} 2\mu_{\Theta}^{2}(x), & 0 \le \mu_{\Theta}(x) \le 0,5 \\ 1-2\left[1-\mu_{\Theta}(x)\right]^{2}, & 0,5 \le \mu_{\Theta}(x) \le 1 \end{cases} \tag{3.18}$$

Bulanık kümelerin kesişim durumu:

<u>*Tanım 3.9*</u>: X_1 ve X_2, X evrensel kümesinde tanımlanmış tip-1 bulanık kümeler ve bu kümelerin üyelik fonksiyonları $\mu_{X_1}(x)$ ve $\mu_{X_2}(x)$ ile gösterilsin (Klir ve Yuan, 1995; Ross, 2010).

X_1 ve X_2 kümelerinin kesişimi $X_1 \bigcap X_2$ ve üyelik fonksiyonu $\mu_{X_1 \cap X_2}(x)$ Eş. 3.19'daki gibi tanımlanır.

$$\otimes : [0,1] \times [0,1] \to [0,1]$$
$$\mu_{X_1 \cap X_2}(x) = \otimes\left(\mu_{X_1}(x), \mu_{X_2}(x)\right) \quad \forall x \in X \tag{3.19}$$

Bulanık kümelerin birleşim durumu:

<u>*Tanım 3.10*</u>: X_1 ve X_2, X evrensel kümesinde tanımlanmış tip-1 bulanık kümeler ve bu kümelerin üyelik fonksiyonları $\mu_{X_1}(x)$ ve $\mu_{X_2}(x)$ ile gösterilsin (Klir ve Yuan, 1995; Ross, 2010).

X_1 ve X_2 kümelerinin birleşimi $X_1 \bigcup X_2$ ve üyelik fonksiyonu $\mu_{X_1 \cup X_2}(x)$ Eş. 3.20'de tanımlanır.

$$\oplus : [0,1] \times [0,1] \to [0,1]$$
$$\mu_{X_1 \cup X_2}(x) = \oplus \left[\mu_{X_1}(x), \mu_{X_2}(x) \right] \quad \forall x \in X \tag{3.20}$$

Bulanık kümelerin tümleyeni:

<u>*Tanım 3.11*</u>: X_1, X evrensel kümesinde tanımlanmış tip-1 BK ve bu kümenin üyelik fonksiyonu $\mu_{X_1}(x)$ ile gösterilsin (Klir ve Yuan, 1995; Ross, 2010).

X_1 kümesinin tümleyeni $\neg X_1$ ve üyelik fonksiyonu Eş. 3.21'deki gibi tanımlanır.

$$N : [0,1] \to [0,1]$$
$$\mu_{\neg X_1}(x) = N\left(\mu_{X_1}(x) \right) \quad \forall x \in X \tag{3.21}$$

Bir fonksiyonun tümleyen olabilmesi için aşağıda verilen şartları sağlamalıdır. Bu özellikler $\forall x, y \in [0,1]$ için:

(A1(N)) $N(0) = 1$ ve $N(1) = 0$

(A2(N)) Eğer $x \le y$ ise $N(y) \le N(x)$ $\forall x, y \in [0,1]$

Eğer bulanık tümleyen aşağıda verilen iki özelliği de sağlıyorsa, katıdır.

(A3(N)) N 'nin sürekli bir fonksiyon olması

(A4(N)) Eğer $x < y$ ise $N(y) < N(x)$ $\forall x, y \in [0,1]$

Eğer bulanık tümleyen (A5(N)) özelliğini sağlıyorsa

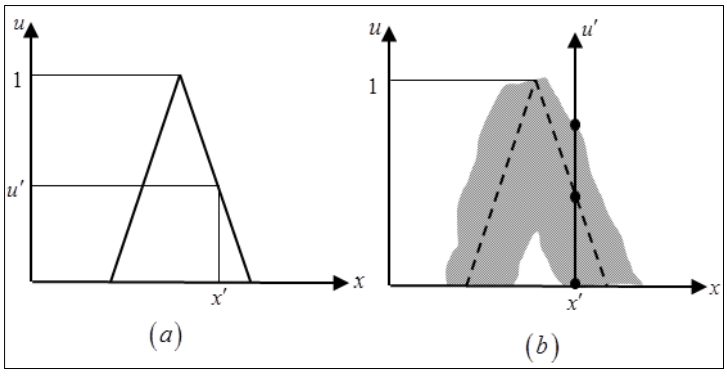
(A5(N)) $N\left(N(x) \right) = x$ $\forall x \in [0,1]$

Bulanık tümleyene kuvvetli bulanık tümleyen denir. $N(x)=1-x$ ve $N(x)=\sqrt{1-x^2}$ kuvvetli bulanık tümleyenlerdir.

3.5.2. Tip-2 bulanık kümeler

Tip-1 BK'lerde bir elemanın bir kümeye ait olma derecesini belirten üyelik fonksiyonu değeri [0,1] aralığındaki kesin bir değere eşittir. Şekil 3.16-a'da $x=x'$ noktasında bir u' değeri bulunmaktadır. Şekil 3.16-a'da gösterilen üyelik fonksiyonları değerleri sağa sola kaydırılarak Şekil 3.16-b'de gösterilen bulanıklaştırılmış tip-1 BK elde edilmektedir. Şekil 3.16-b'de $x=x'$ noktasında u' dikey ekseniyle gri alanın kesişmesiyle birden fazla u oluşmaktadır. Bu değerlerin eşit olarak ağırlıklandırılmaları gerekmemektedir. Bu nedenle tüm bu değerlere bir dağılım atanabilir. Tanım kümesinde verilen tüm elemanlar için bu işlem yapıldıktan sonra 3 boyutlu olan tip-2 üyelik fonksiyonu elde edilmektedir. Tip-1 BK'ler ve tip-2 BK'ler Zadeh tarafından önerilen tip-n bulanık kümelerin dereceleri sırasıyla 1 ve 2 olan özel halleridir (Mendel, 2017; Mendel ve John, 2002).

Tip-2 BK'ler belirsizliği ele almada tip-1 bulanık kümelere göre daha etkindir; çünkü tip-2 bulanık kümeler tip-1 BK'lere göre daha fazla parametreyle açıklanmaktadır. Fakat, bu durum hesaplama zorluğu ve anlaşılma güçlüğünü de beraberinde getirmektedir (M Mendel ve John, 2002).



Şekil 3.16. (a) Üçgensel Tip-1 üyelik fonksiyonu (b) Bulanıklaştırılmış üçgensel Tip-1 üyelik fonksiyonu

Bu bölümde kullanılacak olan semboller ve açıklamaları Çizelge 3.2'de verilmiştir.

Çizelge 3.2. Tip-2 BK'yi tanımlamada kullanılan semboller ve açıklamaları

Sembol	Açıklama
x	Birincil değişken
u	İkincil değişken
$\tilde{A}$	Tip-2 bulanık küme
J_x	Birincil üyelik derecesi
$u_{\tilde{A}}(x,u)$ $\left(f_x(u)/u\right)$	İkincil üyelik derecesi

Tanım 3.12 : $x \in X$ ve $u \in J_x \subseteq [0,1]$ iken $\tilde{A}$ bir tip-2 BK, $u_{\tilde{A}}(x,u)$'de bu kümenin tip-2 üyelik fonksiyonu olmak üzere, tip-2 BK $\tilde{A}$, Eş. 3.22'de tanımlanmıştır (Mendel, 2017; Mendel ve John, 2002).(Jerry M Mendel, 2017)

$$\tilde{A} = \left\{ \left\langle (x,u), \mu_{\tilde{A}}(x,u) \right\rangle \middle| \forall x \in X,\ \forall u \in J_x \subseteq [0,1] \right\} \tag{3.22}$$

$0 \le \mu_{\tilde{A}}(x,u) \le 1$'dir.

Tip-2 BK $\tilde{A}$, aynı zamanda Eş. 3.23'deki gibi ifade edilebilir.

$$\tilde{A} = \int_{x \in X} \int_{u \in J_x} \frac{\mu_{\tilde{A}}(x,u)}{(x,u)} \quad J_x \subseteq [0,1] \tag{3.23}$$

$\int\int$ simgesi sürekli değer alan *x* ve *u*'ların birleşimini göstermektedir. Eğer evrensel küme kesikli formda tanımlanırsa $\iint$ simgesi yerine $\sum\sum$ simgesi kullanılmalıdır.

Tanımda verilen $0 \le \mu_{\tilde{A}}(x,u) \le 1$ kısıtlaması tip-1 BK'lerde verilen $0 \le \mu_{\tilde{A}}(x) \le 1$'de verilen kısıtlamayla aynıdır. Belirsizlik ortadan kalktığı zaman tip-2 BK tip-1 BK'ya dönüşmektedir ve u $\mu_{\tilde{A}}(x)$'e eşit olmaktadır.

Tanım 3.13 : $x \in X$ ve $\forall u \in J_x \subseteq [0,1]$ olmak üzere x' in her bir değeri için $(x = x')$ ikincil üyelik fonksiyonu değeri $\mu_{\tilde{A}}(x,u)$ ekseninin dikey kesitine eşittir (Mendel, 2017; Mendel ve John, 2002).

$$\mu_{\tilde{A}}(x = x', u) = \mu_{\tilde{A}}(x') = \int_{u \in J_{x'}} \frac{f_{x'}(u)}{u} J_{x'} \subseteq [0,1] \tag{3.24}$$

Eş. 3.24 Yardımıyla tip-2 BK $\tilde{A}$ Eş. 3.35'deki gibi

$$\tilde{A} = \left\{ \left\langle x, \mu_{\tilde{A}}(x) \right\rangle \middle| \forall x \in X \right\} \tag{3.25}$$

ya da Eş. 3.26'daki gibi tanımlanabilir.

$$\tilde{A} = \int_{x \in X} \frac{\mu_{\tilde{A}}(x)}{x} = \int_{x \in X} \left[\int_{u \in J_x} f_x(u)/u \right] / x \qquad J_x \subseteq [0,1] \tag{3.26}$$

Tanım 3.14 : İkincil üyelik fonksiyonuna ait tanım kümesi *x*'in birincil üyeliği olarak isimlendirilmektedir. Eş. 3.26'da J_x, *x*'in birincil üyelik fonksiyonudur. Burada $\forall x \in X$ için $J_x \subseteq [0,1]$'dir. Eş. 3.26'da $f_x(u)$ ikincil fonksiyonun büyüklüğünü gösteren ikincil derecedir (Mendel, 2017; Mendel ve John, 2002).

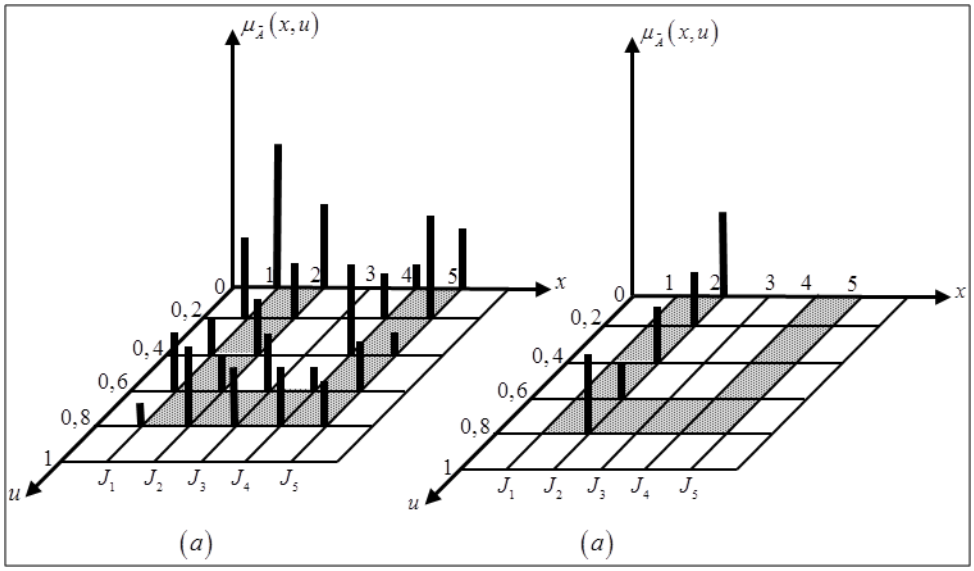
X ve J_x kesikli değerlere sahip ise $\tilde{A}$ Eş. 3.27'deki gibi ifade edilir.

$$\begin{aligned}
\tilde{A} &= \sum_{x \in X} \left[\sum_{u \in J_x} f_x(u)/u \right] / x \\
&= \sum_{i=1}^{N} \left[\sum_{u \in J_{x_i}} f_{x_i}(u)/u \right] / x_i \\
&= \left[\sum_{k=1}^{M_1} f_{x_1}(u_{1k})/u_{1k} \right] / x_1 + \ldots + \left[\sum_{k=1}^{M_N} f_{x_N}(u_{Nk})/u_{Nk} \right] / x_N
\end{aligned} \tag{3.27}$$

Eş. 3.27'de "+" simgesi elemanların birleşimini göstermektedir. X değeri N tane kesikli değere sahiptir ve her bir J_x değeri M_i tane kesikli değere sahiptir.

<u>*Örnek :*</u> Şekil 3.13-a'da x ve u kesikli değer alan değişkenler olmak üzere tip-2 üyelik fonksiyonu $\mu_{\tilde{A}}(x,u)$ dikey kesit gösterim şekli verilmiştir. $X=\{1,2,3,4,5\}$ ve $U=\{0,0,2,0,4,0,6,0,8\}$'dir. Şekil 3.13-b'de $x=2$'de tip-2 üyelik fonksiyonu gösterilmektedir (Mendel, 2017; Mendel ve John, 2002).

$x=2$'de ikincil üyelik fonksiyonu $\mu_{\tilde{A}}(2)=0,5/0+0,35/0,2+0,35/0,4+0,2/0,6+0,5/0,8$'dir. Birincil üyelikler ise $J_1,J_2,J_4,J_5=\{0,0,2,0,4,0,6,0,8\}$ ve $J_3=\{0,6,0,8\}$'dir.



Şekil 3.17. (a) 3 boyutlu tip-2 üyelik fonksiyonu (b) noktasında tip-2 üyelik fonksiyonunun dikey kesit gösterimi (Jerry M Mendel ve John, 2002)

Tanım 3.16: Tip-2 BK'nın birincil üyeliklerindeki belirsizlik, Belirsizliğin Kapladığı Alan (BKA) olarak adlandırılan sınırlı bir alan oluşturur. BKA tüm birincil üyeliklerin birleşimidir (Mendel, 2017; Mendel ve John, 2002).

$$BKA(\tilde{A})=\bigcup_{x\in X} J_x \tag{3.28}$$

BKA kavramı sadece tip-2 BK'lerin üyelik fonksiyonundaki belirsizliğe odaklanmayıp aynı zamanda tip-2 üyelik fonksiyonlarının ikincil dereceleri için uygun destek aralığı sağlamaktadır. Ayrıca BKA tip-2 BK'lerin 3 boyutlu grafik yerine 2 boyutlu grafikle gösterilmesini sağlar.

Tanım 3.17: *X* ve *U* kesikli evrensel kümeler $\tilde{A}_e$ *N* elemana sahip gömülü tip-2 BK olup $J_{x_1}, J_{x_2}, \ldots, J_{x_N}$'den kesinlikle bir tane eleman kapsamaktadır. $u_1, u_2, \ldots, u_N$ ikincil değişkenler ve ilgili ikincil üyelik dereceleri $f_{x_1}(u_1), f_{x_2}(u_2), \ldots, f_{x_N}(u_N)$ olmak üzere $\tilde{A}_e$ gömülü tip-2 BK Eş. 3.29'de tanımlanmıştır (Mendel, 2017; Mendel ve John, 2002).

$$\tilde{A}_e = \sum_{i=1}^{N} \left[f_{x_i}(u_i) / u_i \right] / x_i \quad u_i \in J_{x_i} \subseteq [0,1] \tag{3.29}$$

Tip-2 bulanık $\tilde{A}$ kümesindeki $\tilde{A}_e$ gömülü tip-2 BK'lerin sayısı $\prod_{i=1}^{N} M_i$ kadardır. *X* ve *U* kesikli evrensel kümeler için, *N* elemanlı gömülü tip-1 BK, A_e, Eş. 3.30'da tanımlanmıştır.

$$A_e = \sum_{i=1}^{N} u_i / x_i \quad u_i \in J_{x_i} \subseteq [0,1] \tag{3.30}$$

A_e kümesi Eş. 3.31'de ki $\tilde{A}_e$ kümesinin tüm birincil üyeliklerinin birleşimidir ve toplam sayısı $\prod_{i=1}^{N} M_i$ kadardır.

Teorem 3.1. Şekil 3.18'de BKA gri alan ile gösterilmiştir. u_i ekseninde bulunan her bir nokta düğüm olarak adlandırılsın. u_i ekseni boyunca her bir düğüm

$$n_l = \prod_{j=1, j\neq l}^{N} M_j \tag{3.31}$$

tane gömülü tip-2 BK kapsar (Mendel, 2017; Mendel ve John, 2002).

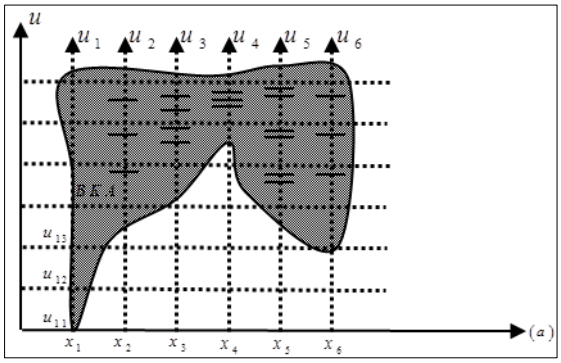
Teorem 3.2. $\tilde{A}_e^j$, j. gömülü tip-2 BK, Eş. 3.32'de ki gibi tanımlansın (Mendel, 2017; Mendel ve John, 2002).

$$\tilde{A}_e^j \equiv \left\{\left(u_i^j, f_{x_i}\left(u_i^j\right)\right), i = 1,\ldots,N\right\} \tag{3.32}$$

Tip-2 BK, tüm gömülü tip-2 BK'lerin birleşiminden oluşur.

$$\tilde{A} = \sum_{j=1}^{n} \tilde{A}_e^j \tag{3.33}$$

$$n \equiv \prod_{i=1}^{N} M_i \tag{3.34}$$



Şekil 3.18. Kesikli u ve x eksenlerinde BKA (Mendel ve John, 2002)

3.5.3. Aralıklı tip-2 bulanık kümeler

Tip-2 BK'lerde ikincil üyelik fonksiyonu birden çok değer alabilmektedir ve bu değerlere bir dağılım atanabilir. Düzgün dağılım atandığı takdirde ikincil üyelik fonksiyonlarının değeri bire (1'e) eşit olup tip-2 BK'ler aralıklı tip-2 BK'ler olarak adlandırılır. Dubois ve Parade , Gehrke, Walker ve Walker, aralıklı BK'nın aralıklı tip-2 BK'ya denk olduğunu göstermişlerdir. Bu nedenle bu bölümde aralıklı tip-2 BK ile aralıklı BK'nın gösterimi aynıdır. Bu bölümde aralıklı tip-2 BK'lerle ilgili temel tanımlar verilmiştir (Dubois ve Prade, 2005; Gehrke, Walker, ve Walker, 1996).

Tanım 3.18.: Tip-2 BK'da $\mu_{\tilde{A}}(x,u)=1 \ \forall x,u$ olduğu takdirde $\tilde{A}^I$, aralıklı tip-2 BK olarak adlandırılır (Mendel, John, ve Liu, 2006).

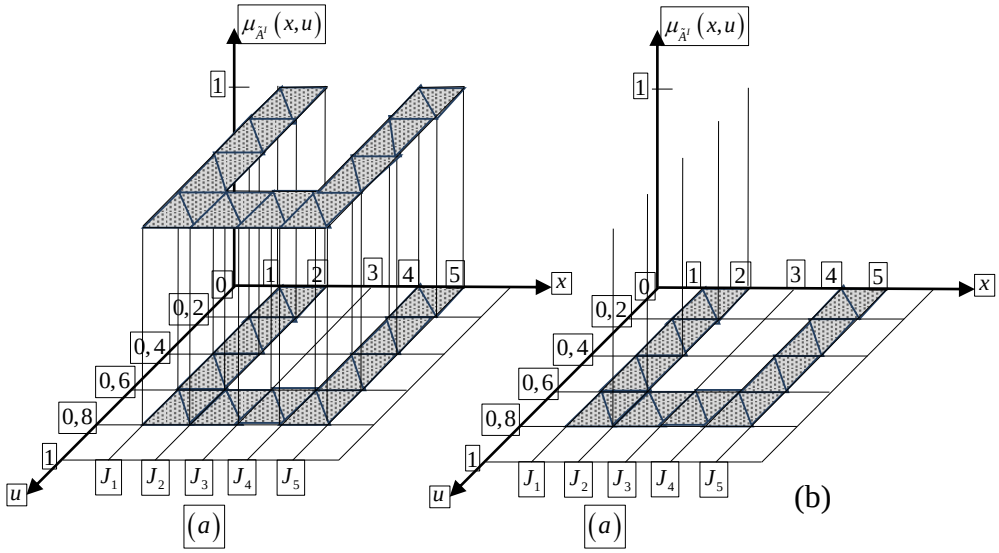
$$\tilde{A}^I = \int_{x\in X}\int_{u\in J_x} 1/(x,u) \quad J_x \subseteq [0,1] \tag{3.35}$$

Tanım 3.19: $x' \in X$ ve $\forall u \in J_x \subseteq [0,1]$ olmak üzere x'in her bir değeri için $(x=x')$ ikincil üyelik fonksiyonu değeri $\mu_{\tilde{A}^I}(x,u)$ ekseninin dikey kesitine eşittir (Mendel ve arkadaşları, 2006).

$$\mu_{\tilde{A}^I}(x=x',u)=\mu_{\tilde{A}^I}(x')=\int_{u\in J_{x'}} 1/u \quad J_{x'}\subseteq[0,1]$$

$$\tilde{A}^I=\int_{x\in X}\mu_{\tilde{A}^I}(x)/x=\int_{x\in X}\left[\int_{u\in J_x} 1/u\right]/x \quad J_x\subseteq[0,1] \tag{3.36}$$

Örnek: x ve u kesikli değer alan değişkenler olmak üzere aralıklı tip-2 üyelik fonksiyonu $\mu_{\tilde{A}^I}(x,u)$ dikey kesit gösterimi Şekil 15-a'dadır. $X=\{1,2,3,4,5\}$ ve $U=\{0,0,2,0,4,0,6,0,8\}$'dir (Mendel ve arkadaşları, 2006).



Şekil 3.19. (a) 3 boyutlu aralıklı tip-2 üyelik fonksiyonu 2.derece üyelik fonksiyonları 1'e eşitlenmiş (b) noktasında aralıklı tip-2 üyelik fonksiyonunun dikey kesit gösterimi (Jerry M Mendel vd.., 2006)

Tanım 3.20: BKA bir alandır ve alt ve üst sınırları belirlidir. Aralıklı tip-2 BK için alt ve üst sınırları tip-1 üyelik fonksiyonudur ve bunlar alt ve üst üyelik fonksiyonları olarak adlandırılmıştır. Eş. 3.37 ve Eş. 3.38'de BKA'nın alt ve üst sınırları ile ilgili alt ve üst üyelik fonksiyonları tanımlanmıştır (Mendel ve arkadaşları 2006).

$$\underline{\mu}_{\tilde{A}^I}(x) \equiv \underline{BKA\left(\tilde{A}^I\right)} \quad \forall x \in X \tag{3.37}$$

$$\overline{\mu}_{\tilde{A}^I}(x) \equiv \overline{BKA\left(\tilde{A}^I\right)} \quad \forall x \in X \tag{3.38}$$

Aralıklı tip-2 BK'ler için $J_x = \left[\underline{\mu}_{\tilde{A}^I}(x), \overline{\mu}_{\tilde{A}^I}(x)\right], \forall x \in X$

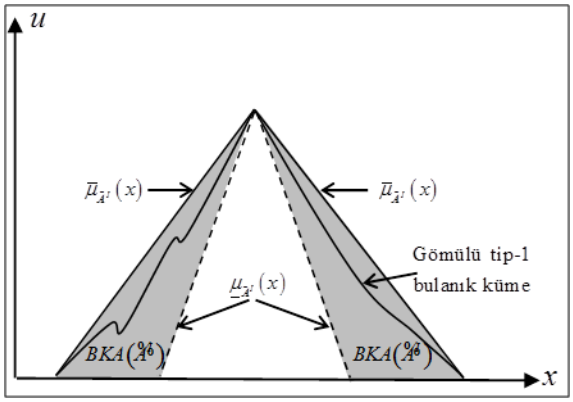
Tanım 3.21.: X ve U kesikli evrensel kümeler için, N elemanlı gömülü aralıklı tip-2 BK $\tilde{A}_e^I$ Eş. 3.39'da verilmiştir (Mendel ve arkadaşları, 2006).

$$\tilde{A}_e^I = \sum_{i=1}^{N} \left[1/u_i\right]/x_i \quad u_i \in J_{x_i} \subseteq [0,1] \tag{3.39}$$

Aralıklı tip-2 bulanık $\tilde{A}^I$ kümesinde $\tilde{A}_e^I$ gömülü kümelerin sayısı $\prod_{i=1}^{N} M_i$ kadardır. X ve U kesikli evrensel kümeler için, N elemanlı gömülü tip-1 BK'sı A_e Eş. 3.40' da verilmiştir.

$$A_e = \sum_{i=1}^{N} u_i / x_i \quad u_i \in J_{x_i} \subseteq [0,1] \tag{3.40}$$

A_e kümesi Eş. 3.39'daki $\tilde{A}_e^I$ kümesinin tüm birincil üyeliklerinin birleşimidir ve toplam sayısı $\prod_{i=1}^{N} M_i$ kadardır. Şekil 3.20'de gömülü tip-1 BK'sı gösterilmektedir.



Şekil 3.20. Aralıklı tip-2 bulanık küme için BKA alt, üst üyelik fonksiyonları ve gömülü tip-1 bulanık kümenin gösterimi

Teorem 3.3: X ve U kesikli olup, aralıklı tip-2 BK'sı $\tilde{A}^I$, tüm gömülü aralıklı tip-2 BK'lerin birleşiminden oluşur (Mendel ve arkadaşları 2006).

$$\tilde{A}^I = \sum_{j=1}^{n_A} \tilde{A}_{e_j}^I \quad \left(j = 1,2,3,\ldots,n_A\right) \tag{3.41}$$

$$\tilde{A}_{e_j}^I = \sum_{i=1}^{N} \left[1/u_i^j\right]/x_i \quad u_i^j \in J_{x_i} \subseteq [0,1] \tag{3.42}$$

ve

$$n_A = \prod_{i=1}^{N} M_i \tag{3.43}$$

Sonuç 3.1: Aralıklı tip-2 BK'lerin ikincil dereceleri 1'e eşit olduğu için Eş. 3.41 ve Eş. 3.42'de tanımlanan $\tilde{A}^I$ ve $\tilde{A}_{e_j}^I$ kümeleri Eş. 3.44-Eş. 3.46'daki gibi tanımlanabilir (Mendel ve arkadaşları 2006).

$$\tilde{A}^I = 1/BKA\left(\tilde{A}^I\right) \tag{3.44}$$

$$BKA\left(\tilde{A}^I\right) = \sum_{j=1}^{n_A} A_e^j = \begin{cases} \left\{\underline{\mu}_{\tilde{A}^I}(x),\ldots,\bar{\mu}_{\tilde{A}^I}(x)\right\} & \forall x \in X_k \\ \left[\underline{\mu}_{\tilde{A}^I}(x),\bar{\mu}_{\tilde{A}^I}(x)\right] & \forall x \in X \end{cases} \tag{3.45}$$

ve

$$A_e^j = \sum_{i=1}^{N} u_i^j / x_i \quad u_i^j \in J_{x_i} \subseteq [0,1] \tag{3.46}$$

Eş. 3.45'in ilk satırında yer alan ifade de kesikli ve n_A tane eleman (fonksiyon) içermektedir, ikinci satırdaki ifadede evrensel küme süreklidir ve $\forall x \in X \;\; \overline{\mu}_{\tilde{A}^I}(x) - \underline{\mu}_{\tilde{A}^I}(x)$ aralığında sonsuz sayıdaki elemanı içermektedir.

İspat: Her bir gömülü aralıklı tip-2 BK, $\tilde{A}^I_{e_j} \;\; 1/A^j_e$ şeklinde ifade edildiğinde Eş. 3.44, Eş. 3.47'deki gibi ifade edilebilir.

$$\tilde{A}^I = \sum_{i=1}^{n_A} \left(1/A_{e_j}\right) = 1/\sum_{i=1}^{n_A} \left(A_{e_j}\right) \equiv 1/BKA\left(\tilde{A}^I\right) \tag{3.47}$$

$\underline{\mu}_{\tilde{A}^I}(x)$ ve $\overline{\mu}_{\tilde{A}^I}(x)$ A^j_e kümesinin n_A tane elemanlarından ikisi olup alt ve üst sınır fonksiyonlarıdır. Bu nedenle $BKA\left(\tilde{A}^I\right)$ kesikli evrensel kümelerde Eş. 3.45'in ilk satırında yer alan ifadeyle, sürekli evrensel kümelerde ise Eş. 3.45'in ikinci satırında yer alan ifadeyle açıklanabilir.

Tanım 3.21: $\tilde{A}^I$ ve $\tilde{B}^I$ aralıklı tip-2 BK'ler olmak üzere bu kümelerin birleşimi, kesişimi ve $\tilde{A}^I$ aralıklı tip-2 BK'sının tümleyeni sırasıyla Eş. 3.48-Eş. 3.50'de verilmiştir (Mendel ve arkadaşları 2006).

$$\tilde{A}^I \cup \tilde{B}^I = 1/\left[\underline{\mu}_{\tilde{A}^I}(x) \vee \underline{\mu}_{\tilde{B}^I}(x), \overline{\mu}_{\tilde{A}^I}(x) \vee \overline{\mu}_{\tilde{B}^I}(x)\right] \tag{3.48}$$

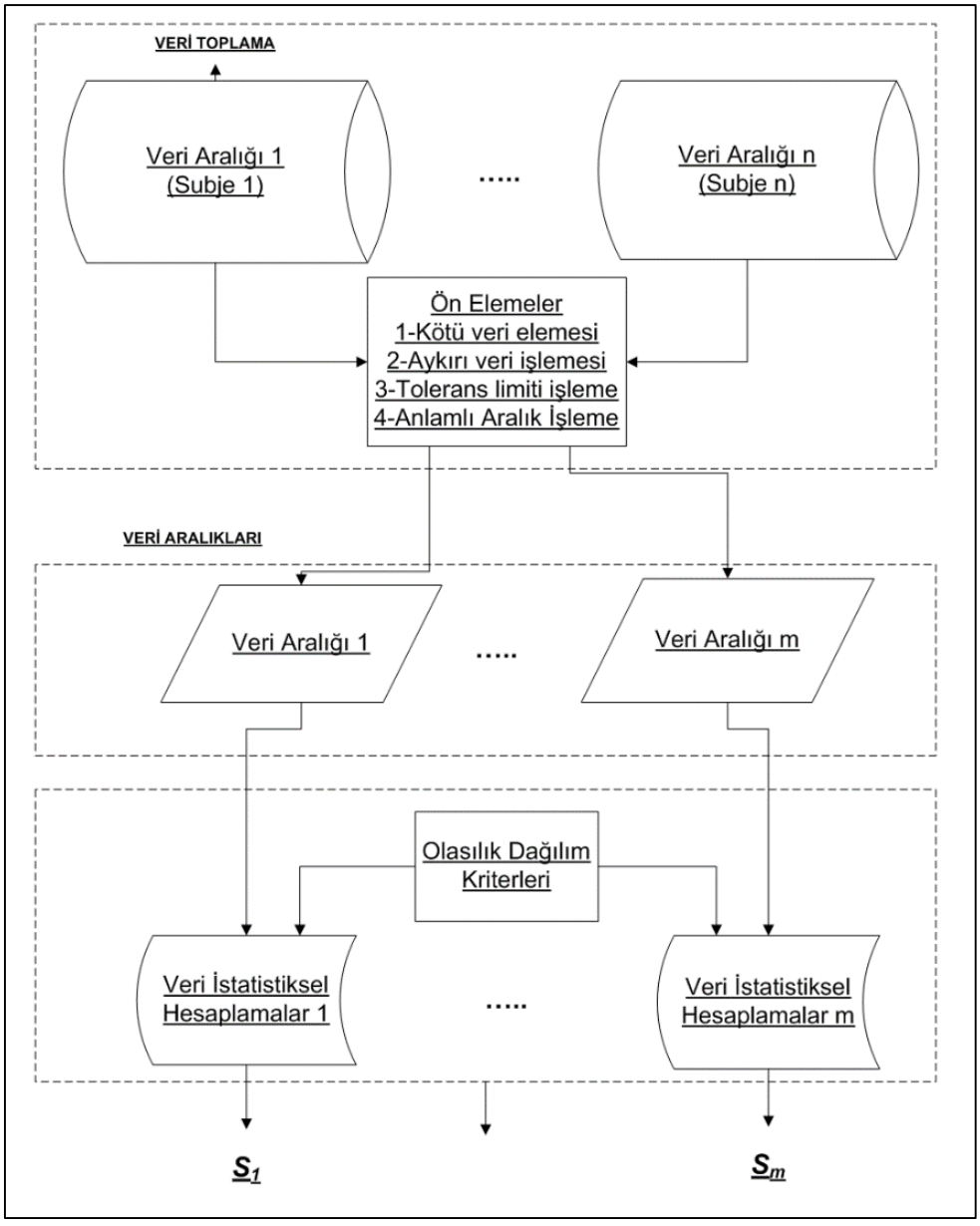
$$\tilde{A}^I \cap \tilde{B}^I = 1/\left[\underline{\mu}_{\tilde{A}^I}(x) \wedge \underline{\mu}_{\tilde{B}^I}(x), \overline{\mu}_{\tilde{A}^I}(x) \wedge \overline{\mu}_{\tilde{B}^I}(x)\right] \tag{3.49}$$

$$\overline{\tilde{A}}^I = 1/\left[1 - \overline{\mu}_{\tilde{A}^I}(x), 1 - \underline{\mu}_{\tilde{A}^I}(x)\right] \tag{3.50}$$

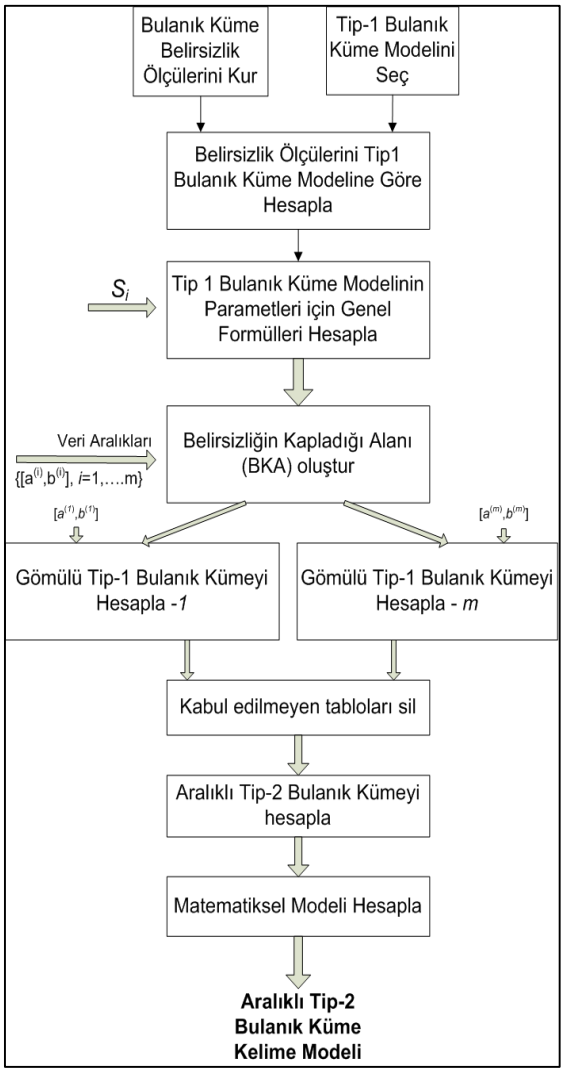
Buraya kadar Bulanık Kümelerin tanımları, matematiksel olarak ifadeleri, aritmetik işlemler anlatılmıştır. Bu bölümden sonra bir bulanık kümenin oluşturulma aşamaları, esnasında kullanılan yöntemler ve veri işleme sürecini kısaca izah edilmektedir.

3.5.4. Gelişmiş aralıklı küme yaklaşımı

Gelişmiş Aralıklı Küme Yaklaşımının yapısı, aralıklı küme yaklaşımına çok enzemektedir. Şekil 3.21ve Şekil 3.22'de gösterildiği gibi veri bölümü ve bulanık küme bölümü içermektedir.



Şekil 3.21. Veri seti



Şekil 3.22. Bulanık küme seti

Adım 1. Aralık tanımlama:

Aralıklı tip-2 BK'ler oluşturmak için ilk olarak $0 \le a^{(i)} < b^{(i)} \le 10$ ve $b^{(i)} - a^{(i)} < 10$ şartını sağlayan aralıklı değerler dikkate alınır ve bunun dışındakiler reddedilir. Bu adımda *n* adet olan aralıklı son nokta sayısı, *n'* adete indirgenir.

Adım 2. Aykırı veriyi işleme:

Box ve Whisker testleri (Kutu Bıyık grafiği) önce $a^{(i)}$ ve $b^{(i)}$ üzerine sonra $L^{(i)} = b^{(i)} - a^{(i)}$ üzerine uygulanarak $Q_a(.25), Q_a(.75), IQR_a, Q_b(.25), Q_b(.75)$ değerleri, adım-1'deki veriye göre ise IQR_b değeri hesaplanır. Sonuç olarak sadece

Eş.**Hata! Başvuru kaynağı bulunamadı.-Hata! Başvuru kaynağı bulunamadı.**'de verilen şartları sağlayan aralıklı değerlerin kalmasına müsaade edilir;

$$a^{(i)} \in \left[Q_a(.25) - 1.5IQR_a, Q_a(.75) + 1.5IQR_a \right] \tag{3.51}$$

$$b^{(i)} \in \left[Q_b(.25) - 1.5IQR_b, Q_b(.75) + 1.5IQR_b \right] \tag{3.52}$$

Bu işlemden sonra *n'* adet olan son noktaların sayısı, *n''* adet son nokta sayısına indirgenir. Daha sonra $Q_L(.25), Q_L(.75)$ ve IQR_L değerleri kalan *n''* aralıklarına göre hesaplanır ve sadece Eş. 3.53'te verilen şartı sağlayan aralıklı sayıların kalmasına müsaade edilir:

$$L^{(i)} \in \left[Q_L(.25) - 1.5IQR_L, Q_L(.75) + 1.5IQR_L \right] \tag{3.53}$$

Bu işlemden sonra *n''* adet olan aralık son nokta sayısı *m' adet* aralık son nokta sayısına indirgenir. Burada gelişmiş aralıklı kümeden farkı, aralıklı küme yaklaşımında, bu üç test eşzamanlı olarak yapılmaktadır.

Adım 3. Tolerans limiti işleme:

Normal dağılımın özelliği kullanılarak bir tolerans limit değeri belirlenir ve bu limit değerlerin dışında kalan değerler elemine edilir. Bunu gerçekleştirmek için ilk olarak $a^{(i)}$ ve $b^{(i)}$ daha sonra $L^{(i)} = b^{(i)} - a^{(i)}$ değerleri için tolerans değerleri belirlenir Eş. 3.54-3.55'te verilen şartları sağlayan aralıklar bir sonraki işlem için dikkate alınır.

$$a^{(i)} \in \left[m_a - k\sigma_a, m_a + k\sigma_a \right] \tag{3.54}$$

$$b^{(i)} \in \left[m_b - k\sigma_b, m_b + k\sigma_b \right] \tag{3.55}$$

Eş.3.54 ve 3.55 belirtilen m_a, m_b değerleri $a^{(i)}$ ve $b^{(i)}$ değerlerinin ortalamalarını, σ_a, σ_b değerleri $a^{(i)}$ ve $b^{(i)}$ değerlerinin standart sapmalarını, *k* katsayısı ise istatistikte kullanılan güven seviyesine karşılık gelen katsayıdır. Bu katsayı eğer güven seviyesi % 95 e karşılık gelen bir katsayı ise bu şartı sağlayan verinin oranı % 95'dir. Bu yaklaşımda son

noktaların normale çok yakın dağıldığı kabul edilmektedir. Bu adım m' olan aralık son nokta sayısını m^+ aralıklı son nokta sayısına indirger. Kalan veriden m_L ve σ_L değerleri hesaplanır ve Eş.3.56'da verilen şartı sağlayan aralıklı veriler dikkate alınır.

$$L^{(i)} \in \left[m_L - k'\sigma_L, m_L + k'\sigma_L\right] \tag{3.56}$$

Eş. belirtilen $k' = \min(k_1, k_2, k_3)$ eşitliği ile bulunur. Bu eşitlikte k_1 katsayısı güven seviyesi % 95 sağlayan ve $\left[m_L - k_1\sigma_L, m_L + k_1\sigma_L\right]$ değerinin % 95'ini içerecek şekilde belirlenir. k_2 ve k_3 değerleri Eş.3.57,3.58 yardımı ile hesaplanır.

$$k_2 = m_L / \sigma_L \tag{3.57}$$

$$k_3 = \left(10 - m_L\right) / \sigma_L \tag{3.58}$$

k_2 değeri $m_L - k'\sigma_L \geq 0$ şartını ve k_3 değeri de $m_L + k'\sigma_L \leq 10$ şartını sağlar. Bu kısıtlamalar $L^{(i)}$ değerinin çok küçük ve çok büyük olduğu durumlarını elemine eder. Bu adım ile m^+ aralık son noktaları m'' aralık son noktalarına indirgenmiş olur.

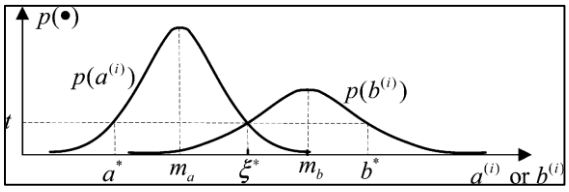
Gelişmiş aralıklı yaklaşımda, önceki model olan aralıklı yaklaşım modelindeki tolerans limitlerine ek olarak şu iki noktada yenilik getirmiştir:

a- Aralıkların kaldırılması için, $L^{(i)}$ değerinin testi ile $a^{(i)}$ ve $b^{(i)}$ değerlerinin testi birbirinden bağımsız olarak gerçekleştirilmiştir.

b- k değerini elde etmek için fazladan iki sınırlama daha getirilerek $L^{(i)}$ değerinin çok küçük ve çok büyük değerleri elenmiştir.

Adım 4. Mantıklı Aralık İşleme:

Liu ve Mendel tarafından yapılan çalışma mantıklı aralık işleme adımında sadece aralıkların çakışmamasını değil aynı zamanda aşırı derecede uzun aralıkların olmamasını da sağlar. Şekil 3.23'de bu durum gösterilmektedir (Wu, Mendel, and Coupland, 2012).



Şekil 3.23. Mantıklı aralık testi

Aralıklı yaklaşımda, Mantıklı aralıklar $a^{(i)} < \xi^* < b^{(i)}$ olmalı. Gelişmiş aralıklı yaklaşımda ise $a^* < a^{(i)} < \xi^* < b^{(i)} < b^*$ aralıklar olmalıdır.

Liu ve Mendel tarafından yapılan çalışmada eşik değeri olan ξ^* değerini Eş.3.59 kullanılarak hesaplanır.

$$\xi^* = \frac{\left\{\left(m_b\sigma_a^2 - m_a\sigma_b^2\right) \pm \sigma_a\sigma_b\sqrt{\left[\left(m_a - m_b\right)^2 + 2\left(\sigma_a^2 - \sigma_b^2\right)\ln\left(\sigma_a/\sigma_b\right)\right]}\right\}}{\left(\sigma_a^2 - \sigma_b^2\right)} \tag{3.59}$$

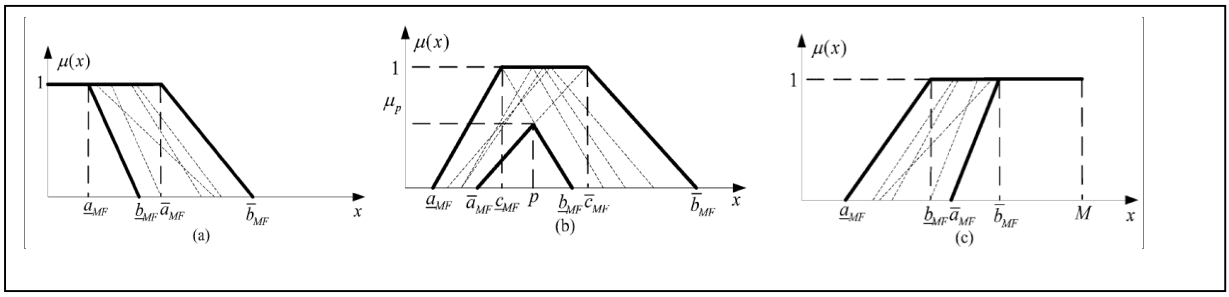
Liu ve Mendel tarafından yapılan çalışmada $a^{(i)} < \xi^*$ ve $b^{(i)} < \xi^*$ şartını sağlayan aralıklar dikkate alınmaktadır. Şekil incelendiğinde ξ^* değeri $p^{(a^{(i)})}$ ve $p^{(b^{(i)})}$ normal dağılımlarının kesişim noktası olduğu görülmektedir. Diğer bir değişle, $p^{(a^{(i)})} = p^{(b^{(i)})} = t$ olduğu durumda ξ^* değeri elde edilmektedir. Bu eşitliğin sadece bir çözümü olmadığı ayrıca Eş. 3.60'da belirtilen iki farklı çözümünün de olduğu görülecektir:

$$\begin{cases} a^{(i)} = a^* = m_a - (\xi^* - m_a) = 2m_a - \xi^* \\ b^{(i)} = b^* = m_b - (\xi^* - m_b) = 2m_b - \xi^* \end{cases} \tag{3.60}$$

Eş.3.60'da tanımlanan m_a ve m_b değerleri Adım 3'den sonra arta kalan aralıklı sayıların sağ ve sol son noktalarının ortalamalarını temsil etmektedir. Eş.3.61'de tanımlanan şartı sağlayan aralıklar dikkate alınarak aralıklı tip-2 BK'lerin elde edilmesinde nihai olarak kullanılacaktır.

$$2m_a - \xi^* < a^{(i)} < \xi^* < b^{(i)} < 2m_b - \xi^* \tag{3.61}$$

Aralıklı Yaklaşımda önerilen mantıklı aralık işleme ile karşılaştırıldığında, $a^{(i)}$ nin alt limitlerine, $b^{(i)}$ nin üst limitlerine, kısıtlamalar eklenmiş olmakta buda gerekli aralıkların genişliğinin kontrol edilmesini sağlar. Bu işlem sonrası $m"$ adet olan aralıklı sayı m adete indirgenir.



Şekil 3.24. (a) Sol omuz tipi BKA (b) İçsel tip BKA (c) Sağ omuz tipi BKA

Bu dört adımdan sonra aralıklı tip-2 bulanık kümelerin oluşturulması aşamasına geçilir.
Aralıklı tip-2 bulanık kümelerin oluşturulması için
Şekil Şekil 3.24'de gösterilen 3 farklı tipteki belirsizliğin kapladığı alan (BKA) çeşitleri dikkate alınır.

Aralıklı tip-2 bulanık kümelerin oluşturulması için aşağıda tanımlanan adımlar izlenir;

1. m adet olan aralıklı sayının alt ve üst değerlerine ait ortalama değerler Eş.3.62-3.63 kullanılarak elde edilir.

$$m_l = \frac{1}{m}\sum_{i=1}^{m} a^{(i)} \tag{3.62}$$

$$m_r = \frac{1}{m}\sum_{i=1}^{m} b^{(i)} \tag{3.63}$$

2. İçsel tip BKA'nın modellenebilmesi için $c^{(i)}$ ve $d^{(i)}$ Eş.3.64-3.65 kullanılarak bulunur.

$$c^{(i)} = b^{(i)} - 5{,}831a^{(i)}, \quad i = 1, 2, ..., m \tag{3.64}$$

$$d^{(i)} = b^{(i)} - 0{,}171a^{(i)} - 8{,}29, \quad i = 1, 2, ..., m \tag{3.65}$$

s_c ve s_d c ve d değerlerinin standart sapmasını göstermektedir.

3. Belirtilen 4 farklı kural kullanılarak BKA tipi belirlenir.

a. Eğer $m_r \le 5,831m_l - t_{\alpha,m-1}\frac{s_c}{\sqrt{m}}$, $m_r \le 0,171m_l + 8,29 - t_{\alpha,m-1}\frac{s_d}{\sqrt{m}}$ ve $m_r \ge m_r$ ise BKA tipi içsel tipdir.

b. Eğer $m_r > 5,831m_l - t_{\alpha,m-1}\frac{s_c}{\sqrt{m}}$ ve $m_r < 0,171m_l + 8,29 - t_{\alpha,m-1}\frac{s_d}{\sqrt{m}}$ ise BKA tipi sol omuz tip BKA'dır.

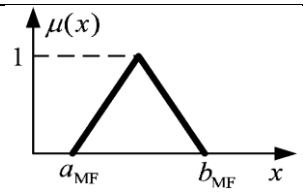
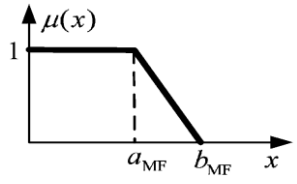
c. Eğer $m_r < 5,831m_l - t_{\alpha,m-1}\frac{s_c}{\sqrt{m}}$ ve $m_r > 0,171m_l + 8,29 - t_{\alpha,m-1}\frac{s_d}{\sqrt{m}}$ ise BKA tipi sağ omuz tip BKA'dır.

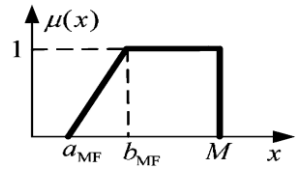
d. Eğer ilk 3 kural sağlanmamış ise herhangi bir BKA söz konusu değildir.

İlk üç kuralda verilen $t_{\alpha,m-1}$ istatistik de kullanılan Student-t dağılımı istatistiği olup α güven düzeyini *m*-1 serbestlik derecesini belirtmektedir.

4. Adım 3'de BKA tipi belirlendikten sonra herbir *m* aralıklı sayı $[a^{(i)}, b^{(i)}]$ Çizelge 'de verilen formüller yardımı ile ilgili parametreleri $\left\{a_{MF}^{(i)}, b_{MF}^{(i)}\right\}$ olan gömülü tip-1 BK'lere dönüştürülür.

Çizelge 3.3. BKA tipine göre m_{MF}, σ_{MF}, a_{MF}, ve b_{MF} değerleri

BKA Tipi	m_{MF} ve σ_{MF} değerleri	a_{MF} ve b_{MF} değerleri
 İçsel tip BKA	$m_{MF} = \frac{a_{MF} + b_{MF}}{2}$ $\sigma_{MF} = \frac{b_{MF} - a_{MF}}{2\sqrt{6}}$	$a_{MF} = \frac{a+b}{2} - \frac{b-a}{\sqrt{2}}$ $b_{MF} = \frac{a+b}{2} + \frac{b-a}{\sqrt{2}}$
 Sol omuz tipi BKA	$m_{MF} = \frac{2a_{MF} + b_{MF}}{3}$ $\sigma_{MF} = \frac{b_{MF} - a_{MF}}{3\sqrt{2}}$	$a_{MF} = \frac{a+b}{2} - \frac{b-a}{\sqrt{6}}$ $b_{MF} = \frac{a+b}{2} + \frac{\sqrt{6}(b-a)}{3}$

 Sağ omuz tipi BKA	$m_{MF} = \frac{a_{MF} + 2b_{MF}}{3}$ $\sigma_{MF} = \frac{b_{MF} - a_{MF}}{3\sqrt{2}}$	$a_{MF} = \frac{a+b}{2} - \frac{b-a}{\sqrt{2}}$ $b_{MF} = \frac{a+b}{2} + \frac{b-a}{\sqrt{2}}$

Adım 5. $b_{MF}^{(i)} > 10$ ve/veya $b_{MF}^{(i)} < a_{MF}^{(i)}$ olan gömülü tip-1 BK'ler elemine edilir. Bu adımdan sonra m adet olan gömülü tip-1 BK sayısı m^* adete indirgenir.

Adım 6. m^* adet gömülü tip-1 BK kullanılarak aralıklı tip-2 BK ve bu kümeye ait parametreler belirlenir. Eğer BKA tipi içsel BKA ise $\left\{\underline{a}_{MF}, \underline{b}_{MF}, \underline{c}_{MF}, \overline{a}_{MF}, \overline{b}_{MF}, \overline{c}_{MF}, \mu_p, p\right\}$ parametreleri, eğer BKA tipi sağ veya sol omuz tip BKA ise $\left\{\underline{a}_{MF}, \underline{b}_{MF}, \overline{a}_{MF}, \overline{b}_{MF}\right\}$ parametreleri hesaplanmalıdır. Bu parametreler Eş.3.66-3.72'de verilen eşitlikler yardım ile elde edilir.

$$\underline{a}_{MF} = \min_{i=1,\ldots,m^*} \left\{a_{MF}^{(i)}\right\} \tag{3.66}$$

$$\overline{a}_{MF} = \text{maks}_{i=1,\ldots,m^*} \left\{a_{MF}^{(i)}\right\} \tag{3.67}$$

$$\underline{b}_{MF} = \min_{i=1,\ldots,m^*} \left\{b_{MF}^{(i)}\right\} \tag{3.68}$$

$$\overline{b}_{MF} = \text{maks}_{i=1,\ldots,m^*} \left\{b_{MF}^{(i)}\right\} \tag{3.69}$$

$$c_{MF}^{(i)} = \frac{a_{MF}^{(i)} + b_{MF}^{(i)}}{2} \tag{3.70}$$

$$\underline{c}_{MF} = \min_{i=1,\ldots,m^*} \left\{c_{MF}^{(i)}\right\} \tag{3.71}$$

$$\overline{c}_{MF} = \text{maks}_{i=1,\ldots,m^*} \left\{c_{MF}^{(i)}\right\} \tag{3.72}$$

$\left(\mu_p, p\right)$ değerlerinin bulunması için ilk olarak tüm gömülü tip-1 BK'lerin sol ayakları ile sağ ayaklarının farklı kesişimleri alınır, daha sonra $\left[\overline{a}_{MF}, \underline{b}_{MF}\right]$ aralığında elde edilen kesişim değerlerinden en düşük yüksekliğe sahip kesişim değeri seçilir. Bu nokta p ve μ_p değerlerini verir.

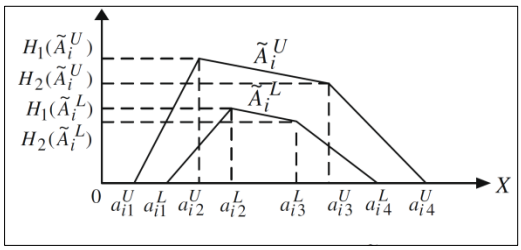
3.5.5. Aralıklı tip-2 kümelerin temel aritmetik işlemler

Bulanık maktık temelli aralıklı tip-2 kümelerde çalışmalar yapıldığında birbirine etki eden olayların toplam olasılıklarının hesaplanması gerekmektedir. Bu hesaplamalarda bir olasılığın diğeri ile çarpılması ve iki çarpımında toplanması gerekliği gibi çok sayıda aritmetik işlem gerekmektedir.

Bu aritmetik işlemlerin matematiksel tanımları aşağıda verilmiştir. Çok sayıda aritmetik işlem ihtmali bulunmaktadır ancak burada önerilen tekniğin ispatı için kullanılmak üzere gerektiği kadar artitmetik işlem açıklanmıştır.

Bulanık girdilerle yapılan bir aritmetik işlemin sonucu, yine bulanık olacaktır. Bir sonraki bölümde ise, bu bulanık işlemlerin durulaştırılması için gereken algoritmalar verilecektir.

X evrensel uzayda tanımlı bir aralıklı tip-2 küme $\tilde{\tilde{A}}_i = \left(\tilde{A}_i^U, \tilde{A}_i^L\right) = \left(\left(a_{i1}^U, a_{i2}^U, a_{i3}^U, a_{i4}^U; H_1\left(\tilde{A}_i^U\right), H_2\left(\tilde{A}_i^U\right)\right), \left(a_{i1}^L, a_{i2}^L, a_{i3}^L, a_{i4}^L; H_1\left(\tilde{A}_i^L\right), H_2\left(\tilde{A}_i^L\right)\right)\right)$ olarak verilmiş ve Şekil ’de gösterilmiştir. $\tilde{\tilde{A}}_i$ aralıklı tip-2 BK, alt ve üst gölümü tip-1 BK ile gösterilir.



Şekil 3.25. Aralıklı tip-2 bulanık küme olan $\tilde{A}_i$ nin, üst yamuk üyelik fonksiyonu $\tilde{A}_i^U$ ve alt yamuk üyelik fonksiyonu $\tilde{A}_i^L$

Şekil 3.25’de gösterilen $\tilde{\tilde{A}}_i$ aralılı tip-2 BK, $1 \le j \le 2$, $H_j\left(\tilde{A}_i^U\right) \in [0,1]$ ve $H_j\left(\tilde{A}_i^L\right) \in [0,1]$ şartlarını sağladığında $H_j\left(\tilde{A}_i^U\right)$, $a_{i(j+1)}^U$ elemanlarının üst gömülü tip-1 yamuk BK’sına ait üyelik üyelik derecesini, benzer şekilde $H_j\left(\tilde{A}_i^L\right)$ ifadesi de $a_{i(j+1)}^L$ elemanlarının alt gömülü tip-1 yamuk BK’sına ait üyelik derecesini göstermektedir.

$\tilde{\tilde{A}}_1$ ve $\tilde{\tilde{A}}_2$ iki farklı aralıklı tip-2 BK olsun.

$$\tilde{\tilde{A}}_1 = \left(\tilde{A}_1^U, \tilde{A}_1^L\right) = \left(\left(a_{11}^U, a_{12}^U, a_{13}^U, a_{14}^U; H_1\left(\tilde{A}_1^U\right), H_2\left(\tilde{A}_1^U\right)\right), \left(a_{11}^L, a_{12}^L, a_{13}^L, a_{14}^L; H_1\left(\tilde{A}_1^L\right), H_2\left(\tilde{A}_1^L\right)\right)\right)$$

$$\tilde{\tilde{A}}_2 = \left(\tilde{A}_2^U, \tilde{A}_2^L\right) = \left(\left(a_{21}^U, a_{22}^U, a_{23}^U, a_{24}^U; H_1\left(\tilde{A}_2^U\right), H_2\left(\tilde{A}_2^U\right)\right), \left(a_{21}^L, a_{22}^L, a_{23}^L, a_{24}^L; H_1\left(\tilde{A}_2^L\right), H_2\left(\tilde{A}_2^L\right)\right)\right)$$

Bu iki küme üzerinde toplama, çıkarma ve çarpma aritmetik işlemleri Eş. 3.73-3.75'te tanımlanmıştır.

$$\tilde{\tilde{A}}_1 + \tilde{\tilde{A}}_2 = \left(\tilde{A}_1^U, \tilde{A}_1^L\right) + \left(\tilde{A}_2^U, \tilde{A}_2^L\right) =$$
$$\left(\begin{array}{l}\left(a_{11}^U + a_{21}^U, a_{12}^U + a_{22}^U, a_{13}^U + a_{23}^U, a_{14}^U + a_{24}^U; \min\left(H_1\left(\tilde{A}_1^U\right), H_1\left(\tilde{A}_2^U\right)\right), \min\left(H_2\left(\tilde{A}_1^U\right), H_2\left(\tilde{A}_2^U\right)\right)\right), \\ \left(a_{11}^L + a_{21}^L, a_{12}^L + a_{22}^L, a_{13}^L + a_{23}^L, a_{14}^L + a_{24}^L; \min\left(H_1\left(\tilde{A}_1^L\right), H_1\left(\tilde{A}_2^L\right)\right), \min\left(H_2\left(\tilde{A}_1^L\right), H_2\left(\tilde{A}_2^L\right)\right)\right)\end{array}\right) \quad (3.73)$$

$$\tilde{\tilde{A}}_1 - \tilde{\tilde{A}}_2 = \left(\tilde{A}_1^U, \tilde{A}_1^L\right) - \left(\tilde{A}_2^U, \tilde{A}_2^L\right) =$$
$$\left(\begin{array}{l}\left(a_{11}^U - a_{21}^U, a_{12}^U - a_{22}^U, a_{13}^U - a_{23}^U, a_{14}^U - a_{24}^U; \min\left(H_1\left(\tilde{A}_1^U\right), H_1\left(\tilde{A}_2^U\right)\right), \min\left(H_2\left(\tilde{A}_1^U\right), H_2\left(\tilde{A}_2^U\right)\right)\right), \\ \left(a_{11}^L - a_{21}^L, a_{12}^L - a_{22}^L, a_{13}^L - a_{23}^L, a_{14}^L - a_{24}^L; \min\left(H_1\left(\tilde{A}_1^L\right), H_1\left(\tilde{A}_2^L\right)\right), \min\left(H_2\left(\tilde{A}_1^L\right), H_2\left(\tilde{A}_2^L\right)\right)\right)\end{array}\right) \quad (3.74)$$

$$\tilde{\tilde{A}}_1 x \tilde{\tilde{A}}_2 = \left(\tilde{A}_1^U, \tilde{A}_1^L\right) x \left(\tilde{A}_2^U, \tilde{A}_2^L\right) =$$
$$\left(\begin{array}{l}\left(a_{11}^U \times a_{21}^U, a_{12}^U \times a_{22}^U, a_{13}^U \times a_{23}^U, a_{14}^U \times a_{24}^U; \min\left(H_1\left(\tilde{A}_1^U\right), H_1\left(\tilde{A}_2^U\right)\right), \min\left(H_2\left(\tilde{A}_1^U\right), H_2\left(\tilde{A}_2^U\right)\right)\right), \\ \left(a_{11}^L \times a_{21}^L, a_{12}^L \times a_{22}^L, a_{13}^L \times a_{23}^L, a_{14}^L \times a_{24}^L; \min\left(H_1\left(\tilde{A}_1^L\right), H_1\left(\tilde{A}_2^L\right)\right), \min\left(H_2\left(\tilde{A}_1^L\right), H_2\left(\tilde{A}_2^L\right)\right)\right)\end{array}\right) \quad (3.75)$$

Bölme işlemi bu doktora tezindeki matematiksel işlemlerde kullanılmayacağından ele alınmamıştır.

3.5.6. Gelişmiş Karnik-Mendel algoritmaları

Çalışmanın en önemli bölümlerinden birisi de bulanıklaştırılmış veri setlerinin ve küme üyelik derecelerinin, durulaştırılmasıdır. Bilinen birkaç durulaştırma yöntemi mevcuttur ancak bu tezde en yaygın ve gelişmiş yöntem olan gelişmiş Karnik-Mendel algoritmaları (GKMA) kullanılacaktır.

Sağ ve sol değerlerini antek yolu ile topladıktan sonra veritabanımıza kaydedebilir ve operatörleri kullanarak bu değerleri durulaştırılabilir.

Sol değerlerimiz (minimumlar) = y_l

Sağ değerlerimiz (maksimumlar) = y_r olsun;

y_l için GKMA hesaplaması aşağıdaki prosedürlere göre yapılır:

1- $\underline{x}_i \left(x = 1, 2, ..., N\right)$ artan bir dizi olarak sıralanır. Sıralanmış $\underline{x}_i$ değerlerini değiştirmeden aynı isimle adlandırılmaya devam edilir (sıralı değerler $\underline{x}_1 \le \underline{x}_2 \le ... \le \underline{x}_N$). Her bir ağırlık (w_i) değerlerine karşılık gelen (x_i) değerleri eşleştirilir ve ilgili indeks numaralarını x_i ile aynı olacak şekilde düzenlenir.

2-k değeri en yakın tam sayı N değerine $k = \left[N / 2.4\right]$ sağlayacak şekilde hesaplanır ve Eş.3.76-3.78 kullanılarak a, b ve y değerleri bulunur:

$$a = \sum_{i=1}^{k} \underline{x}_i \overline{w}_i + \sum_{i=k+1}^{N} \underline{x}_i \underline{w}_i \tag{3.76}$$

$$b = \sum_{i=1}^{k} \overline{w}_i + \sum_{i=k+1}^{N} \underline{w}_i \tag{3.77}$$

$$y = \frac{a}{b} \tag{3.78}$$

3- $\underline{x}_{k'} \le y \le \underline{x}_{k'+1}$ $k' \in \left[1, N-1\right]$ sağlayan k' değerleri bulunur.

4- $k' = k$ durumu kontrol edilir, eğer eşitse algoritma durdurulur ve y_1 değeri y değerine eşitle ve devam et, k değerini artık L olarak adlandır. $k' \neq k$ ise devam edilir.

5- s değerini $s = sign(k' - k)$ kullanılarak bulunur ve a', b' ve y' değerleri Eş.3.79-3.80 yardımı ile hesaplanır.

$$a' = a + s \sum_{i=\min(k,k')+1}^{\max(k,k')} \underline{x}_i \left(\overline{w}_i - \underline{w}_i\right) \tag{3.79}$$

$$b' = b + s \sum_{i=\min(k,k')+1}^{\max(k,k')} \underline{x}_i \left(\overline{w}_i - \underline{w}_i \right) \tag{3.80}$$

$$y' = \frac{a'}{b'} \tag{3.81}$$

6- y değeri y' değerine eşitlenir $\left(y = y' \right)$. Benzer şekilde; $a = a', b = b', k = k'$ eşitlemeleri yapılır ve 3. Adıma tekrar geri dönülür.

y_r için GKMA hesaplaması aşağıdaki prosedürlere göre yapılır:

1- $\underline{x}_i \left(x = 1, 2, ..., N \right)$ artan olarak sıralanır. Sıralanmış $\underline{x}_i$ değerlerini değiştirmeden aynı isimle adlandırmaya devam edilir (sıralı değerler $\underline{x}_1 \le \underline{x}_2 \le ... \le \underline{x}_N$). Her bir ağırlık ($w_i$) değerlerine karşılık gelen (x_i) değerlerini eşleştir ve ilgili indeks numaralarını x_i ile aynı olacak şekilde düzenlenir. $k' > k$ olduğu durumda Eş.3.82-3.83 doğru olacaktır:

$$a' = a + s \sum_{i=k+1}^{k'} \underline{x}_i (\overline{w}_i - \underline{w}_i) \tag{3.82}$$

$$b' = b + s \sum_{i=k+1}^{k'} (\overline{w}_i - \underline{w}_i) \tag{3.83}$$

$k > k'$ olduğu durumda Eş.3.84-3.85 doğru olacaktır:

$$a' = a + s \sum_{i=k'+1}^{k} \underline{x}_i (\overline{w}_i - \underline{w}_i) \tag{3.84}$$

$$b' = b + s \sum_{i=k'+1}^{k} (\overline{w}_i - \underline{w}_i) \tag{3.85}$$

2-k değerini en yakın tam sayı N değerine $k = \left[N / 1.7 \right]$ sağlayacak şekilde eşleştir ve Eş.3.86-3.87 kullanılarak a, b ve y değerleri hesaplanır:

$$a = \sum_{i=1}^{k} \overline{x}_i \underline{w}_i + \sum_{i=k+1}^{N} \overline{x}_i \overline{w}_i \tag{3.86}$$

$$b = \sum_{i=1}^{k} \underline{w}_i + \sum_{i=k+1}^{N} \overline{w}_i \tag{3.87}$$

$$y = \frac{a}{b} \tag{3.88}$$

3- $\overline{x}_{k'} \le y \le \overline{x}_{k'+1}$ $k' \in [1, N-1]$ sağlayan k' değerleri bulunur.

4- $k' = k$ durumu kontrol edilir, eğer eşitse algoritma durdurulur ve y_r değeri y değerine eşitlenir ve devam edilir, k değeri artık R olarak adlandır. $k' \neq k$ ise algoritma devam eder.

5- s değeri $s = sign(k' - k)$ formülü yardımı ile bulunur ve a', b' ve y' değerleri Eş.3.89-3.90 yardımı ile hesaplanır.

$$a' = a - s \sum_{i=\min(k,k')+1}^{\max(k,k')} \overline{x}_i \left(\overline{w}_i - \underline{w}_i \right) \tag{3.89}$$

$$b' = b - s \sum_{i=\min(k,k')+1}^{\max(k,k')} \left(\overline{w}_i - \underline{w}_i \right) \tag{3.90}$$

$$y' = \frac{a'}{b'} \tag{3.91}$$

6- y değerini y' değerine eşitle $(y = y')$ Benzer şekilde; $a = a', b = b', k = k'$ eşitlenir ve 3. Adıma tekrar geri dönülür.

Böylece döngü tüm elemanlar için çevirildikten sonra ilgili veritabanı için durulaştırılmış değerlerin elde edilmesi beklenebilir.

4. ARALIKLI TİP-2 BULANIK CORAS TEKNİĞİ

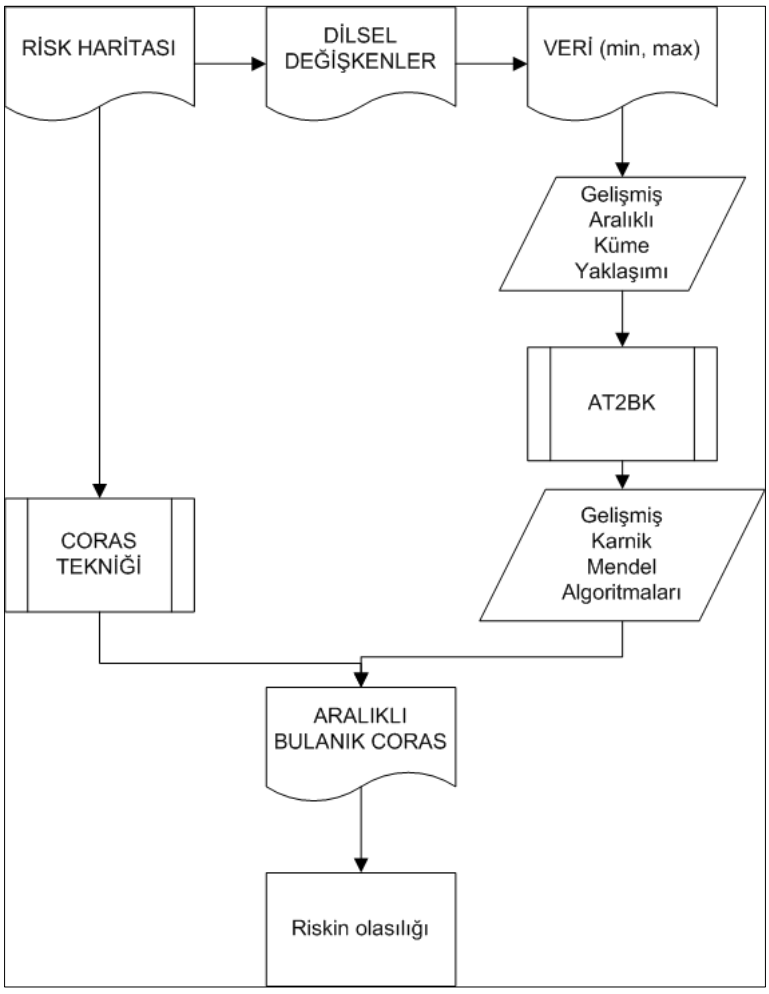
Bulanık Mantığın CORAS tekniği ile kullanıldığı tek çalışma, Tran tarafından 2017 yılında yapılan yüksek lisans tezidir. Bu doktora tezinin hazırlandığı sıralarda yayınlanan tezin sahibi Tran bu çalışmayı, Stolen'in çıktılarını doğrulamak ve yorumsuz olarak bir karşılaştırma yapmak için çalıştığını ifade etmiştir. Ayrıca tip-2 ve aralıklı küme yaklaşımı yerine Tip-1 bulanık kümeler ile yöntemini ispatlamaya çalışmıştır. Sonuç olarak bu tezin konusu ile doğrudan bir bağı bulunmadığı anlaşılmıştır. Ayrıca Tran, çalışmasında yönteme odaklandığı için, yine sentetik verilerle çalışmış ve herhangi bir sonuç yayınlamadan, değerlendirmeyi okuyucuya bırakmıştır. Tran çalışmasında kelime değerlerine karşılık gelen tip-1 bulanık küme üyelerini bulanıklaştırıp, önerdiği yöntemden sonra iki ayrı deneyde durulaştırarak Stolen'in kitabındaki kelimesel aralıkları doğrulamaya çalışmıştır. Ancak hangi yöntemin doğru ve daha hassas olduğu yönünde geribildirim verilmemiştir. Bu bakımdan yöntemin geçerliliği konusunda gerçek verilerle test edilmesi gereklidir (Tran, 2017)

Beckers ve arkadaşları yaptıkları bir çalışmada ISO 27001 bilgi yönetim sistemini, CORAS tekniği ile karşılaştırıp uyumlu hale getirmişlerdir (Beckers ve arkadaşları 2014).Özellikle bilgi yönetim sisteminin aşamalarından olan, içeriği belirleme, riskleri tanımlama ve riskleri yönetme safhaları için CORAS tekniği ile entegrasyonu ve uyumluluğu öngörmüşlerdir.

Bölüm 3'te özetlendiği gibi, CORAS tekniği şekilsel olarak siber risklerin birbirlerini olan etkilerini haritalamak ve aralarındaki ilişkiyi özetlemek için kullanılmıştır. Her bir olasılığın, ister gerçek dünyadan toplansın, ister araştırma yöntemleri ile toplansın, belli bir minimum ve maksimun değeri olduğu varsayılmıştır. Bu minimum ve maksimum değerli, her bir adım için bilinmeyen bulanık değerleri üretecektir. Ancak aynı değer için belli sayıda deneğe sorular sorulduğunda karşımıza bir dağılım çıkacaktır. Bu dağılım en genel hali ile bir "Gaus Dağılımı"dır. Daha sonra ististiksel yöntemlerle ve bölüm 3 te bahsedilen aritmetik işlemler yapılarak, oluşturulan tüm risk haritasının sonundaki istenmeyen olayın oluşma ihtimali yüzdesel olarak bulunabilir.

Aralıklı Tip-2 Bulanık Coras tekniği, CORAS haritalarından miras olarak aldığı risk ilişkilerini, aralıklı girdiler ile önce bulanık kümelerin oluşturuldu ve sonra aritmetik

işlemlerin yapıldığı, nihayet durulaştırma ile net ihtimal değerlerinin hesaplandığı bir yöntemolarak bu çalışmada önerilmiştir. Şekil 4.2' de görüldüğü gibi,



Şekil 4.1. Aralıklı tip-2 bulanık CORAS tekniğinin oluşturulması

Ancak bulduğumuz küme hala bulanık verilerden oluşan bir küme olacaktır ve grafiği çizildiğinde bir BKA oluşturacaktır. BKA gelişmiş karnik mendel algoritmaları ile durulaştırıldığında bu alanı işaret eden tek bir değere, yani "merkez" (centroid) değerine ulaşılacaktır.

En genel hali ile tekniğin kullanılmasındaki adımlar Şekil 'deki gibi kısaca;

1- İstenmeyen olayın tespit edilmesi
2- İstenmeyen sonuç olarak doğuracak geriye doğru tüm olayların birbiri üzerlerindeki etkilerinin şematik olarak gösterilmesi (CORAS Tekniği ile geliştirilen CORAS aracını kullanılacaktır).

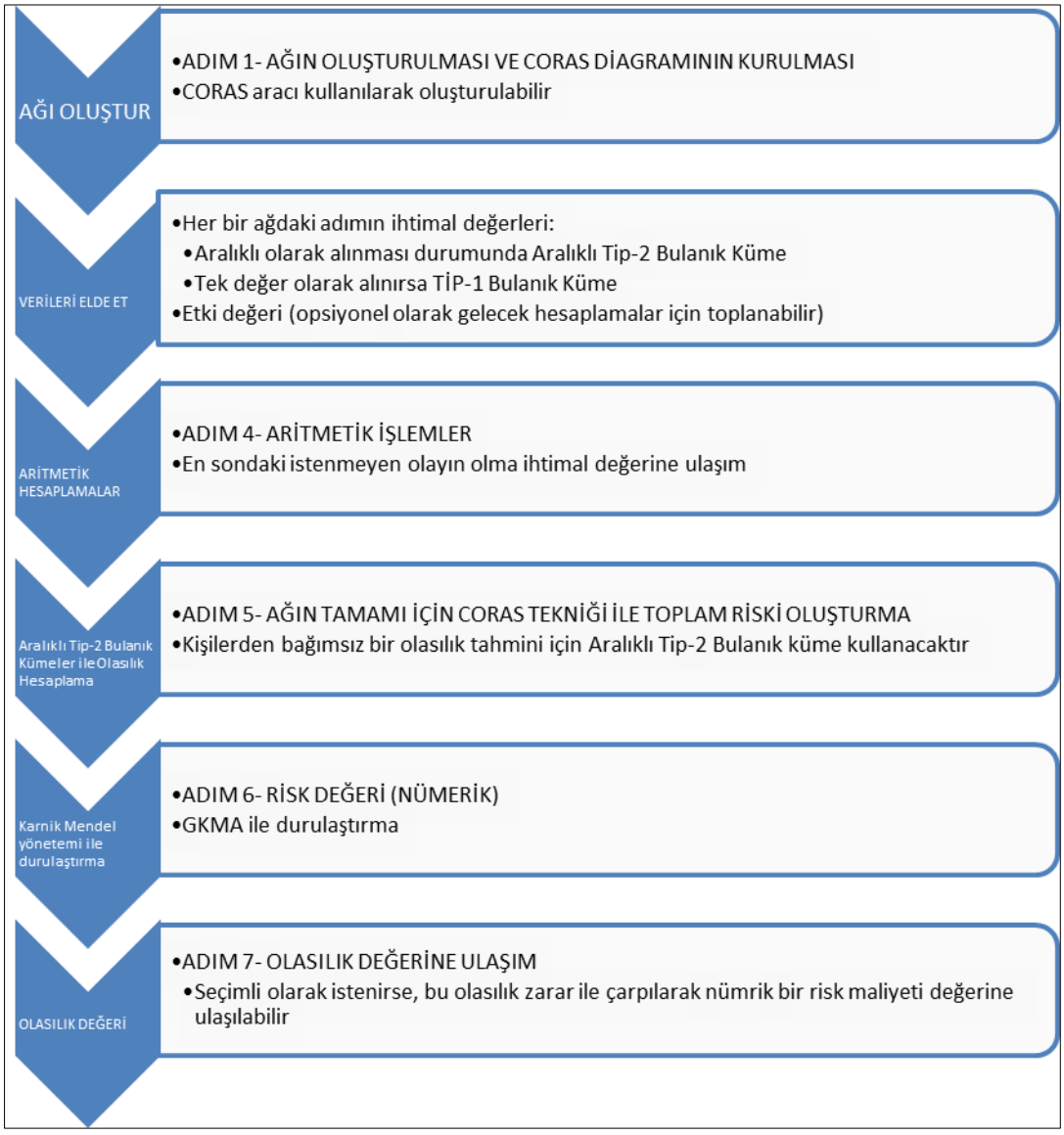
3- Her bir olay ve bu olay olduğunda sonraki oluşacak olayın anotasyonla gösterilmesi

a. A olayı, A olayı olduğunda X olayı oluyorsa, A olayı olduğunda X olayının olma olasılığı A1 şeklinde yazılabilir.

4- İlgili Matlab kütüphanelerindeki toplama ve çarpım formülleri bu haritaya göre güncellenmeli ve nihai sonuçlar elde edilmedir.

5- Sonuç olarak bir grafik ekranda tüm bu BKA'ler her adım için ayrı ayrı gösterilebilir.

6- Tamamını ifade eden bulanık küme, Gelişmiş Karnik Mendel algoritmalarının ilgili kütüphaneleri çalıştırılarak durulaştırma işlemi yapılır, merkez (centroid) değeri bulur.



Şekil 4.2. Aralıklı tip-2 bulanık CORAS çalışma akışı

5. DENEYSEL ÇALIŞMA VE TARTIŞMA

Bu tezin ana amacı, küme teorisi, siber güvenlik risk yönetimi, mantık teorisi ve CORAS yöntemlerini kullanarak, akıllı araçlar için, belirsiz riskleri belirli hale getirecek bir teknik önermektir. Bu maksatla şekilsel ve ilişkisel bir risk değerlendirme yöntemi olan CORAS tekniğini, akıllı araçlar için kurgulayıp, sonrasında toplam olasılık oranlarını bulmaktır. Bunu yaparken, konunun uzmanlarından, anket çalışması ile elde ettiğimiz bulanık olasılıkları, yukarıda bahsedilen yöntemlerle önce bulanık kümelere dönüştürülecektir. Daha sonra risk haritasından kaynaklanan aritmetik işlemler bölüm 3'te gösterildiği gibi uygulanacaktır. Ardından elde ettiğimiz bulanık aralıklı tip-2 kümeleri, durulaştırma yaparak net bir risk değerine ulaşılması hedeflenmektedir. Aritmetik işlemler neticesinde eğer, bulanık küme oluşmuyorsa, bu durumda bulanıklığın ayak izi olmadığı anlamına geliyor ki bu da anket sonucunda alınan değerlerin kendi içlerinde ve birbirlerine karşı ilgili olmadığı, yani aralıklı tip-2 bulanık küme uluşturamadığı anlamına gelecektir. Bir başka ifade ile, bu bilgilerin tutarsız olduğu ve değerlendirmeye alınmaması gerektiği anlaşılacaktır. Eğer BKA oluşursa, gerçekten bir belirsizliğin varolduğu ve bu belirsizliğin neticesinde yapılan işlemler sonucunda net bir alan oluşacak, yani durulaştırma sonrası nümerik risk değeri gerçeğe yakın bir sonuçla elde edilmesi beklenmektedir.

Uygulamanın adımları

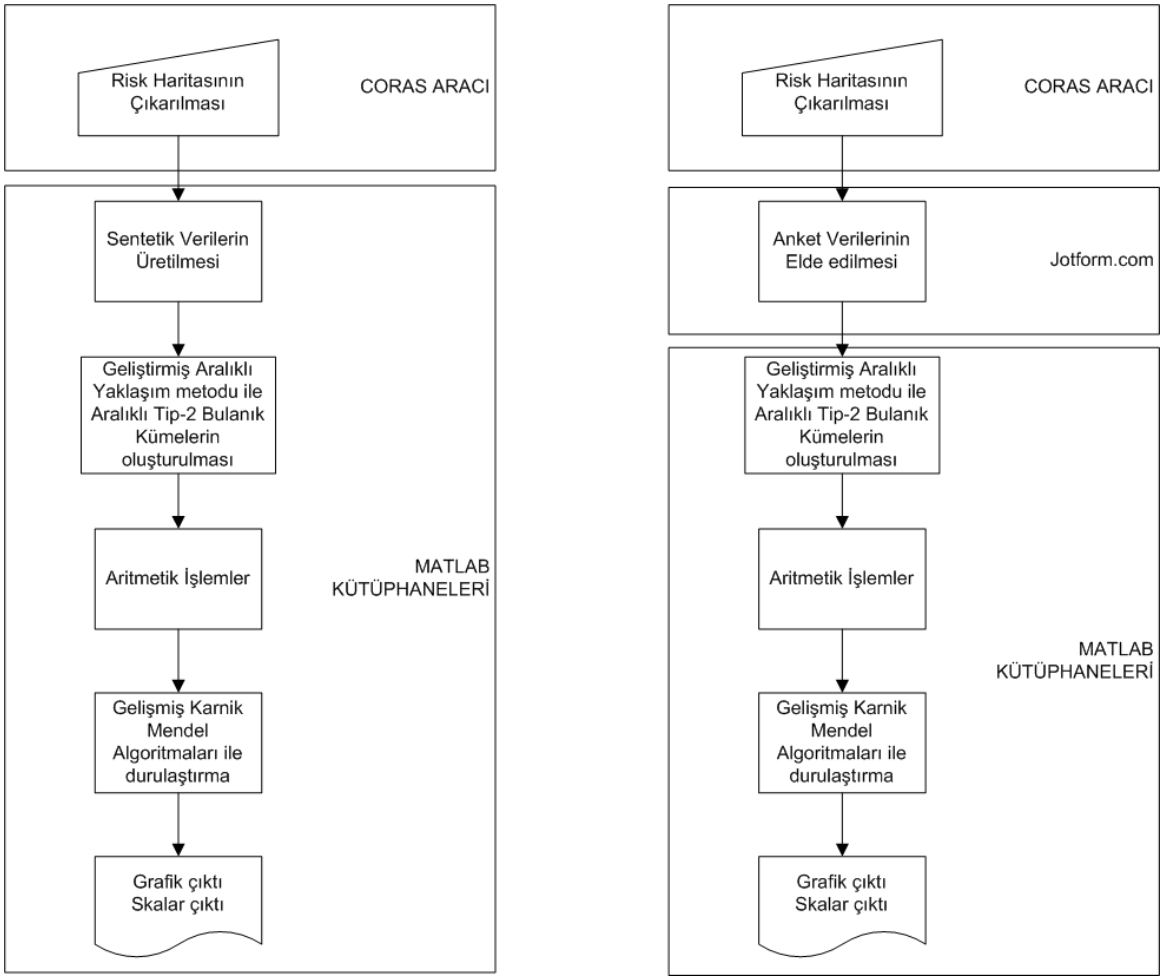
Jotform.com portalı aracılığı ile EK1'deki soru seti, EK2'de listesi bulunan konu uzmanlarına sorulmuştur. % ihtimal değerleri olarak alt ve üst limitleri söz konusu sorudaki olay için istenmiştir. Tüm denekler girildiğinde, gelişmiş aralıklı yaklaşım ve Karnik Mendel algoritmalarının matlab kütüphanelerine uygulanmış sonucunda;

a- Tüm sorular için bulanık kümeler
b- Tüm hayati kayıpla sonuçlanan siber riskler bulanık küme olarak
c- Tüm konfor kaybına sebep olan siber riskler bulanık küme olarak
d- Tüm hayati kayıpla sonuçlanan siber riskler durulaştırılmış nümerik bir rakam olarak muhtemel olasılığı
e- Tüm konfor kaybına sebep olan siber riskler durulaştırılmış nümerik bir rakam olarak muhtemel olasılıkları

elde edilmiş olunacaktır.

5.1. Uygulama Altyapısı

Uygulama altyapısı sentetik veri ve gerçek saha verilerinin kullanımı aşağıdaki şekilde şematik olarak özetlenmiştir.



Şekil 5.1. Araştırma altyapısının, sentetik veri ve saha verisi için özeti

5.2. Uygulama A: Sentetik Verilerle Yöntemin Test Edilmesi

Bu tekniğin birleştirilmesi için önce sentetik rakamlarla oluşturulan bir veritabanından denemeler yapılmıştır. Oluşturulacak CORAS risk haritasına göre her adımdaki olması ihtimal olayın bir maksimum birde minimum değeri anket yolu ile toplanmıştır. Teorinin kolayca anlatımı ve modelin gösterimi amaçlanmıştır.

Bunun için izlenen adımlar aşağıdaki şekildedir;
1.adım –CORAS tekniği kullanılarak araçlardaki ölümle sonuçlanabilecek kazayı doğuran risklerin olasılık haritası çıkarıldı.

2.adım- Bu risk haritasındaki Bulanık Kümelerde "kelime" anlamına gelen anotasyonlar yapılmıştır (A,B,A1,B1,…).

3.adım- Bir anket setine, matlab içerisindeki rastgele sayı üretecinde kullanılmak üzere 1 anket cevabı yazar tarafından verilmiştir. Burada her soru için minimum ve maksimum değerlerin girilmesi sağlanmıştır. Böylece girdi olarak bulanık ve ikinci derece aralıklı kümeler elde edilmiştir. Zadeh'nin önerdiği yöntemlerin kullanılabilmesi için, 2. Derece ÜF=1 varsayılmıştır.

4.adım- Matlab fonksiyonu kullanılarak bu randomize tek satır cevaplardan 30 set (satır)
İlgili Matlab rastgele sayı üreteç kodu için, şu kısa kod parçası kullanılmıştır;

```
function  [aralikli_sayi]=aralikli_sayi_ureteci(a,b,c)
for i=1:c
r = (b-a).*rand(100000,1) + a;
rassal_sayi=randi([1,100000],2,1);
r=r(rassal_sayi,1);
aralikli_sayi(i,:) = [min(r) max(r)];
end
end
```

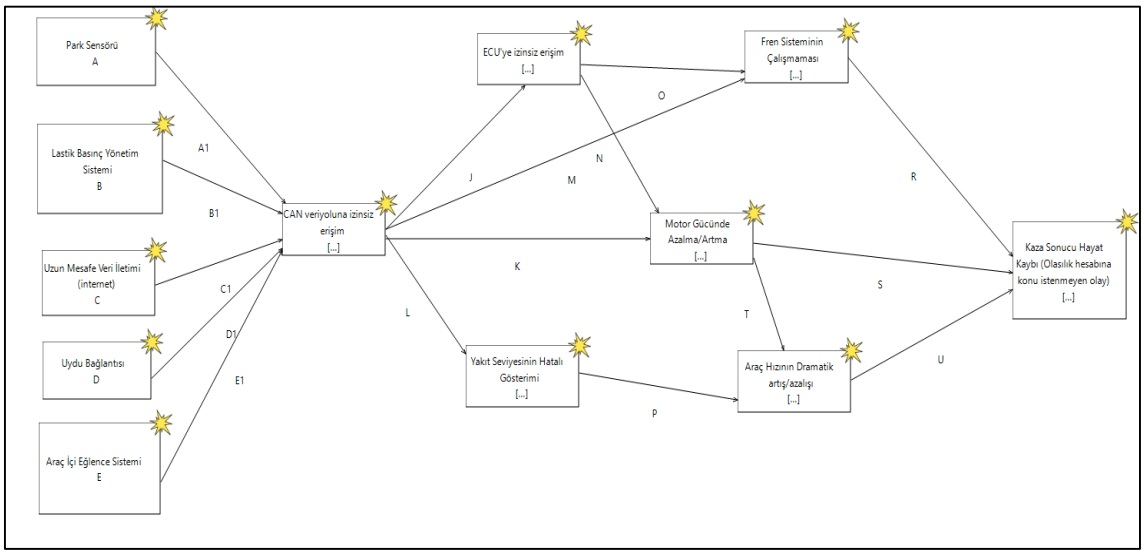
toplam 30 denek olduğu varsayıldı, 30 sıra minimum ve maksimum değeleri ilgili risk haritası için, EK-3'teki sentetik veri tabanı türetilmiştir.

5.adım- Matlab kütüphanesinde ilgili veri tabanı excel olarak okutulup ve çalıştırılmıştır.

Sonuç olarak her bir olasılık için aşağıdaki bulanık kümeler birer birer ve en son da da durulaştırılmış merkezi değere (centroid) ulaşılmıştır.

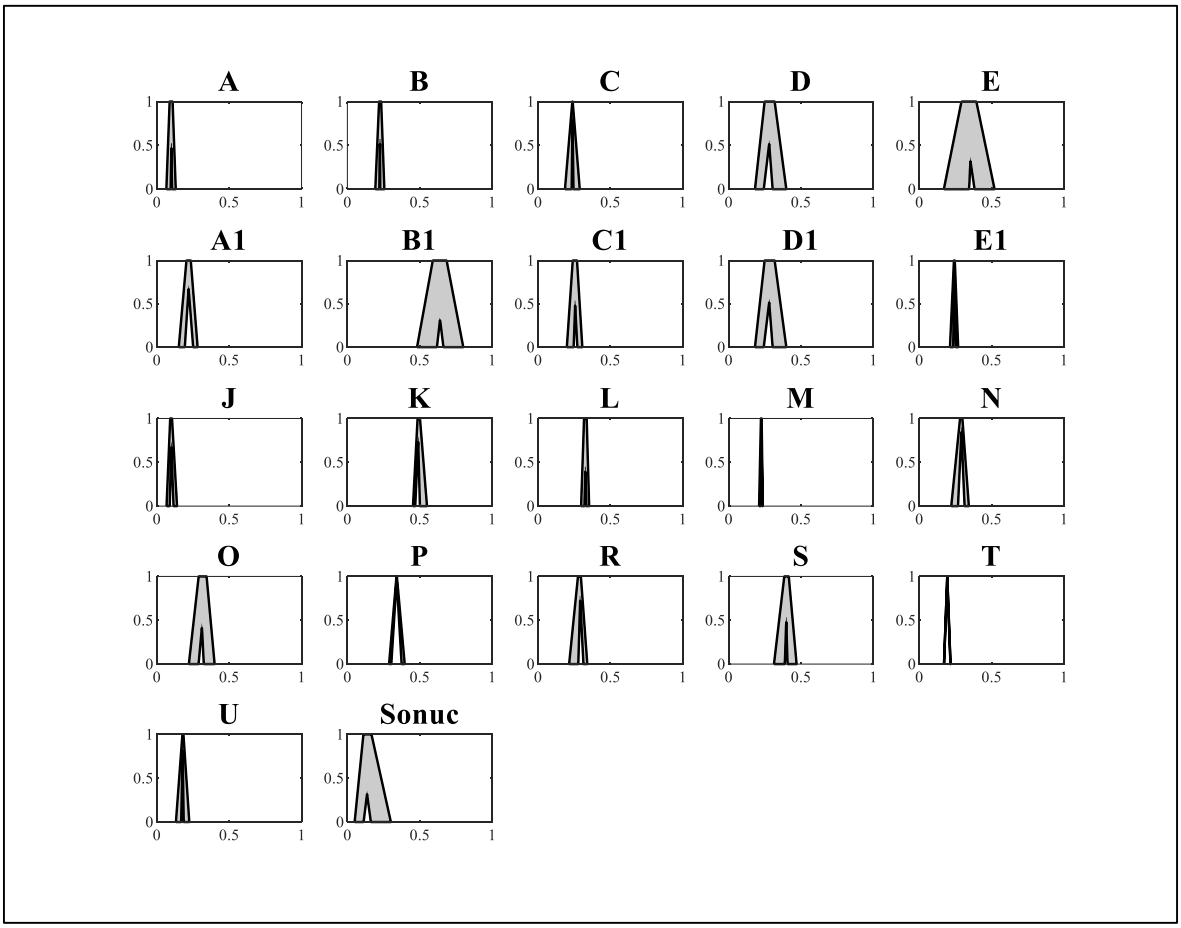
1.Adımda bahsedilen Aralıklı tip-2 bulanık kümeler ile örnek CORAS diyagramının çalıştırılması;

Bir akıllı araçtaki istenmeyen olay “Hayat Kaybı” olduğu varsayılmıştır. Bu istenmeyen olaya etki eden siber atakların birbirlerini etkileyecek şekilde ilişki ağı, CORAS aracı ile aşağıdaki şekilde hazırlanmış ve Şekil 5.2’ de gösterilmiştir.



Şekil 5.2. Hayat kaybı ile sonuçlanan siber atakların CORAS risk analiz haritası

Şekil 5.2’deki ilişki ihtimal ağı ve sonucunda yapılan hesaplamalar Şekil 5.3’deki BKA sonuçlarını ayrı ayrı her bir dilsel değişken ve sonuç değeri için göstermiştir.



Şekil 5.3. Sentetik veri tabanının ilgili matlab aralıklı tip-2 bulanık CORAS yöntemi ile analiz edilmesi ve sonuç değeri

Hesaplama için gereken yalancı kodlar aşağıdaki şekilde ifade edilebilir;

$$[AA] = A \times A1$$

$$[BB] = B \times B1$$

$$[CC] = C \times C1$$

$$[DD] = D \times D1$$

$$[EE] = E \times E1$$

$$[CAN] = [AA] + [BB] + [CC] + [DD] + [EE]$$

$$[ECU] = [CAN] \times J$$

$$[Mul\_brake] = [CAN] \times M + [ECU] \times O$$

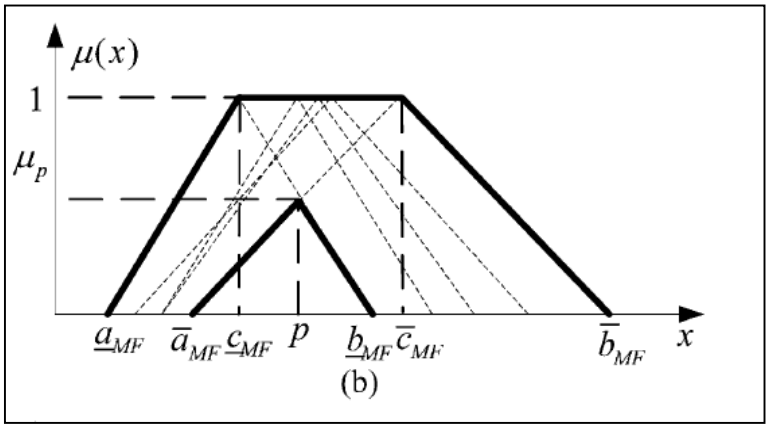
$$[Los\_Eng] = [CAN] \times K + [ECU] \times N$$

$$[Inc\_fuel] = [CAN] \times L$$

$$[Dec\_speed] = [Inc\_fuel] \times P + [Loss\_Eng] \times T$$

$$[sonuc] = [Mul\_brake] \times R + [Loss\_Eng] \times S + [Dec\_speed] \times U$$

Şekil 3.25-b'den hatırlanacak olursa; dışsal bulanık küme (Yamuk) ve gömülü bulanık küme arasında kalan BKA koordinatlarının (Şekil 5.4), x eksenini kestiği koordinatları matlab kütüphanesi çıktıları ile aşağıdaki şekilde gösterilebilir.



Şekil 5.4. Aralıklı tip-2 bulanık kümenin x ekseni değerleri ve üyelik fonksiyonları

Bulanıklığın ayak izi ve bu izi oluşturan değerlerin tüm kelimeler için değerleri Çizelge 5.1'de verilmiştir.

Çizelge 5.1. Konfor kaybı risk haritası için, sentetik olarak üretilen verilerin, tüm kelimelerin BKA koordinat değerleri

x Eks.	A	A1	AA	B	B1	BB	C	C1	CC	CAN	D
$\underline{a}_{MF}$	0,07	0,15	0,01	0,19	0,48	0,09	0,19	0,20	0,04	0,21	0,18
$\underline{c}_{MF}$	0,09	0,20	0,02	0,22	0,59	0,13	0,24	0,24	0,06	0,34	0,25
$\overline{c}_{MF}$	0,11	0,23	0,03	0,23	0,69	0,16	0,24	0,27	0,06	0,45	0,32
$\overline{b}_{MF}$	0,13	0,28	0,04	0,26	0,80	0,20	0,29	0,31	0,09	0,63	0,40
$\overline{a}_{MF}$	0,10	0,19	0,02	0,22	0,62	0,14	0,23	0,25	0,06	0,35	0,24
p	0,10	0,22	0,02	0,23	0,64	0,14	0,24	0,26	0,06	0,39	0,28
p	0,10	0,22	0,02	0,23	0,64	0,14	0,24	0,26	0,06	0,39	0,28
$\underline{b}_{MF}$	0,11	0,25	0,03	0,23	0,66	0,15	0,24	0,27	0,07	0,43	0,30
BKA	0,47	0,68	0,47	0,54	0,32	0,32	0,84	0,48	0,48	0,32	0,52

x Eks.	D1	DD	Dec_Speed	E	E1	ECU	EE	Inc_Fuel	J	K	L
$\underline{a}_{MF}$	0,18	0,03	0,03	0,17	0,21	0,01	0,04	0,06	0,07	0,45	0,30
$\underline{c}_{MF}$	0,25	0,06	0,07	0,29	0,24	0,03	0,07	0,11	0,09	0,48	0,32
$\overline{c}_{MF}$	0,32	0,10	0,10	0,39	0,25	0,05	0,10	0,15	0,11	0,50	0,34
$\overline{b}_{MF}$	0,40	0,16	0,17	0,52	0,27	0,09	0,14	0,22	0,14	0,55	0,35
$\overline{a}_{MF}$	0,24	0,06	0,06	0,35	0,23	0,03	0,08	0,11	0,09	0,47	0,32
p	0,28	0,08	0,08	0,35	0,24	0,04	0,09	0,13	0,10	0,49	0,33
p	0,28	0,08	0,08	0,35	0,24	0,04	0,09	0,13	0,10	0,49	0,33
$\underline{b}_{MF}$	0,30	0,09	0,10	0,38	0,25	0,05	0,10	0,14	0,12	0,50	0,33
BKA	0,52	0,52	0,32	0,33	0,88	0,32	0,33	0,32	0,68	0,74	0,40

x Eks.	Loss_Eng	M	Mul_breake	N	O	P	R	S	T	U	Sonuc
$\underline{a}_{MF}$	0,10	0,21	0,05	0,22	0,22	0,29	0,31	0,31	0,17	0,13	0,05
$\underline{c}_{MF}$	0,17	0,22	0,08	0,28	0,29	0,34	0,38	0,38	0,19	0,18	0,11
$\overline{c}_{MF}$	0,24	0,23	0,12	0,30	0,34	0,34	0,42	0,42	0,19	0,18	0,17
$\overline{b}_{MF}$	0,38	0,24	0,18	0,34	0,40	0,40	0,47	0,47	0,22	0,22	0,30
$\overline{a}_{MF}$	0,17	0,22	0,09	0,27	0,29	0,30	0,39	0,39	0,17	0,17	0,11
p	0,20	0,23	0,10	0,29	0,31	0,34	0,40	0,40	0,19	0,18	0,14
p	0,20	0,23	0,10	0,29	0,31	0,34	0,40	0,40	0,19	0,18	0,14
$\underline{b}_{MF}$	0,23	0,23	0,12	0,31	0,32	0,37	0,41	0,41	0,22	0,19	0,16
BKA	0,32	0,75	0,32	0,85	0,42	0,97	0,50	0,50	1,00	0,82	0,32

Burada hemen fark edilecek olursa, p değeri iki yazılmış gibi görünmektedir. Aslında yine bir yamuk olan gömülü bulanık kümenin 2. ve 3. değerleri birbirine eşit olduğu için, her iki p değeri bir biri üstüne çakışır ve bir üçgen oluşturmaktadır.

BKA ise tüm bu bulanık kümelerin ayrı ayrı ve sonuç değeri için durulaştırılmış ihtimal değerini vermektedir. Tüm BKA'ların durulaştırılarak elde edilen değere "Merkez" (Centroid) denir.

Bu adımdansonra merkezi değeri (Centroid) hesaplanabilir. Sonuç olarak elde edilen merkezi değer; 0.1587'dir. Bu durumda % 15,87 oranında hayat kaybı ile sonuçlanacak siber atağa maruz kalma olasılığı var denilmektedir. Bir başka ifadeyle her 100 ataktan yaklaşık 16 tanesi hayat kaybı ile sonuçlanabilecek olaylar zincirini tetiklemektedir denilebilir.

Gelecek bölümde bu konuda daha gerçekçi bir çalışmaya ulaşabilmek ve akademiye katkı sağlamak amacıyla, konunun uzmanlarından oluşan bir topluluğa iki ayrı olasılık haritası için, sorular sorularak bir araştırma anteki yapılmış (EK-1 ve EK-2) ve aynı teknik denenerek gerçeklenmeye çalışılmıştır.

5.3. Uygulama B: Anket Verileri Ile Elde Edilen Verilerin Değerlendirilmesi

Kısaca deney akışı ve izlenmesi gereken adımlar aşağıdaki şekilde gösterilmiştir;
1.adım –CORAS tekniği kullanılarak araçlardaki ölümle sonuçlanabilecek kazayı doğuran risklerin olasılık haritası çıkarılmıştır.

2.adım- Bu risk haritasındaki Bulanık Kümelerde "kelime" anlamına gelen dilsel değişkenler anotasyonlar yapıldı (A, B, A1, B1, …).

3.adım- Anketle konu uzmanlarından toplanan verilen veritabanı olarka gösterildi. Burada her soru için minimum ve maksimum değerlerin girilmesi sağlandı. Böylece girdi olarak bulanık ve ikinci derece aralıklı kümeler elde edilmiş oldu. Zadeh'nin önerdiği yöntemlerin kullanılabilmesi için, 2. Derece ÜF=1 varsayılmıştır.

4.adım- Matlab kütüphanesinde ilgili veri tabanı excel olarak okutuldu ve çalıştırıldı.
Sonuç olarak her bir olasılık için aşağıdaki bulanık kümeler birer birer ve en son da da durulaştırılmış merkezi değere (centroid) ulaşılmıştır.

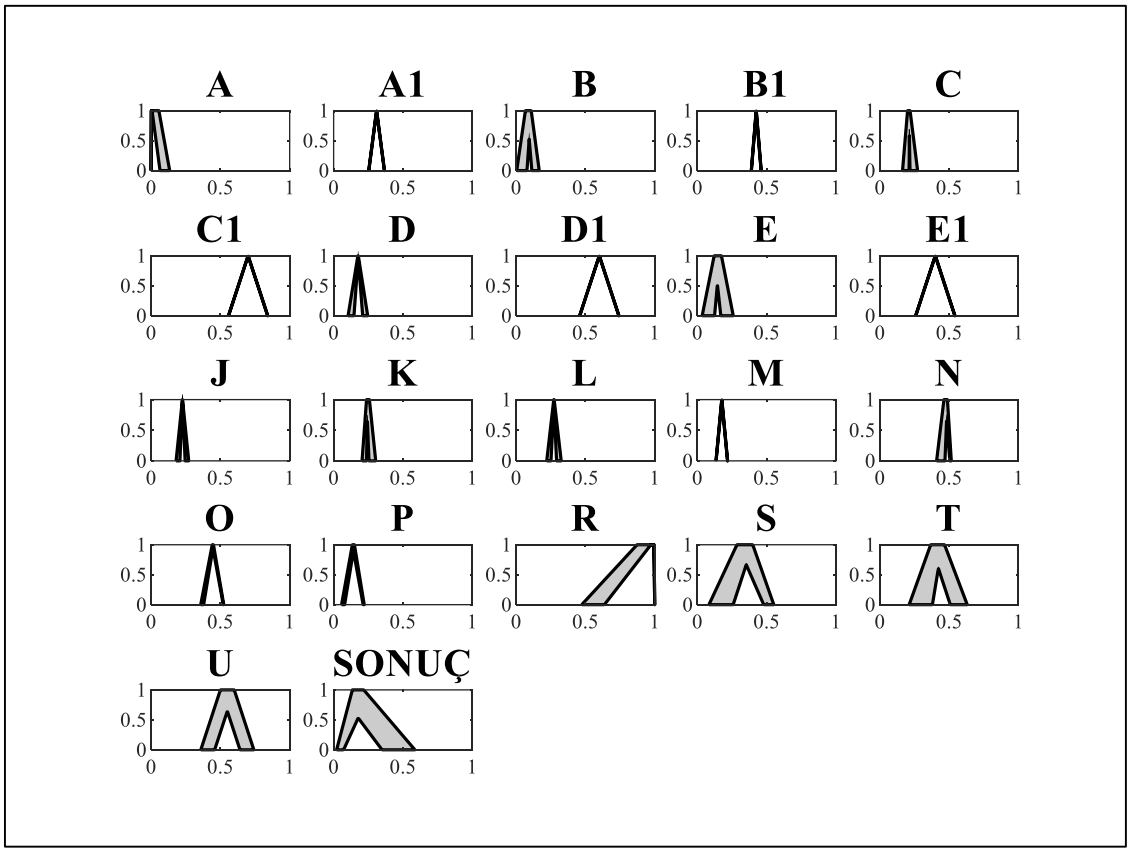
1.Adımda bahsedilen Aralıklı tip-2 bulanık kümeler ile örnek CORAS diyagramının çalıştırılması;

Bir akıllı araçtaki istenmeyen olay “Hayat Kaybı” olduğu varsayılmıştır. Bu istenmeyen olaya etki eden siber atakların birbirlerini etkileyecek şekilde ilişki ağı, CORAS aracı ile hazırlanmış ve Uygulama A’daki harita kullanılmıştır (Şekil 5.2).

Uygulamanın sahada uygulanması anlamına gelecek bir veritabanı elde edebilmek için, 34 kişiden oluşan, otomotive ve elektronik mühendisliği, yada otomotiv ve siber güvenlik gibi alanlarda ortak tecrübeleri olan uzman odak gruba EK-1’de bulunan geniş soru seti sorulmuş ve tablo halinde tüm olasılıklar için en düşük ve en yüksek ihtimallerinin değerleri toplanmıştır.

Aynı olan siber olaylar, ankette tek soru olarak sorulmuştur. Tüm sorular bu iki risk haritasındaki tüm hesaplamalar için gereken bulanık aralıkları (olasılık değerlerini) içermektedir.

Bu hali ile veriler değerlendirmeye alınmıştır. Şekil 5.2’de verilen harita ve ilgili algoritmalar ile hesaplamalar yapıldığında, aritmatik işlemler yine benzer şekilde olacaktır.Bu bakımdan yalancı kodların tekrarına gerek duyulmamıştır.



Şekil 5.5. Deney veri tabanının ilgili matlab aralıklı tip-2 bulanık CORAS yöntemi ile analiz edilmesi ve Sonuç değeri (Hayat Kaybı Riski İçin)

Sonuç olarak Şekil 5.5'de tek tek gösterilen BKA'lar, bunları takip eden nihai Merkezi Değer (Centroid) değeri hesaplanmıştır: 0,2375. Bu hesaplamaya göre tüm risk haritasının ihtimal değerleri % 23.75 ihtimalle hayat kaybı ile sonuçlanacak siber ataklara maruz kalacaktır.

Tüm bu veriler bu merkezi değere ulaşmak için yapılmıştır ve sadece bir istenmeyen olay için olasılık hesaplanabilmiştir.

Belirsizliğin kapladığı alan ve *x* ekseni değerleri aşağıdaki Çizelge 5.2'de verilmiştir.

Çizelge 5.2. Hayat kaybı risk haritası için, saha verilerinden elde edilen, tüm kelimelerin BKA koordinat değerleri

x Eks.	A	A1	AA	B	B1	BB	C	C1	CC	CAN	D
$\underline{a}_{MF}$	0,00	0,25	0,00	0,00	0,39	0,00	0,16	0,56	0,09	0,15	0,10
$\underline{c}_{MF}$	0,00	0,31	0,00	0,07	0,43	0,03	0,20	0,70	0,14	0,32	0,18
$\overline{c}_{MF}$	0,06	0,31	0,02	0,11	0,43	0,05	0,22	0,70	0,15	0,39	0,18
$\overline{b}_{MF}$	0,13	0,37	0,05	0,17	0,46	0,08	0,27	0,84	0,23	0,68	0,25
$\overline{a}_{MF}$	0,00	0,25	0,00	0,08	0,39	0,03	0,21	0,56	0,12	0,25	0,15
p	0,00	0,31	0,00	0,09	0,43	0,04	0,21	0,70	0,15	0,35	0,18
p	0,01	0,31	0,00	0,09	0,43	0,04	0,21	0,70	0,15	0,36	0,18
$\underline{b}_{MF}$	0,06	0,37	0,02	0,11	0,46	0,05	0,22	0,84	0,18	0,51	0,21
BKA	1,00	1,00	1,00	0,53	1,00	0,53	0,59	1,00	0,59	0,52	0,97

x Eks.	D1	DD	Dec_Speed	E	E1	ECU	EE	Inc_Fuel	J	K	L
$\underline{a}_{MF}$	0,46	0,05	0,01	0,03	0,26	0,03	0,01	0,03	0,18	0,21	0,22
$\underline{c}_{MF}$	0,60	0,11	0,05	0,12	0,40	0,07	0,05	0,09	0,23	0,24	0,27
$\overline{c}_{MF}$	0,60	0,11	0,08	0,17	0,40	0,09	0,07	0,11	0,23	0,26	0,27
$\overline{b}_{MF}$	0,74	0,18	0,24	0,26	0,54	0,18	0,14	0,22	0,27	0,30	0,33
$\overline{a}_{MF}$	0,46	0,07	0,04	0,12	0,26	0,05	0,03	0,06	0,21	0,24	0,25
p	0,60	0,11	0,07	0,14	0,40	0,08	0,06	0,10	0,23	0,24	0,27
p	0,60	0,11	0,07	0,14	0,40	0,08	0,06	0,10	0,23	0,24	0,27
$\underline{b}_{MF}$	0,74	0,16	0,13	0,17	0,54	0,12	0,09	0,15	0,25	0,26	0,29
BKA	1,00	0,97	0,39	0,52	1,00	0,52	0,52	0,52	0,99	0,66	0,94

Çizelge 5.2. (devam) Hayat kaybı risk haritası için, saha verilerinden elde e dilen, tüm kelimelerin BKA koordinat değerleri

x Eks.	Loss_Eng	M	Mul_breake	N	O	P	R	S	T	U	SONUC
$\underline{a}_{MF}$	0,04	0,13	0,03	0,38	0,36	0,06	0,47	0,08	0,21	0,36	0,02
$\underline{c}_{MF}$	0,11	0,18	0,09	0,44	0,44	0,14	0,87	0,29	0,37	0,50	0,13
$\overline{c}_{MF}$	0,14	0,18	0,11	0,49	0,45	0,15	1,00	0,40	0,47	0,60	0,22
$\overline{b}_{MF}$	0,30	0,22	0,24	0,52	0,52	0,22	1,00	0,55	0,63	0,74	0,59
$\overline{a}_{MF}$	0,08	0,13	0,05	0,47	0,38	0,08	0,64	0,26	0,38	0,46	0,07
p	0,12	0,18	0,10	0,48	0,45	0,14	0,97	0,35	0,42	0,55	0,18
p	0,12	0,18	0,10	0,48	0,45	0,14	1,00	0,35	0,42	0,55	0,18
$\underline{b}_{MF}$	0,19	0,22	0,17	0,50	0,52	0,21	1,00	0,48	0,51	0,64	0,35
BKA	0,39	1,00	0,52	0,39	0,94	0,90	1,00	0,67	0,61	0,65	0,39

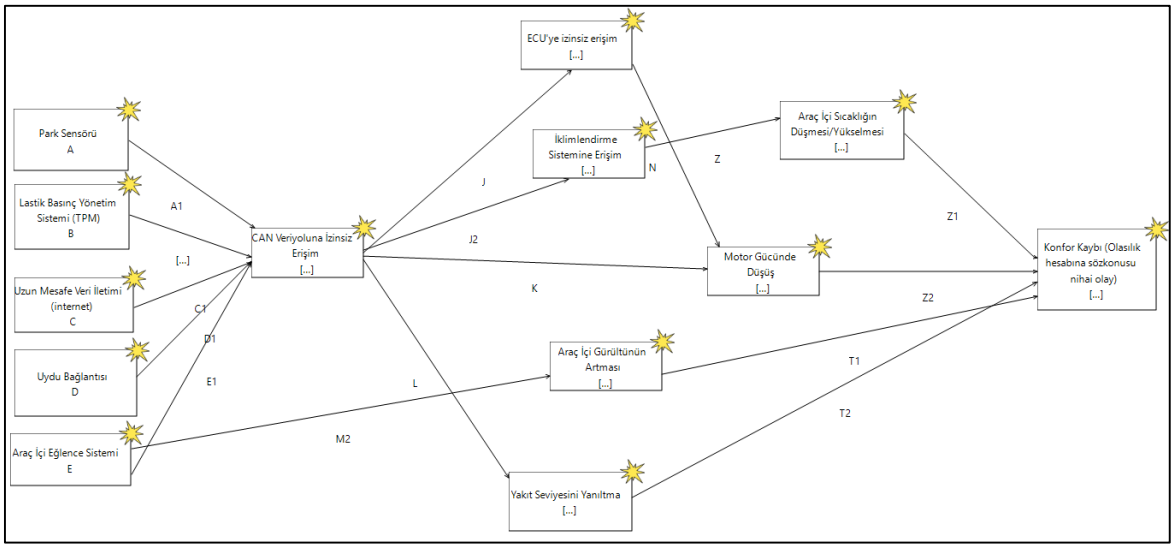
Bu değerler anket verileri olmadan, gerçek sistemlerden elde edilen değerlendirilse, bu olasılık belli bir standart sapma ile gerçek değere yakın bir değeri ifade edebilecektir.

Risk hesaplanmasında kullanılabilecek bu değer bulunduktan sonra bu olasılığın maliyeti ile çarpılarak, risk için gerçek bir değere ulaşmak söz konusu olabilir.

Haritanın sıhhati, ilişki ağının doğruluğu ve veritabanındaki ham verilerin gerçeğe yakın olması çıkan olasılık sonucunu gerçeğe yaklaştıracaktır.

5.4. Uygulama C: Anket Verileri Ile Alınmış Verilerin Konfor Düşüklüğüne Sebep Olan Siber Risklerin Değerlendirilmesinde Kullanılması

Uygulama adımları Uygulama B ile aynıdır. Ancak bu kez risk haritası değişmiştir;



Şekil 5.6. Aralıklı tip-2 bulanık CORAS tekniği için konfor kaybı risk haritası

Uygulamanın sahada uygulanması anlamına gelecek bir veritabanı elde edebilmek için, 34 kişiden oluşan, otomotive ve elektronik mühendisliği, yada otomotiv ve siber güvenlik gibi alanlarda ortak tecrübeleri olan uzman odak gruba EK-1'de bulunan geniş soru seti sorulmuş ve tablo halinde tüm olasılıklar için en düşük ve en yüksek ihtimallerinin değerleri toplanmıştır. Bu hali ile veriler değerlendirmeye alınmıştır.Şekil 5.6'da verilen harita ve ilgili algoritmalar ile hesaplamalar aşağıdaki şekilde yapılmıştır. Sonuçlar Şekil 5.7'deki gibi çıktılar sağlamıştır.

Bu haritaya göre aritmetik işlemler aşağıdaki şekilde olacaktır;

$$[AA] = A \times A1$$

$$[BB] = B \times B1$$

$$[CC] = C \times C1$$

$$[DD] = D \times D1$$

$$[EE] = E \times E1$$

$$[CAN] = [AA] + [BB] + [CC] + [DD] + [EE]$$

$$[ECU] = [CAN] \times J$$

$$[Los\_Eng] = [CAN] \times K + [ECU] \times N$$

$$[fuel] = [CAN] \times L$$

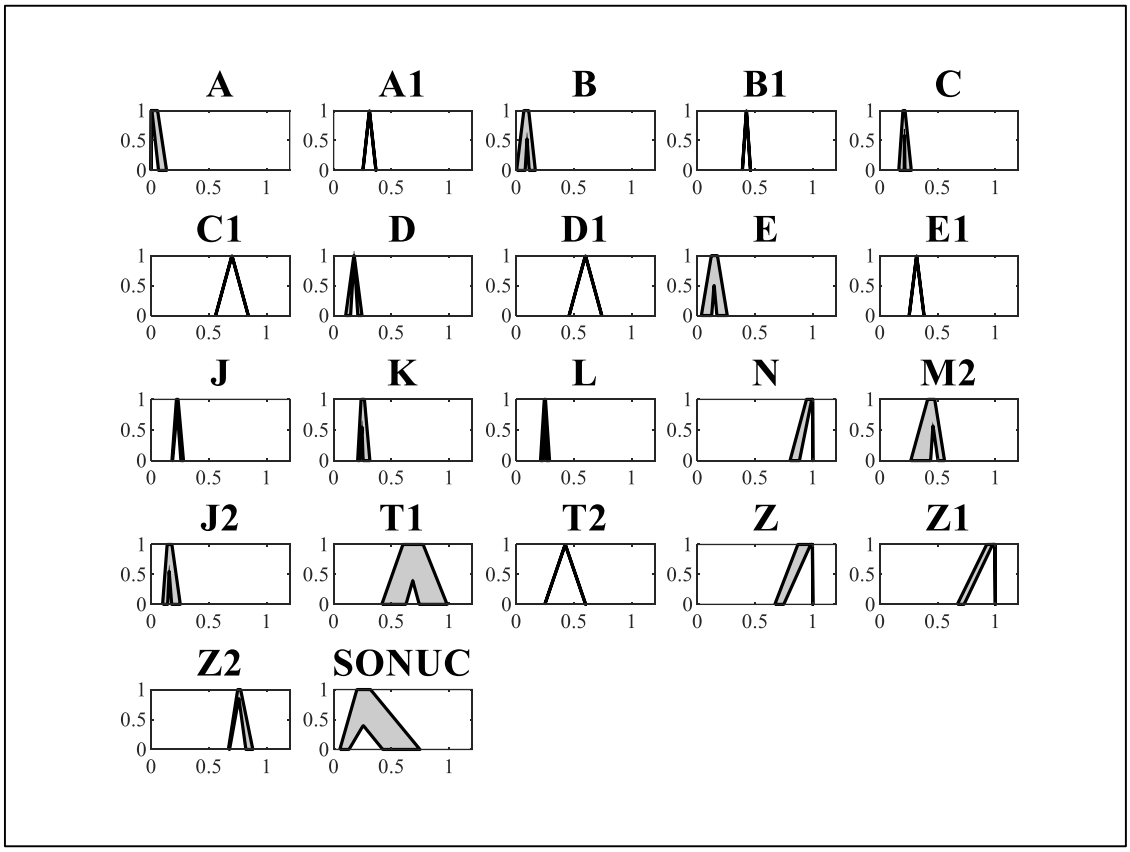
$$[hvac] = [CAN] \times J2$$

$$[heat] = [hvac] \times Z$$

$$[noise] = [E] \times M2$$

$$[sonuc] = [fuel] \times T2 + [noise] \times T1 + [Loss\_Eng] \times Z2 + [heat] \times Z1$$

şeklinde yazılabilir.



Şekil 5.7. Deney veritabanının ilgili matlab aralıklı tip-2 bulanık CORAS yöntemi ile analiz edilmesi ve sonuç değeri (konfor kaybı)

Sonuç olarak ortaya aşağıdaki gibi BKA'lar ve bunları takip eden nihai Merkezi Değer (Centroid) ortaya çıkacaktır (Şekil 5.7).

Merkezi Değer: 0,3276 olarak hesaplanmıştır. Bu durumda bu akıllı aracın % 32.76 ihtimalle, konfor kaybına sebep olabilecek ataklar maruz kalacağı ifade edilebilir.

Yukarıda grafiği verilen BKA'ların 'te değerleri verilmiştir:

Çizelge 5.3. Konfor kaybı risk haritası için, saha verilerinden elde edilen, tüm kelimelerin BKA koordinat değerleri

x Eks.	A	A1	AA	B	B1	BB	C	C1	CC	CAN	D
$\underline{a}_{MF}$	0,00	0,25	0,00	0,00	0,39	0,00	0,16	0,56	0,09	0,15	0,10
$\underline{c}_{MF}$	0,00	0,31	0,00	0,07	0,43	0,03	0,20	0,70	0,14	0,31	0,18
$\overline{c}_{MF}$	0,06	0,31	0,02	0,11	0,43	0,05	0,22	0,70	0,15	0,38	0,18
$\overline{b}_{MF}$	0,13	0,37	0,05	0,17	0,46	0,08	0,27	0,84	0,23	0,64	0,25
$\overline{a}_{MF}$	0,00	0,25	0,00	0,08	0,39	0,03	0,21	0,56	0,12	0,25	0,15
p	0,00	0,31	0,00	0,09	0,43	0,04	0,21	0,70	0,15	0,34	0,18
p	0,01	0,31	0,00	0,09	0,43	0,04	0,21	0,70	0,15	0,34	0,18
$\underline{b}_{MF}$	0,06	0,37	0,02	0,11	0,46	0,05	0,22	0,84	0,18	0,48	0,21
BKA	1,00	1,00	1,00	0,53	1,00	0,53	0,59	1,00	0,59	0,52	0,97

x Eks.	D1	DD	E	E1	EE	ECU	fuel	heat	hvac	J	J2
$\underline{a}_{MF}$	0,46	0,05	0,03	0,25	0,01	0,03	0,03	0,01	0,01	0,18	0,10
$\underline{c}_{MF}$	0,60	0,11	0,12	0,32	0,04	0,07	0,08	0,04	0,04	0,22	0,14
$\overline{c}_{MF}$	0,60	0,11	0,17	0,32	0,06	0,09	0,10	0,07	0,07	0,23	0,18
$\overline{b}_{MF}$	0,74	0,18	0,26	0,38	0,10	0,18	0,18	0,16	0,16	0,28	0,25
$\overline{a}_{MF}$	0,46	0,07	0,12	0,25	0,03	0,05	0,06	0,03	0,04	0,19	0,14
p	0,60	0,11	0,14	0,32	0,05	0,08	0,08	0,05	0,05	0,23	0,16
p	0,60	0,11	0,14	0,32	0,05	0,08	0,09	0,05	0,05	0,23	0,16
$\underline{b}_{MF}$	0,74	0,16	0,17	0,38	0,06	0,12	0,13	0,09	0,09	0,26	0,18
BKA	1,00	0,97	0,52	1,00	0,52	0,52	0,52	0,52	0,52	0,84	0,56

x Eks.	K	L	Loss_Eng	M2	N	noise	T1	T2	Z	Z1	Z2	Sonuc
$\underline{a}_{MF}$	0,21	0,21	0,05	0,27	0,80	0,01	0,42	0,25	0,67	0,67	0,67	0,05
$\underline{c}_{MF}$	0,24	0,24	0,14	0,41	0,95	0,05	0,60	0,43	0,87	0,93	0,75	0,20
$\overline{c}_{MF}$	0,27	0,25	0,19	0,48	1,00	0,08	0,78	0,43	1,00	1,00	0,78	0,32
$\overline{b}_{MF}$	0,31	0,29	0,38	0,56	1,00	0,15	0,98	0,60	1,00	1,00	0,88	0,75
$\overline{a}_{MF}$	0,23	0,23	0,10	0,44	0,88	0,05	0,63	0,25	0,75	0,73	0,68	0,13
p	0,25	0,25	0,16	0,46	0,99	0,07	0,69	0,43	0,98	0,98	0,76	0,25
p	0,25	0,25	0,16	0,46	1,00	0,07	0,69	0,43	1,00	1,00	0,76	0,26
$\underline{b}_{MF}$	0,26	0,26	0,25	0,50	1,00	0,09	0,74	0,60	1,00	1,00	0,82	0,43
BKA	0,55	0,74	0,52	0,57	1,00	0,52	0,40	1,00	1,00	1,00	0,86	0,40

Tüm bu veriler bu merkezi değere ulaşmak için yapılmıştır ve sadece bir istenmeyen olay için olasılık hesaplanabilmiştir.

Bu değerler antek değilde, gerçek sistemlerden elde edilen değerlendirilse, bu olasılık belli bir standart sapma ile neredeyse gerçek değeri ifade edecekti.

Risk hesaplanmasında kullanılabilecek bu değer bulunduktan sonra bu olasılığın maliyeti ile çarpılarak, risk için gerçek bir değere ulaşmak söz konusu olabilir.

Haritanın sıhhati, ilişki ağının doğruluğu ve veritabanındaki ham verilerin gerçeğe yakın olması çıkan olasılık sonucunu gerçeğe yaklaştıracaktır.

6. SONUÇLAR VE GELECEK ÇALIŞMALAR

CORAS diyagramlarında, teoriye odaklanılmak ve sadelik adına, akıllı aracın kendisi ve içindeki akıllı parçalar varlıklar (assets) olarak kabul edilmiş ve gösterilmeye gerek duyulmamıştır. Elbette varlığın olmadığı yerde risk de yok sayılır. Ancak gösterimlerin karmaşıklaşmaması için bu varlıklar CORAS diyagramlarında gösterilmemiştir. Risk hesaplamalarında;

R= olasılık x mali değer (zarar)

Formülü ile nihai zararın maliyeti de belirlenebilir ve risk analizlerinde bunlar gösterilebilir. Ancak bu çalışma da çalışmanın odağını dağıtacağı için ihmal edilmiştir.

CORAS risk haritaları görüldüğü gibi tüm bir akıllı aracın risklerini modellememiştir. Eğer istenirse çok daha karmaşık ve araç üzerindeki tüm atak yüzeylerini kapsayan bir risk haritası gelecek çalışması olarak yapılabilir. Bu çalışma başlı başına bir risk haritası çalışması olacaktır.

Bu çalışma sadece akıllı araçlar için değil, akıllı parça taşıyan, insansız hava araçlarından, kalp piline, uydulardan kol saatlerine kadar tüm sistem ve cihazlar için yapılabilir. Çalışma yeterli istatistiksel veriler elde edilmesi durumunda, ankete dayalı neticeler ile test edilebilir, genişletilebilir, ya da güncellenebilir. Buna ilave olarak makine öğrenmesi ve derin öğrenme teknikleri ile yapay zekâ eklenebilir, ya da yapay zekâ ile modelin gürbüz ve güvenilir olması sağlanabilir.

Çalışmada gelişmiş aralıklı yaklaşım (GAY) ve Mendel ve Wu tarafından geliştirilen, gelişmiş Karnik Mendel algoritmaları (GKMA) ve bu algoritmalar içindeki optimize edilmiş veri eleme yöntemleri kullanılmıştır (Outlier process, barrier calculation vb gibi).Buradaki yöntemler teknolojiye, subjeye ve sürece göre, eğer yeterli sayıda ve olgunlukta çalışma yapılırsa geri besleme ile tekrar hesaplanabilir. Bu durumda otomasyon ve mühendislik sistemleri için aykırı sayılabilecek verilen belki de risk analiz sistemlerinde normal sayılabilecektir.

Çalışmada; hayat kaybına sebep olan sıralı olayların, olasılık hesapları sonucu elde edilen ve belirsizliğin kapladığı alan olarak belirtilen toplam olasılık değeri bir miktar yüksek çıkmış görünmektedir. Neredeyse her 5 ataktan birisi ölümle sonuçlanmış gibi görünmektedir. Bunun çok sayıda sebebi olmakla beraber en önemli sebepleri şunlardır:

a-Risk haritasının mükemmeli yansıtmaması; burada risk haritası sadece yöntemi ispatlamak için deneysel olarak kullanılmıştır. Bazı denekler üzerinde denense de istenmeyen olayların tamamını ve buna etki eden alt faktörlerin tamamı haritada gösterilmemektedir. Bu bakımdan bu değerin gerçekten uzak (ve yüksek) çıkması normal olarak görülmüştür. Benzer bir durum Konfor Kaybı haritasında da gerçekleştirmiştir. Gerçekten tüm konfor kaybına sebep olan alt olaylar haritalansa idi daha doğru bir sonuca yaklaşmak mümkün olabilecektir.

b- Deneklerin sorular verdiği cevaplar incelendiğinde aralıkların ya çok yakın ya çok uzak olduğu ve genel olarak özensiz olduğu görülmüştür. Olasılık rakamlarının, dolayısıyla riskin yüksek görünmesindeki ikincil temel faktör olarak düşülmektedir.

Ayrıca 3. bölümde bahsedilen CORAS ilişki türlerinden “sebep olan” ilişki türünün bağımsız olaylar zinciri ile olasılık hesabı yapılmıştır. Başka bir çalışmada sebep olan ilişki türünde ancak bu kez istatistiksel olarak birbirinden bağımlı (dâhil eden veya hariç tutan) verilerle de hesaplanarak daha gerçekçi sonuçlara yaklaşılacaktır.

Yine 3. bölümde anlatılan, tolerans işleme limitleri güven seviyesi % 95 değilde daha düşük yada daha yüksek bir limit olarak işlenebilir ve verinin esnekliği ile oynanarak en uygun rakamlar, saha verileri ile karşılaştırılabilir. Sonuçta gerçek dünyaya en yakın tolerans işleme limiti, bu alan için standart kabul edilebilir.

Gelecekte denek sayısı artırılarak, soruların kalitesi ve sorulma şekli artırılabilir. Ven şemasında bahsedilen birbirini destekleyen ve birbirini dışlayan olasılık durumlarının tamamını içeren soru seti hazırlanabilir. Özellikle birbirini dışlayan istenmeyen olayların olasılıklarının hesabı, nihai olasılık hesabını daha hassaslaştırmaya yardımcı olacaktır.

Bu çalışmada risk yönetiminin en temel öğelerinden olan, “olasılık” odaklı bir çalışma yapılmıştır. Bu amaçlara deneklere seçilmiş olayların olma olasılıkları aralıklı olarak

sorulmuştur. Benzer bir çalışma gelecekte, frekans temelli olarak da yapılabilir. Senaryonun kurgulanmasının ardından, senaryo frekans modeli CORAS benzeri haritalarla çıkarılabilir ve benzer bir probabilistik yöntem buraya da uygulanabilir. Olasılıkla ters orantılı olark düşünülebilecek frekans değerinin de benzer sonuçlar üreteceği düşünülmektedir.

Bu teknik; otomotiv şirketlerin ellerinde bulunduğu düşünülen atak veritabanları (attack profile) elde edilerek genişletilebilir ve mevcut yöntemle kaşılaştırılabilir. Alternatif olarak akıllı araçların haricinde örneğin operasyonel riskler alanında değerlendirilip sonuçlar doğrulanabilir.

Doktora sonrası çalışmalarda, olasılık değerinin yanında risk maliyeti de benzer bir yöntemle hesaplanabilir. Ayrıca risk haritaları daha karmaşık hale getirilebilir. Farklı istatistiksel veri işleme yöntemleri kullanılarak, daha sağlıklı veri üzerinde çalışılması sağlanabilir. Ayrıca derin öğrenme ve yapay sinir ağları kullanılarak yönteme geri bildirim anlamına gelecek girdiler ile karnik mendel algoritmaları ve tolerans limitleri daha da olgunlaştırılabilir.

Sonuç olarak; bu doktora tezinde yapılan çalışmalar; akıllı araçlar alanından, akıllı sistemler alanına doğru genişletilebilir. Bununla beraber uygulama alanı aynı kalmakla beraber, alternatif risk yönetim yöntemlerine yaygınlaştırılabilir. Buradaki risk yönetim yöntemleri operasyonel risklerin belirlenmesi amacı ile verinin eksik olduğu ve kişiler arası anket sonuçlarının farklılaştığı durumlarda rahatlıkla kullanılabilecektir. Risk yönetim yaklaşımları çok sayıda olmakla beraber en doğru risk yönetim yaklaşımı için bu çalışmaların doğrulanarak yönetim sistemlerine dönüşmesi yapılabilecektir.

KAYNAKLAR

Beckers, K., Heisel, M., Solhaug, B., & Stølen, K. (2014). ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System, 315–344. https://doi.org/10.1007/978-3-319-07452-8_13

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *40*(1), 131–158.

Brooks, R. R., Sander, S., Deng, J., & Taiber, J. (2009). Automobile security concerns. *IEEE Vehicular Technology Magazine*, *4*(2).

Cebula, J. J., & Young, L. R. (2010). A Taxonomy of Operational Cyber Security Risks. *Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst*, (December), 1–47. https://doi.org/10.1007/978-1-4419-7133-3

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., … Kohno, T. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *USENIX Security Symposium*. San Francisco.

Cho, A.-R., Jo, H. J., Woo, S., Son, Y. D., & Lee, D. H. (2012). A message authentication and key distribution mechanism secure against CAN bus attack. *Journal of the Korea Institute of Information Security and Cryptology*, *22*(5), 1057–1068.

Dubois, D., & Prade, H. (2005). Interval-valued fuzzy sets, possibility theory and imprecise probability. *Proceedings of International Conference in Fuzzy Logic and Technology*, 314–319. Retrieved from ftp://ieut1.irit.fr/pub/IRIT/ADRIA/DP311.pdf

Eling, M., & Wirfs, J. H. (2015). Modelling and Management of Cyber Risk. *Wriec.Net*, 1–20. Retrieved from http://www.wriec.net/wp-content/uploads/2015/07/6J2_Eling.pdf

Francillon, A., Danev, B., & Capkun, S. (2011). Relay attacks on passive keyless entry and start systems in modern cars. In *IN PROCEEDINGS OF THE 18TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM. THE INTERNET SOCIETY*. Citeseer.

Gehrke, M., Walker, C., & Walker, E. (1996). Some comments on interval valued fuzzy sets! *Structure*, *1*, 2.

Hossain, I., & Mahmud, S. M. (2007). Analysis of a secure software upload technique in advanced vehicles using wireless links. In *Intelligent Transportation Systems Conference, 2007. ITSC 2007. IEEE* (pp. 1010–1015). IEEE.

Ingoldsby, T. R. (2013). *AttackTreeThreatRiskAnalysis*. *Amenaza Technologies Limited*. Retrieved from https://www.amenaza.com/downloads/docs/AttackTreeThreatRiskAnalysis.pdf

Ishtiaq Roufa, R. M., Mustafaa, H., Travis Taylora, S. O., Xua, W., Gruteserb, M.,

Trappeb, W., & Seskarb, I. (2010). Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *19th USENIX Security Symposium, Washington DC* (pp. 11–13).

Kim, J. E., Chun, B. J., & Park, S. B. (2013). Secure diagnostic implementation for automotive ECU with crypto library. In *Korea Society Automotive Engineers2013 Annual Conference* (pp. 20–22).

Klimov, S. M., & Kotyashev, N. N. (2013). METHOD OF RISK MANAGEMENT FOR AUTOMATED, (1), 101–107.

Klir, G. J., & Yuan, B. (1995). Fuzzy sets and fuzzy logic: theory and applications. *Upper Saddle River*, 563.

Kong, H.-K., Kim, T.-S., & Hong, M.-K. (2016). A security risk assessment framework for smart car. In *Proceedings - 2016 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2016*. https://doi.org/10.1109/IMIS.2016.42

Kordy, B., Mauw, S., Radomirović, S., & Schweitzer, P. (2014). Attack-defense trees. *Journal of Logic and Computation*, *24*(1), 55–87. https://doi.org/10.1093/logcom/exs029

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., … Shacham, H. (2010). Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on* (pp. 447–462). IEEE.

Lund, M. S., Solhaug, B., & Stølen, K. (2010). *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media.

Macher, G., Sporer, H., Berlach, R., Armengaud, E., & Kreiner, C. (2015). SAHARA: a security-aware hazard and risk analysis method. In *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition* (pp. 621–624). EDA Consortium.

McGrath, J. E. (1984). Groups: Interaction and Performance. *Administrative Science Quarterly*. https://doi.org/10.2307/2393041

Mendel, J.M. (2017). Uncertain rule-based fuzzy systems. In *Introduction and new directions* (p. 684). Springer.

Mendel, J. M, & John, R. I. B. (2002). Type-2 Fuzzy Sets Made Simple, *10*(2), 117–127.

Mendel, J. M, John, R. I., & Liu, F. (2006). Interval type-2 fuzzy logic systems made simple. *IEEE Transactions on Fuzzy Systems*, *14*(6), 808–821.

Microsoft. (2007). DREAD Model. Retrieved December 2, 2019, from https://blogs.msdn.microsoft.com/david_leblanc/2007/08/14/dreadful/

Nilsson, D. K., & Larson, U. E. (2008). Secure firmware updates over the air in intelligent

vehicles. In *Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on* (pp. 380–384). IEEE.

Paja, E., Dalpiaz, F., & Giorgini, P. (2014). STS-tool: Security requirements engineering for socio-technical systems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-319-07452-8_3

Pouyan, A. A., & Alimohammadi, M. (2014). Sybil Attack Detection in Vehicular Networks. *Computer Science and Information Technology*, *2*(4), 197–202.

Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security*, *15*(1), 39–68.

Ren, D., Du, S., & Zhu, H. (2011). A novel attack tree based risk assessment approach for location privacy preservation in the VANETs. In *Communications (ICC), 2011 IEEE International Conference on* (pp. 1–5). IEEE.

Rhim, W.-W., Kim, J.-S., Kim, S.-J., & Oh, H.-K. (2011). Reduced RSU-dependency authentication protocol to enhance vehicle privacy in VANET. *Journal of the Korea Institute of Information Security and Cryptology*, *21*(6), 21–34.

Ross, T. J. (2010). *Fuzzy Logic with Engineering Applications: Third Edition*. *Fuzzy Logic with Engineering Applications: Third Edition*. https://doi.org/10.1002/9781119994374

Solheim, I., and Stølen, K. (2007) , *Technology research explained.* , Rapor numarası : SINTEF A313, SINTEF ICT, OSLO/NORWAY

Standardizing Cyber Threat Intelligence Information with the Structured Threat *Information eXpression (STIX™)* (t.y.), Aralık 1, 2019, from STIX, http://stixproject.github.io/getting-started/whitepaper/

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., & Laarouchi, Y. (2013). Survey on security threats and protection mechanisms in embedded automotive networks. In *Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on* (pp. 1–12). IEEE.

Technology Quarterly, T. connected car. (2003). The connected car. https://doi.org/10.1108/978-1-78714-833-820181017

Tran, T. H. D. (2017). Risk Assessment Based on CORAS and Fuzzy logic.

Trifts, V. (2019). Deductive Inference. Retrieved December 1, 2019, from http://penta.ufrgs.br/edu/telelab/3/deductiv.htm

Weiss, J. D. (1991). A system security engineering process. In *Proceedings of the 14th National Computer Security Conference* (Vol. 249, pp. 572–581).

Wolf, M., & Gendrullis, T. (2012). Design, implementation, and evaluation of a vehicular

hardware security module. *Information Security and Cryptology-ICISC 2011*, 302–318.

Wolf, M., Scheibel, M., & Gmbh, T. Ü. V. I. (2012a). *A Systematic Approach to a Qualified Security Risk Analysis for Vehicular IT Systems.* In *Automotive-Safety & Security* (pp. 195–210).

Wolf, M., Scheibel, M., & Gmbh, T. Ü. V. I. (2012b). A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems. *ESCRYPT Automotive Safety and Security*, 195–210.

Wu, D., Mendel, J. M., & Coupland, S. (2012). *Enhanced Interval Approach for Encoding Words Into Interval Type-2 Fuzzy Sets and Its Convergence Analysis*, *20*(3), 499–513.

Zima, P. V. (2007). *What is Theory? : Cultural Theory as Discourse and Dialogue*. *What is Theory? : Cultural Theory as Discourse and Dialogue*. https://doi.org/10.5040/9781472546029

EKLER

Ek-1. Anket soru tablosu

Her iki risk haritasının hazırlanması için oluşturulmuş birleşik soru veritabanı
A-Bir akıllı aracın, park sensörünün siber atağa maruz kalarak ele geçirilme ihtimali, diğer sensör ve aksamları gözünüzün önüne getirdiğinizde sizce % en az ve en çok kaçtır?

A1- Park Sensörünün ele geçirildiğini var sayalım. Buradan CAN Bus (Controller Area Network) sistemine sızması ihtimali nedir?

B-Araçlardaki TPM, Lastik Basınç Yönetim sensörünün (sisteminin), siber atağa maruz kalarak ele geçirilme ihtimali % en az ve en çok kaçtır?

B1-Lastik Basınç Sisteminin ele geçirildiğini düşünelim, sizce buradan CAN Bus (Controller Area Network) sistemine sızması ihtimali nedir?

C-Bazı araçlarda internet-data bağlantısı da vardır. Sizce bu bağlantının, diğer akıllı parçalara göre (park sensörü, uydu bağlantısı vb.) ele geçirilme (hacklenmesi) ihtimali sizce % en az ve en çok kaçtır?

C1- İnternet bağlantısının uzaktan ele geçirildiğini düşünelim. Sizce atak eden kişinin buradan CAN Bus (Controller Area Network) sistemine sızması ihtimali nedir?

D- Bazı akıllı araçlara uydu bağlantısı da bulunur. Sizce bu uydu bağlantısının, diğer akıllı parçalara göre atak alarak ele geçirilmesi ihtimali nedir?

D1-Uydu bağlantısını ele geçirildiği durumda, CAN Bus'a ulaşma (ele geçirme ve sömürme) ihtimali nedir?

E-Araç içi eğlence sisteminin ele geçirildiğini düşünelim. Sizce buradan CAN BUS (Controller Area Network)'e sızılması olasılığı % en az ve en çok kaçtır?

E1-Araç İçi Eğlence Sistemini ele geçiren bir kişi, CAN Bus (Controller Area Network) sistemine sızması ihtimali nedir?

J-Bu kez CAN Bus'ın ele geçirildiğini düşünelim. Sizce atak eden kişi, ECU(ler)e ulabilir mi? % kaç ihtimalle en az ve en çok ulaşabilir.?

K-Bu kez CAN Bus'ın ele geçirildiğini düşünelim. Sizce Araç motorunda bir güç azaltma yapılabilme ihtimali % kaçtır Minimum ve Maksimum rakam giriniz?

Ek-1. (devam) Anket soru tablosu

L-Bu kez CAN Bus'ın ele geçirildiğini düşünelim. Yakıt seviyesini farklı gösterebilirler mi?

M- CAN Bus'ın ele geçirildiğini düşünelim. Sizce atak eden kişi fren sistemini çalışmaz hale getirebilirmi?

N-Aracın ECU'süne ulaşıldığını farz edelim, Sizce Araç motorunda bir güç azaltma yapılabilme ihtimali % kaçtır Minimum ve Maksimum rakam giriniz?

O- Aracın ECU'süne ulaşıldığını farz edelim. Sizce atak eden kişi fren sistemini çalışmaz hale getirebilir mi?

R- Sizce aracın fren sisteminin devre dış olma olasılığı hangi ihtimalle can kaybına sebep olan bir kaza ile sonuçlanabilir?

S- Siber atak sebebi ile motor gücündeki bir kayıp, sizce ne ihtimalle can kaybına sebep olan bir kaza ile sonuçlanabilir?

P- Yakıt seviyesinin düşük olmasının (siber atak sebebi ile), hangi ihtimalle araç hızında dramatik bir düşüş veya yükselişe sebep olabilir?(panik vb sebeplerle)

T-Siber atak sebebi ile motor gücündeki bir kayıp, sizce ne ihtimalle araç hızında dramatik bir düşüş veya yükselişe sebep olabilir?(panik vb sebeplerle)

U- Araç hızında dramatik bir değişiklik sizce hangi ihtimalle can kaybına sebep olan bir kaza ile sonuçlanabilir?

M2- Araç içi eğlence sisteminin ele geçirildiği bir durumda, ses patlaması yaparak sürücünün dikkatini dağıtılma ihtimali nedir?

J2- CAN Bus'ın ele geçirildiği durumda, Klima siteminin ele geçirilme ihtimali nedir?

T1-Aracın içindeki ses düzeyinin ele geçirilip kontrol edilebildiği bir durumda, netice olarak araç konforu bundan hangi aralıkta etkilenir?

T2-Yakıt düzeyinin yanlış gösterildiği bir durumda, aracın konforunun etkilenme ihtimali nedir?

Z- Eğer klima sistemi kötü niyetli kullanıcılar tarafından ele geçirilirse, araç sıcaklığı değiştirebilme ihtimali nedir?

Ek-1. (devam) Anket soru tablosu

Z1-Araç-içi ortam sıcaklığının kontrolünün ele geçirildiği durumda, bunun araç konforunu olumsuz etkilemesi ihtimali nedir?

Z2-Aracın gücünün ele geçirildiği durumda, bu hangi ihtimalle konfor kaybına sebep olur?

Anketin yapıldığı uygulama ve form;

https://form.jotform.com/91486740176969

EK-2. Denek listesi ve veri tablosu

			A		A1		B		B1		C	
Cevap Tarihi	Ad	Soyadı	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
2019-07-03 08:59:42	En.	F..	1	15	85	95	1	15	85	95	45	85
2019-06-21 11:34:03	Sin…	K..	10	20	30	40	50	60	70	80	80	90
2019-06-17 14:07:02	Er…	Ç..	60	30	30	10	50	10	30	20	70	10
2019-06-14 13:03:59	Os..	K..	20	50	20	40	10	20	20	30	50	60
2019-06-13 09:48:16	Mu..	E..	0	10	10	60	0	20	10	60	30	90
2019-06-13 09:24:24	Mu..	K..	0	5	95	100	0	5	95	100	90	95
2019-06-13 09:10:24	Se..	B..	0	10	20	30	20	30	10	20	50	70
2019-06-13 08:32:32	Du..	Y..	20	80	15	85	20	80	15	85	30	70
2019-06-13 08:19:22	Öm..	E..	10	40	10	30	10	30	10	30	20	40
2019-06-13 06:38:27	Me..	K..	1	5	0	0	1	5	0	0	60	95
2019-06-12 21:53:51	İs..	V..	20	40	15	25	40	60	40	70	70	80
2019-06-12 21:28:59	Öm..	G..	0	20	0	20	0	20	100	100	100	100
2019-06-12 21:19:27	İb..	Ö..	5	20	1	5	5	60	10	30	5	40
2019-06-12 21:17:06	Gö..	A..	5	10	20	40	5	10	20	40	60	80
2019-06-12 21:10:01	Y…	S..	80	99	50	70	70	90	70	90	80	90
2019-06-12 19:00:40	Le..	S..	20	40	10	20	80	100	60	100	70	100
2019-06-12 17:19:19	Ha..	M..	5	30	10	45	5	30	10	45	25	50
2019-06-12 17:02:46	Ah..	A..	15	67	25	99	10	67	34	99	25	55
2019-06-12 10:51:59	Em..	P..	0	10	30	60	25	50	40	60	60	80
2019-06-12 09:03:45	K..	G..	5	20	20	80	1	5	20	80	50	99
2019-06-11 20:29:46	Gö..	T..	85	99	35	95	50	75	45	50	99	100
2019-06-11 19:48:36	Ka..	K..	0	0	0	0	0	0	0	0	90	100
2019-06-11 18:58:11	Ah..	A..	85	98	95	99	50	72	50	62	98	100
2019-06-11 17:20:52	Me..	T..	30	70	50	80	30	80	50	80	50	90
2019-06-11 15:35:50	Şü…	O..	3	28	27	35	11	38	15	26	51	91
2019-06-11 14:42:15	Me..	D..	1	2	10	15	2	3	10	15	1	2
2019-06-11 14:41:39	Ut…	Ö..	2	3	3	4	15	20	40	45	50	55
2019-06-11 12:51:52	Hü…	K..	90	97	95	98	80	90	80	85	95	99
2019-06-11 12:11:39	İb..	K..	80	100	50	70	0	50	50	70	80	100
2019-06-11 11:32:58	Ha..	G..	0	20	100	100	0	5	100	100	50	100
2019-06-11 11:14:33	Em…	A..	20	50	1	10	1	20	1	10	30	70
2019-06-11 09:09:14	Me	O..	1	20	20	50	1	10	5	25	30	50
2019-06-11 08:58:37	Ab..	Ö..	20	80	20	60	10	50	10	40	80	90
2019-06-10 22:50:10	Mü	Y..	5	15	1	5	5	25	1	3	20	50

EK-2. (devam) Denek listesi ve veri tablosu

C1		D		D1		E		E1		J		K		L	
Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
85	95	1	15	85	95	1	15	85	95	85	95	5	25	85	95
80	90	60	70	60	70	50	60	30	40	80	90	100	100	30	40
70	10	80	30	70	30	20	10	15	5	80	20	60	40	80	60
40	50	10	15	20	30	20	50	5	10	10	30	50	70	60	100
50	100	30	90	30	70	40	90	50	90	90	100	90	100	90	100
90	95	50	50	90	95	50	50	90	95	90	95	90	95	90	95
50	70	50	70	50	70	20	50	50	70	30	50	70	90	50	70
10	10	25	75	30	70	30	70	10	10	30	70	20	80	30	70
20	40	20	50	20	50	30	50	10	30	30	50	30	40	40	60
10	80	10	30	1	10	10	30	0	1	5	90	50	100	90	100
80	90	20	50	20	50	10	30	10	30	80	90	90	95	80	90
100	100	50	70	100	100	20	50	20	50	100	100	100	100	50	100
30	90	30	80	10	50	5	30	1	10	90	100	98	99	5	20
60	80	50	80	50	70	30	50	30	50	40	70	80	100	80	100
80	90	70	90	70	90	60	80	60	90	70	100	80	100	90	100
80	100	70	100	70	100	20	50	20	50	80	100	90	100	30	50
20	50	15	40	5	30	10	50	5	25	10	25	5	20	20	50
15	35	15	40	10	30	20	67	34	100	25	100	34	100	9	67
70	80	50	60	10	30	20	40	70	80	60	80	70	90	80	90
20	50	30	99	35	70	30	60	5	20	70	99	80	100	80	100
90	99	90	95	90	95	45	75	45	70	99	100	99	100	99	100
90	100	90	100	90	100	90	100	90	100	90	100	90	100	90	100
96	100	100	100	100	100	89	92	76	88	88	9	77	87	67	88
50	90	50	90	50	90	30	70	50	90	50	90	50	90	70	90
53	79	7	17	11	21	39	67	25	57	39	67	11	23	80	95
40	45	2	4	2	4	20	25	1	2	70	90	80	100	80	95
15	20	45	50	15	20	50	55	15	20	90	95	90	95	90	95
99	99,9	90	99	95	99	95	97	95	97	98	99	70	85	99	99
80	100	80	100	80	100	80	100	80	100	80	100	20	50	20	50
100	100	20	50	100	100	100	100	100	100	100	100	100	100	100	100
70	100	1	30	70	100	50	100	50	100	50	70	50	100	99	100
60	80	40	60	80	100	80	100	80	100	60	100	60	100	80	100
80	90	80	90	80	90	30	40	30	40	10	20	20	30	30	40
25	60	90	100	90	100	20	35	1	2	95	100	90	100	95	100

EK-2. (devam) Denek listesi ve veri tablosu

M		N		O		R		S		P		T		U	
Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
45	65	38	50	38	50	85	100	0	15	0	5	1	5	75	100
90	100	44	47	47	53	60	70	40	50	30	40	50	60	40	50
100	90	28	44	44	56	70	30	40	30	60	60	100	70	70	70
50	90	38	56	25	44	50	60	50	80	60	80	60	90	40	90
90	100	45	50	45	50	80	90	20	40	20	40	20	40	20	50
0	5	90	95	0	5	50	50	20	25	0	5	90	95	50	50
50	70	36	50	36	50	20	30	50	70	20	30	50	70	50	70
30	70	21	50	21	50	40	60	20	80	20	80	20	80	40	60
30	40	21	57	21	43	60	100	5	20	5	10	20	30	20	40
0	5	48	95	0	5	75	95	1	5	1	5	25	35	25	35
80	100	40	50	40	50	80	95	80	95	60	80	80	90	80	95
20	50	67	67	13	33	50	100	0	50	20	50	20	50	50	100
1	2	97	98	1	2	60	99	1	2	10	30	10	25	1	2
80	100	45	50	40	50	70	90	50	80	20	30	40	70	10	30
90	100	45	50	45	50	80	100	80	100	70	100	80	100	80	100
80	100	40	50	40	50	50	80	30	50	20	50	20	50	20	50
5	10	33	83	8	17	25	75	5	15	10	40	10	20	25	75
5	55	26	75	4	25	40	85	5	35	15	50	25	78	25	90
40	50	57	64	29	36	70	100	20	40	0	5	60	80	40	60
80	100	40	50	40	50	50	100	20	100	10	100	80	100	20	100
99	100	45	50	45	50	99	100	45	75	50	70	80	90	45	65
20	50	45	50	45	50	90	100	50	80	10	20	90	100	90	100
98	100	48	50	48	50	100	100	100	100	77	89	89	95	96	100
60	90	35	53	29	47	60	90	30	70	50	90	40	80	50	70
79	93	40	48	45	52	33	77	33	67	8	19	17	29	11	27
5	15	47	50	47	50	5	10	2	3	1	2	3	10	50	100
2	3	47	50	47	50	2	3	1	2	1	2	4	5	3	4
95	99	38	47	52	53	0	99	0	99	20	45	20	45	0	99
20	50	20	50	20	50	50	100	50	100	20	50	20	50	80	100
100	100	25	50	50	50	80	100	0	20	0	0	100	100	0	50
50	70	50	50	43	50	70	100	70	82	42	75	70	99	51	100
80	100	40	50	40	50	90	100	20	40	10	30	10	30	0	20
0	5	57	86	0	14	40	50	40	50	20	30	20	25	30	40
5	25	72	80	4	20	80	100	75	90	5	10	5	10	75	95

EK-2. (devam) Denek listesi ve veri tablosu

M2		J2		T1		T2		Z		Z1		Z2	
Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
85	95	5	25	75	100	5	15	85	100	85	100	85	100
60	70	30	40	70	80	30	40	70	80	60	70	40	50
40	40	40	40	50	50	30	40	70	50	100	90	80	80
20	30	50	60	60	90	10	20	10	15	60	90	50	100
50	90	70	90	70	100	30	70	80	100	80	100	60	90
0	5	50	50	90	95	0	5	90	95	90	95	90	95
50	70	50	70	50	70	50	70	50	70	50	70	50	70
40	60	40	60	50	50	20	80	40	60	40	60	30	70
10	20	30	50	20	30	30	40	30	70	30	60	30	60
60	80	0	100	90	100	0	1	99	100	95	100	60	80
50	60	50	60	40	50	50	60	80	100	80	100	80	100
50	100	0	50	50	100	0	0	50	100	50	100	0	50
30	80	1	2	30	80	60	80	98	99	45	85	98	99
2	10	70	90	20	40	20	40	70	90	60	90	60	90
80	100	80	100	70	100	60	80	90	100	60	90	80	100
30	80	20	40	80	100	80	100	80	100	80	100	20	50
10	50	10	40	40	75	20	45	50	80	50	80	40	75
33	99	10	49	15	75	5	51	15	67	21	67	51	90
80	90	20	40	70	100	0	5	90	100	80	100	70	80
20	100	50	90	50	100	5	40	60	100	80	100	75	90
45	75	50	75	45	55	45	75	35	55	55	60	70	85
90	100	90	100	90	100	20	50	90	100	90	100	90	100
78	89	67	77	67	88	88	92	78	88	78	94	93	96
70	90	40	70	50	90	40	60	60	90	40	90	50	90
11	26	7	15	19	29	3	11	19	29	19	33	23	41
20	80	20	80	90	100	80	95	70	95	80	90	80	95
80	85	6	7	80	90	60	75	90	95	90	95	90	95
70	90	95	97	0	0	0	45	95	97	90	97	85	95
0	50	50	75	50	75	50	75	75	100	75	100	50	75
100	100	50	100	50	100	0	0	100	100	50	100	100	100
81	99	30	70	1	50	75	90	87	100	1	47	90	100
0	10	40	60	40	100	0	5	80	100	80	100	40	100
25	30	10	20	40	70	20	30	5	10	20	25	20	25
5	10	75	100	5	15	75	100	75	100	75	100	75	100

EK-3. Matlab rastgele sayı üreteci ile hazırlanmış sentetik veri tablosu

	A		B		C		D		E		A1		B1	
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
Denek1	12	15	21	21	21	23	11	23	20	42	22	23	52	61
Denek2	9	10	21	25	32	33	24	37	26	32	17	24	56	66
Denek3	10	11	21	23	15	32	26	37	33	42	20	26	70	73
Denek4	5	14	21	23	29	30	14	35	28	46	16	19	65	70
Denek5	7	13	22	23	20	24	20	37	22	33	24	27	58	75
Denek6	5	14	20	24	19	30	24	26	46	48	18	25	60	60
Denek7	11	13	20	24	16	21	32	35	34	45	24	26	56	67
Denek8	6	12	20	23	26	33	28	32	34	37	17	29	62	74
Denek9	9	14	23	24	20	27	20	28	34	41	21	21	54	80
Denek10	9	11	21	23	20	33	36	39	22	46	26	29	53	75
Denek11	13	14	20	24	17	22	30	40	23	36	24	27	50	67
Denek12	10	11	22	25	27	27	33	39	27	39	20	25	53	55
Denek13	7	10	21	22	22	35	26	34	27	47	16	26	54	75
Denek14	9	14	20	22	28	29	20	29	20	26	17	18	76	77
Denek15	10	13	22	25	21	24	14	19	35	39	20	27	69	78
Denek16	8	12	20	22	21	30	21	30	29	44	17	25	52	59
Denek17	7	11	21	25	15	23	25	29	28	40	19	26	57	60
Denek18	7	9	22	24	21	21	11	34	20	21	20	25	64	73
Denek19	7	12	22	25	21	21	19	37	20	42	19	28	55	75
Denek20	12	13	21	23	24	29	38	39	28	46	16	28	51	75
Denek21	6	7	24	24	23	24	15	31	25	45	19	28	51	70
Denek22	11	14	22	23	27	34	12	27	38	39	18	20	55	70
Denek23	6	14	24	24	30	30	11	19	25	47	15	27	54	64
Denek24	10	12	20	25	18	33	13	24	29	46	16	22	60	71
Denek25	6	8	21	24	24	31	10	12	21	44	23	28	73	77
Denek26	8	11	22	23	17	21	29	33	40	49	25	28	57	67
Denek27	8	9	20	24	23	24	38	39	25	45	16	30	52	67
Denek28	10	12	21	21	18	20	21	34	31	33	16	22	66	79
Denek29	5	7	23	25	18	25	20	31	43	49	20	25	68	74
Denek30	6	7	24	24	22	31	29	39	27	33	19	21	55	70

EK-3. (devam) Matlab rastgele sayı üreteci ile hazırlanmış sentetik veri tablosu

C1		D1		E1		J		K		L		M		N	
Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
22	23	11	23	20	28	7	10	41	58	33	34	22	22	20	36
22	29	24	37	26	30	9	12	47	49	31	32	20	21	27	31
22	28	26	37	22	23	6	11	49	56	33	35	21	22	27	37
22	30	14	35	23	24	9	14	43	49	31	34	20	24	33	39
25	27	20	37	22	29	8	10	41	49	35	35	22	25	16	34
25	27	24	26	26	27	5	5	42	47	33	34	20	21	32	33
21	28	32	35	20	27	6	11	51	57	32	32	22	23	37	40
27	28	28	32	24	29	12	14	50	54	31	33	20	21	27	33
22	30	20	28	23	26	5	9	52	53	33	33	23	24	17	30
20	24	36	39	21	26	6	7	45	50	31	35	20	25	37	39
24	28	30	40	24	25	11	14	48	58	31	35	22	24	24	32
20	21	33	39	22	26	8	13	47	54	32	35	21	24	24	38
24	25	26	34	22	29	11	14	56	59	32	34	20	22	26	27
26	29	20	29	20	24	11	13	45	57	33	35	21	23	17	19
23	27	14	19	25	29	8	14	44	45	31	33	24	24	16	36
22	24	21	30	22	26	6	12	40	42	31	34	23	23	18	21
22	24	25	29	21	24	8	12	53	55	32	33	20	24	17	17
22	30	11	34	21	27	9	12	55	58	31	34	21	22	20	25
22	28	19	37	20	21	8	11	43	56	31	34	22	24	28	36
24	28	38	39	23	28	5	6	43	48	30	33	24	25	19	35
25	29	15	31	21	27	13	14	42	50	31	34	21	22	19	30
21	27	12	27	28	29	12	13	41	50	31	32	20	25	24	35
23	24	11	19	21	24	11	14	47	52	32	34	21	24	19	26
20	29	13	24	21	22	11	14	46	48	32	32	20	22	24	40
27	30	10	12	21	27	6	8	54	57	34	35	24	25	15	19
25	29	29	33	23	30	11	13	47	50	31	34	23	23	15	16
28	29	38	39	26	26	7	10	46	56	31	35	20	20	16	37
22	29	21	34	26	26	8	10	56	59	32	34	23	25	33	38
23	28	20	31	28	30	9	12	46	47	31	33	24	25	28	39
22	26	29	39	23	24	9	13	42	46	32	35	23	24	23	35

EK-3. (devam) Matlab rastgele sayı üreteci ile hazırlanmış sentetik veri tablosu

O		P		R		S		T		U	
Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max
25	33	26	42	23	26	36	36	10	21	14	22
25	29	30	31	20	31	32	45	21	24	20	22
21	39	41	42	24	25	32	48	12	16	13	23
27	32	26	36	30	32	31	34	14	21	21	24
24	35	35	35	21	30	49	49	23	24	19	19
22	26	42	45	28	31	42	48	14	14	11	17
24	31	40	41	24	32	42	50	12	23	23	24
26	35	33	42	21	33	34	35	22	22	12	18
30	39	28	30	26	28	34	39	22	23	18	18
20	35	31	41	34	36	32	50	14	16	13	21
35	39	30	35	21	34	32	43	11	23	21	21
30	38	29	44	29	38	34	45	22	24	17	18
21	39	26	28	23	26	35	47	16	19	15	21
23	29	27	29	23	24	39	42	13	24	20	22
27	40	39	44	31	36	39	44	21	22	11	12
27	34	27	35	27	27	38	49	12	17	13	14
24	30	32	43	26	39	36	41	13	25	15	18
36	38	28	33	29	39	33	38	13	15	17	19
33	36	36	37	20	36	45	48	18	21	10	18
23	36	34	43	28	31	37	46	22	24	14	24
37	40	26	30	39	39	38	47	19	19	11	22
21	37	31	36	34	34	46	49	14	17	19	25
38	38	38	45	26	38	30	49	12	25	12	23
27	37	33	41	23	23	34	34	15	21	23	24
23	28	28	35	29	38	37	48	11	13	12	12
33	38	35	41	38	38	33	47	24	24	16	21
30	31	40	41	23	32	31	33	21	24	10	24
24	36	31	33	22	26	38	40	16	21	14	23
25	37	30	38	27	31	47	50	16	22	19	23
25	29	26	27	27	38	39	43	16	23	14	15

EK-4. Matlab kütüphaneleri

Aşağıdaki linkten indirilebilir

https://www.mathworks.com/matlabcentral/fileexchange/29006-functions-for-interval-type-2-fuzzy-logic-systems

EK-5. Coras Yazılımı

Coras yazılımı aşağıdaki linkten indirilebilir;

http://coras.sourceforge.net/coras_tool.html

EK-6 Literatür araştırması için yapılmış haritalar: konu hakkında yazılmış temel makalelerin sınıflandırılması

*Dijital kopya olarak verilmiştir.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: MURATOĞLU, Orhan
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 09.05.1979, Bolu
Medeni hali	: Evli
Telefon	: 0 (532) 418 08 07
Faks	: -
e-mail	: muratoglu.orhan@gmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Doktora	Gazi Üniversitesi /Kazalar	Devam ediyor
Yüksek lisans	Hoca Ahmet Yesevi / Bilgisayar Müh.	2010
Lisans	O.D.T.Ü / Fen Fak/Kimya	2006
Lise	Gerede Lisesi	1996

İş Deneyimi

Yıl	Yer	Görev
2016-Halen	TÜBİTAK BİLGEM	Başkan Yrd.
2013-2016	HAVELSAN A.Ş.	Genel Müdür Yrd.
2009-2013	TÜRK TELEKOM A.Ş.	İl Müdürü
2005-2009	Çözüm Bilgisayar A.Ş.	Kurumsal Satış uzmanı
2003-2005	CPM Kompitür Printer A.Ş.	Şirket Sahibi-Kurucu

Yabancı Dil

İngilizce

Yayınlar

Makaleler

Okul, Ş , Muratoğlu, O , Aydın, M , Bilge, H . (2019). *A Review on Cyber Risk Management. Acta Infologica ,* 3 (1) , 34-45 . DOI: 10.26650/acin.502589

Okul, Ş, Muratoğlu, O, Aydın, M, Bilge H., (2019). Security Attacks in V2V Communication, 1 (3), Milli Təhlükəsizlik və Hərbi Elmlər − National Security and Military Sciences 4 (4)/2018, 58-63

Konferanslar

Okul, Ş, Muratoğlu, O, Aydın, A.M, Bilge H.,, "*Review On Cyber Risks Relating to Security Management in Smart Cars*", International Computer Science and Engineering Conference, 20-23 September 2018, Saraybosna, Bosnia

Okul, Ş, Muratoğlu, O, Aydın, M, Bilge H., M. Aydın A., (2018) "*Comparison of Cyber Risks with Respect to Operational Risk in Terms of Assessment Methods*", 1st International Symposium on Graduate Research in Science, 4-6 October 2018, İstanbul, Turkey

Okul, Ş., Muratoğlu, O., Aydın, M. A., Bilge,H.B. (2018) "*A Review On Cyber Risk Management*", 1st International Symposium on Graduate Research in Science, 4-6 October 2018, İstanbul, Turkey

Muratoğlu, O. (2019, May 21). *Fuzzy Based Cyber Risk Management Approach for Smart Car. Seminar presented at the meeting of the Sıntef, Oslo, Norway.* -

Hobiler

Yüzme, Balık Tutma, Seyahat

GAZİ GELECEKTİR...