

**ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

YÜKSEK LİSANS TEZİ

**GEMİ SAVUNMA SİSTEMLERİNDE TEHDİT DEĞERLENDİRME VE SİLAH
ATAMA UYGULAMALARI**

Kerem KALCI

ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA

2008

Her hakkı saklıdır

TEZ ONAYI

Kerem KALCI tarafından hazırlanan “**Gemi Savunma Sistemlerinde Tehdit Değerlendirme ve Silah Atama Uygulamaları**” adlı tez çalışması 09.10.2008 tarihinde aşağıdaki jüri tarafından oy birliği ile Ankara Üniversitesi Elektronik Mühendisliği Anabilim Dalı’nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Yrd.Doç. Dr. Murat EFE

Jüri üyeleri:

Başkan: Yrd.Doç. Dr. Mehmet DEMİRER
Hacettepe Üniversitesi Elektrik ve Elektronik Mühendisliği Anabilim Dalı

Üye: Yrd.Doç. Dr. Murat EFE
Ankara Üniversitesi Elektronik Mühendisliği Anabilim Dalı

Üye: Yrd.Doç. Dr. Murat Hüsni SAZLI
Ankara Üniversitesi Elektronik Mühendisliği Anabilim Dalı

Yukarıdaki sonucu onaylarım

Prof. Dr. Orhan ATAOL
Enstitü Müdürü

ÖZET

Yüksek Lisans Tezi

GEMİ SAVUNMA SİSTEMLERİNDE TEHDİT DEĞERLENDİRME VE SİLAH ATAMA UYGULAMALARI

Kerem KALCI

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Elektronik Mühendisliği Anabilim Dalı

Danışman: Yrd. Doç. Dr. Murat EFE

Bu tezde, kaynak kullanımında optimizasyon konusu ele alınmıştır. Daha detaylı olarak ise deniz harbinin önemli unsurlarından gemi savunma sisteminin bir parçası olan tehdit değerlendirme ve silah atama sistemi incelenmiştir. Sistem adından da anlaşılacağı üzere iki ana bölümden oluşur. İlk bölüm algılanan tehdidin, savunulan gemi için oluşturduğu “öldürücülük (*lethality*)” değerinin hesaplandığı “tehdit değerlendirme” bölümüdür. İkinci bölüm ise; ilk bölümde elde edilen öldürücülük değerine göre geminin kendisini savunma amaçlı olarak, hangi silahların hangi sırayla kullanılmasının gerektiğini planlayan “silah atama” bölümüdür.

Tehdit değerlendirme bölümünde, algılanan tehdidin ihtiva ettiği özelliklere göre değerlendirilip, öldürücülük değerinin hesaplanabilmesi için üç farklı algoritma (Bayes Çıkarımı, Dempster – Shafer Teorisi, Transfer Edilebilir İnanış Modeli), operatörün kullanımına sunulmuştur. Bu üç algoritmanın da çalışma prensipleri farklı olduğu için, aynı özelliklere sahip tehdit algılamalarında hesaplanan öldürücülük değerleri farklı olabilmektedir. Bu algoritmaların temelleri ve silah atama sistemi içerisinde kullanım şekilleri MATERYAL VE YÖNTEM bölümünde detaylı olarak ele alınmıştır.

Sistemin ikinci bölümü olan silah atama bölümünde ise, minimum sistem kaynağı kullanımıyla, en başarılı biçimde tehdidin bertaraf edilmesini sağlayan silah atama algoritması çalıştırılır ve olabilecek en optimize çözümü operatörün kullanımına sunar. Silah atama algoritmasının çalışma şekli MATERYAL VE YÖNTEM bölümünde detaylı olarak açıklanmıştır.

İlk bölümde kullanılabilecek olan üç farklı algoritma, birbirlerinden farklı öldürücülük değerleri ürettiği için, her algoritmanın sisteme maliyeti birbirinden farklı olabilmektedir. Burada başarı kriteri en az maliyetle algılanan tehdidin bertaraf edilmesidir.

Ekim 2008, 67 sayfa

Anahtar Kelimeler: Tehdit Değerlendirme ve Silah Atama, Gemi Savunma Sistemleri, Bayes Çıkarımı, Dempster – Shafer Teorisi, Transfer Edilebilir İnanış Modeli

ABSTRACT

Master Thesis

THREAT EVALUATION AND WEAPON ASSIGNMENT APPLICATIONS IN NAVAL DEFENSE SYSTEMS

Kerem KALCI

Ankara University
Graduate School of Natural and Applied Sciences
Department of Electronics Engineering

Supervisor: Asst. Prof. Dr. Murat EFE

Detected threats and their lethality for a defending naval vehicle were studied. Three different algorithms (Bayesian Inference, Dempster – Shafer Theory, Transferable Belief Model) were used. Since these three algorithms work different, they produced different results for detected threats comprising same features. In order to evaluate and compare these results different results, a variable called “lethality” was defined. All algorithms worked in its own way and evaluated the detected threat, then produced a “lethality” value for that threat. Evaluation of lethality was the first part of naval defense system. The success criterion in the first part of the system was the time duration which each algorithm required to evaluate the threat. In the second part of the system, if the produced lethality value was bigger than a threshold value, the defending naval vehicle started weapons assignment algorithm against the detected threat, in order to defend itself and defeat the threat with minimum resource consumption. Success criterion of the whole system was the resource consumption of the system for defeating the threat. Since lethality value depended on the algorithm type which were used in the first part of the system (each algorithm might have produced different lethality values), choice of the algorithm affected the resource consumption.

October 2008, 67 pages

Key Words: Threat Evaluation and Weapons Assignment (TEWA), Naval Defense Systems, Bayesian Inference, Dempster – Shafer Theory, Transferable Belief Model

TEŞEKKÜR

Çalışmalarımın her aşamasında beni destekleyen danışmanım Yrd. Doç. Dr. Murat EFE' ye ve aileme teşekkür ederim.

Kerem KALCI
Ankara, Ekim 2008

İÇİNDEKİLER

ÖZET	i
ABSTRACT	ii
TEŞEKKÜR.....	iii
SİMGELER DİZİNİ.....	vi
ŞEKİLLER DİZİNİ.....	vii
ÇİZELGELER DİZİNİ	viii
1. GİRİŞ.....	1
2. KURAMSAL TEMELLER	3
2.1 Sistem Tanımı.....	3
2.2 Sistemin Kullanılabileceği Platformlar	4
2.3 Deniz Harp Tipleri ve Savunma Amaçlı Kullanılabilecek Silahlar	4
2.3.1 Hava savunma harbi	4
2.3.2 Su üstü savunma harbi.....	5
2.4 Tehdit Modelleri.....	5
2.4.1 Su üstü kaynaklı tehdit modelleri.....	5
2.4.2 Hava kaynaklı tehdit modelleri	6
2.5 Angajman Kuralları.....	6
2.6 Silah Modelleri	7
3. MATERYAL VE YÖNTEM.....	8
3.1 Tehdit Değerlendirmede Kullanılan Algoritmaların Temelleri	8
3.1.1 Bayes çıkarımı	8
3.1.1.1 Bayes Kuralı (<i>Bayes Rule</i>).....	8
3.1.1.2 Bayes ağı (<i>Bayesian network</i>)	9
3.1.1.3 Bayes çıkarımı (örnek – 1)	10
3.1.1.4 Bayes çıkarımı (örnek – 2)	11
3.1.2 Dempster – Shafer teorisi.....	13
3.1.2.1 Dempster Birleştirme Kuralı	14
3.1.2.2 Dempster – Shafer teorisi (örnek – 1).....	15
3.1.2.3 Dempster – Shafer teorisi (örnek – 2).....	16
3.1.3 Transfer Edilebilir İnanış Modeli.....	17
3.1.3.1 Transfer edilebilir inanış modeli (örnek) (Elouedi <i>et al.</i> 2004).....	18

3.2 Değerlendirme Algoritmalarının Silah Atama Sisteminde Kullanımı ve Sistemin Çalışma Prensipleri.....	20
3.2.1 Tehdit değerlendirme ve silah atama sisteminin çalışma prensipleri	20
3.2.2 Bayes çıkarımı yöntemiyle öldürücülük değeri hesaplanması	25
3.2.3 Dempster – Shafer teorisi uygulanarak öldürücülük değeri hesaplanması	30
3.2.4 Transfer edilebilir inanış modeli uygulanarak öldürücülük değeri hesaplanması	35
3.2.5 Silah atama sistemi.....	40
3.2.6 Tehdit değerlendirme algoritmalarının karşılaştırılması	46
4. BULGULAR.....	47
4.1 Algoritmalarda aynı tipte tehdit modellerinin kullanılması.....	47
4.1.1 Bayes Çıkarımı kullanıldığında sistemin çıktısı.....	48
4.1.2 Dempster – Shafer teorisi kullanıldığında sistemin çıktısı	51
4.1.3 Transfer edilebilir inanış modeli kullanıldığında sistemin çıktısı	54
4.2 Algoritmalarda farklı tipte tehdit modellerinin kullanılması	58
4.2.1 Dempster – Shafer teorisinin avantajları	58
4.2.2 Transfer edilebilir inanış modeli algoritmasının avantajları	59
5. TARTIŞMA ve SONUÇ	61
5.1 Tartışma	61
5.2 Sonuç	63
KAYNAKLAR.....	65
ÖZGEÇMİŞ.....	67

SİMGELER DİZİNİ

DSS	Decision Support System
ECM	Electronic Counter Measures
ESM	Electronic Support Measures
SAM	Surface-to-air missile
SSM	Surface-to-surface missile
TEWA	Threat Evaluation and Weapons Assignment
DST	Dempster – Shafer Theory
TBM	Transferable Belief Model

ŞEKİLLER DİZİNİ

Şekil 2.1 Tehdit Değerlendirme ve Silah Atama Sisteminin Angajman Sürecindeki Yeri (Huang and Kar 1994)	3
Şekil 2.2 Sistemin Kullanılabileceği Örnek Bir Platform (Firkateyn)	4
Şekil 2.3 Gemi Savunma Sistemlerinde Kullanılan Silahlardan GÜdümlü Füze	5
Şekil 2.4 Gemi Savunma Sistemlerinde Kullanılan Silahlardan Güverte Topu	5
Şekil 2.5 Hava Kaynaklı Tehdit unsuru: F16-C Savaş Uçağı	6
Şekil 3.1 Bayes Ağı: örnek – 1 (Das 1999).....	10
Şekil 3.2 Gözlemlerden Önce Değişkenlerin Olasılıkları (rain = yağmur, sprinkler = fiskiye, grass = çimen).....	12
Şekil 3.3 Gözlemlerle Güncellenmiş Olasılıklar	13
Şekil 3.4 Sistemin genel akış diyagramı	24
Şekil 3.5 Algılanan tehdidin özelliklerine göre oluşturulan Bayes Ağı	25
Şekil 3.6 Dempster – Shafer Teorisinde kullanılan ağ yapısı	31

ÇİZELGELER DİZİNİ

Çizelge 3.1 Yağmur Yağmasının Marjinal olasılığı	11
Çizelge 3.2 Fıskiye'nin Çalışmasının Yağmura Koşullu Olasılığı.....	11
Çizelge 3.3 Çimenlerin Islak Olmasının Yağmura ve Fıskiye'ye Koşullu Olasılığı.....	11
Çizelge 3.4 Alt Küme – Kütle değerleri (örnek – 1)	14
Çizelge 3.5 Alıcılardan Gelen Kütle Verileri (Koks 2003).....	16
Çizelge 3.6 S_1 alıcısının inanış kütleleri değerleri (Elouedi <i>et al.</i> 2004).....	19
Çizelge 3.7 S_2 alıcısının inanış kütleleri değerleri (Elouedi <i>et al.</i> 2004).....	19
Çizelge 3.8 S_1 alıcısı için hesaplanan BetP değerleri (Elouedi <i>et al.</i> 2004).....	20
Çizelge 3.9 Algılanan tehdide ait verilerin saklandığı hafıza yapısı	21
Çizelge 3.10 Bayes Çıkarımı ve TBM'de değişken değerleri.....	22
Çizelge 3.11 Dempster – Shafer Teorisinde değişken değerleri	22
Çizelge 3.12 $P(position lethal)$ için eşleştirme tablosu	27
Çizelge 3.13 Algılanan tehditlerin özellikleri	28
Çizelge 3.14 Pozisyon değişkeni için alıcı değeri – DST tanım değeri eşleme fonksiyonu	33
Çizelge 3.15 Algılanan tehditlerin özellikleri	34
Çizelge 3.16 Devinim değişkeninin altkümeleri	36
Çizelge 3.17 Devinim için temel inanış kütleleri değer dağılımı	37
Çizelge 3.18 Satış kaynaklı tehdit için örnek karşı etkinlik tablosu	42
Çizelge 3.19 Hava kaynaklı tehdit için örnek karşı etkinlik tablosu	42
Çizelge 3.20 Kullanılan silahlara ait maliyet tablosu	46
Çizelge 4.1 Algılanan tehditlerin özellikleri	47
Çizelge 4.2 Dempster – Shafer teorisi için belirsizlik örneği	58

1. GİRİŞ

Silah sistemlerinde varolan kaynakları belirlemek ve doğru yer ve zamanda kullanımlarını sağlamak büyük önem taşımaktadır. Son dönemlerde, radar, güdüm ve haberleşme teknolojilerinin gelişmesiyle birlikte tehdit unsurlarının zarar verebilme yetenekleri de artmıştır. Buna paralel olarak ise, tehdide angaje olabilmek ve tehdidi bertaraf edebilmek için gerekli olan zaman aralığı kısalmıştır. Ayrıca; platformlar üzerinde bulunan savunma amaçlı silah ve cephaneler sınırlı sayıda ve farklı özelliktedirler. Bunlara bağlı olarak ortaya çıkan sonuç ise; yüksek yoğunluklu tehdit ortamlarında, kısa zaman aralıklarının en verimli şekilde değerlendirilebilmesi için tehditler ile bunlara karşı kullanılabilir silahları ve cephaneleri çok kısa zaman aralıklarında analiz edebilen ve uygun savunma stratejisini belirlemeye yardım eden bir karar destek sistemine (*Decision Support Sistem*) ihtiyaç duyulmasıdır (Chalmers 1993). Bu sistem tehdit değerlendirme ve silah atama sistemi (*Threat Evaluation and Weapon Assignment System - TEWA*) olarak adlandırılır.

Bu tezde, kaynak kullanımında optimizasyon konusu ele alınmıştır. Daha detaylı olarak ise deniz harbinin önemli unsurlarından gemi savunma sisteminin bir parçası olan tehdit değerlendirme ve silah atama sistemi incelenmiştir. Sistem adından da anlaşılacağı üzere iki ana bölümden oluşur. İlk bölüm algılanan tehdidin, savunulan gemi için oluşturduğu “öldürücülük (*lethality*)” değerinin hesaplandığı “tehdit değerlendirme” bölümüdür. İkinci bölüm ise; ilk bölümde elde edilen öldürücülük değerine göre geminin kendisini savunma amaçlı olarak, hangi silahların hangi sırayla kullanılmasının gerektiğini planlayan “silah atama” bölümüdür.

Tehdit değerlendirme bölümünde, algılanan tehdidin ihtiva ettiği özelliklere göre değerlendirilip, öldürücülük değerinin hesaplanabilmesi için üç farklı algoritma (Bayes Çıkarımı, Dempster – Shafer Teorisi, Transfer Edilebilir İnanış Modeli), operatörün kullanımına sunulmuştur. Bu üç algoritmanın da çalışma prensipleri farklı olduğu için, aynı özelliklere sahip tehdit algılamalarında hesaplanan öldürücülük değerleri farklı olabilmektedir. Bu algoritmaların temelleri ve silah atama sistemi içerisinde kullanım şekilleri MATERYAL VE YÖNTEM bölümünde detaylı olarak ele alınmıştır.

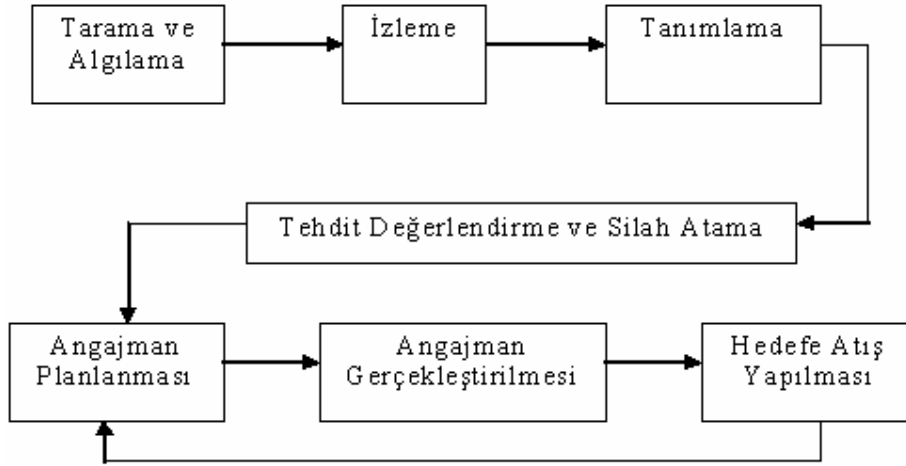
Sistemin ikinci bölümü olan silah atama bölümünde ise, minimum sistem kaynağı kullanımıyla, en başarılı biçimde tehdidin bertaraf edilmesini sağlayan silah atama algoritması çalıştırılır ve olabilecek en optimize çözümü operatörün kullanımına sunar. Silah atama algoritmasının çalışma şekli MATERYAL VE YÖNTEM bölümünde detaylı olarak açıklanmıştır.

İlk bölümde kullanılabilecek olan üç farklı algoritma, birbirlerinden farklı öldürücülük değerleri ürettiği için, her algoritmanın sisteme maliyeti birbirinden farklı olabilmektedir. Burada başarı kriteri en az maliyetle algılanan tehdidin bertaraf edilmesidir.

2. KURAMSAL TEMELLER

2.1 Sistem Tanımı

Tehdit değerlendirme ve silah atama, algılanan tehditleri belirli kriterlere göre değerlendirerek, kullanılabilir kaynakların (aktif ve pasif silahlar) en optimize şekilde, savunma amaçlı olarak kullanılmasını koordine eden gerçek zamanlı bir karar destek sistemidir.



Şekil 2.1 Tehdit Değerlendirme ve Silah Atama Sisteminin Angajman Sürecindeki Yeri (Huang and Kar 1994)

Şekil 2.1’de görüldüğü üzere angajman süreci; tarama, algılama, izleme, tanımlama, tehdit değerlendirme, silah atama, angajman planlaması ve yürütmesi, ve son olarak ta hedefe atış yapılması işlemlerinden oluşur. Bu işlemlerin tamamı çok kısa zaman aralıklarında ve yüksek gerilimli bir ortamda yapılır. Bu nedenle angajman sürecinde; tehditlerin değerlendirilmesi, kullanılacak silahların belirlenmesi, ve angajmanın planlanması işlemleri ne kadar hızlandırılırsa, savunulan platformun isabet almama olasılığı o kadar artar. Angajman planlamasından atış işleminin sonuna kadar olan döngü, karşılaşılan tüm tehditler tam anlamıyla bertaraf edilinceye kadar tekrarlanır.

2.2 Sistemin Kullanılabileceği Platformlar

Tehdit Değerlendirme ve Silah Atama sistemi çeşitli deniz platformları üzerinde kullanılabilir. Bunlara örnek olarak, firkateyn (Şekil 2.2), muhrip ve hücum bot gösterilebilir. Platform seçiminde önemli olan nokta; seçilen platformun, sistemin angajman için kullanacağı silah sistemlerine sahip olmasıdır.



Şekil 2.2 Sistemin Kullanılabileceği Örnek Bir Platform (Firkateyn)¹

2.3 Deniz Harp Tipleri ve Savunma Amaçlı Kullanılabilecek Silahlar

2.3.1 Hava savunma harbi

Hava savunma harbi; havadan gelebilecek tehditlere karşı yapılan harp tipidir. Amaç, havadan gelebilecek tehditlere karşı savunma hattı oluşturmaktır. Savunma silahı olarak, flare, satıhtan havaya güdümlü füze (*surface-to-air missile - SAM*) (Şekil 2.3) güverte topu (Şekil 2.4) veya makineli tüfek kullanılır.

¹ Resim dosyası Türkiye Cumhuriyeti Deniz Kuvvetleri Komutanlığı'nın Internet sayfasından (<http://www.dzkk.tsk.mil.tr/>) alınmıştır. Şekil 2.3 ve Şekil 2.4 için de aynı durum geçerlidir.

2.3.2 Su üstü savunma harbi

Su üstü savunma harbi; yüzen araçlardan gelebilecek tehditlere karşı yapılan harp tipidir. Amaç, sudan gelebilecek tehditlere karşı savunma hattı oluşturmaktır. Savunma silahı olarak, sathıtan sathiha güdümlü füze (*surface-to-surface missile - SSM*) (Şekil 2.3), güverte topu (Şekil 2.4) veya makineli tüfek kullanılır.



Şekil 2.3 Gemi Savunma Sistemlerinde Kullanılan Silahlardan Güdümlü Füze



Şekil 2.4 Gemi Savunma Sistemlerinde Kullanılan Silahlardan Güverte Topu

2.4 Tehdit Modelleri

2.4.1 Su üstü kaynaklı tehdit modelleri

Su üstü kaynaklı tehdit modelleri, askeri unsurlar, sivil taşımacılık ve ticari unsurlar olarak üç alt başlıkta incelenebilir. Askeri unsurlar; bölüm 2.2’de bahsedilen fırkateyn, muhrip ve hücum botun yanı sıra mayın tarama, mayın avlama, uçak gemisi, çıkarma

gemisi olarak çeşitlendirilebilir. Sivil taşımacılıktan kasıt ise yolcu gemileri ve bireylere ait özel deniz araçlarıdır. Bunların yanında, ticari deniz araçları olan tankerler, yük gemileri ve balıkçı gemileri de tehdit modellerine dahil edilebilir.

2.4.2 Hava kaynaklı tehdit modelleri

Hava kaynaklı tehdit modelleri, askeri unsurlar ve sivil hava taşımacılığı olarak iki ayrı bölümde incelenebilir. Askeri unsurlar; savaş uçakları (Şekil 2.5), bombardıman uçakları, keşif uçakları, saldırı helikopterleri ve gözetleme helikopterleri olarak sınıflandırılırken; sivil hava taşımacılığı ise yolcu uçakları, nakliye uçakları ve bireylere ait özel hava araçları olarak kategorilere ayrıştırılabilir.



Şekil 2.5 Hava Kaynaklı Tehdit Unsuru: F16-C Savaş Uçağı²

2.5 Angajman Kuralları

Askeri ya da polisiye bir operasyonda kuvvetin (aktif veya pasif silahların) ne zaman, nerede ve nasıl kullanılacağını düzenleyen kurallardır (USDOD 2003). Hızlı ve doğru karar verilebilmesi için operasyon öncesinde açıkça, tereddüt yaratmayacak şekilde tanımlanmalıdırlar.

² Resim dosyası Türkiye Cumhuriyeti Hava Kuvvetleri Komutanlığı'nın Internet sayfasından (<http://www.hvkk.tsk.mil.tr/>) alınmıştır.

2.6 Silah Modelleri

Savunma sisteminde kullanılabilecek silahlar, savunma amaçlı (*soft-kill*) silahlar ve öldürücü (*hard-kill*) silahlar olarak ikiye ayrıştırılabilir.

Chaff, flare, ve decoy savunma amaçlı (*soft-kill*) silahlardır. Bu tip silahların, kısa sürede kullanıma hazır hale gelmeleri, maliyetlerinin daha ucuz olması, çok miktarda bulundurulabilmeleri ve hataları affeder yapıda olmaları gibi avantajları vardır. Bu avantajlarının yanında, kesin sonuç sağlamamaları gibi azımsanmayacak bir dezavantajları da bulunmaktadır (Huang and Kar 1994).

Güdümlü füze, top, gibi silahlar, öldürücü (*hard-kill*) silahlar olarak adlandırılırlar. Atışa hazırlanmalarının uzun sürmesi, maliyetin yüksek olması, boyutları sebebiyle sınırlı sayıda bulundurulabilmeleri, kullanılabilmesi için hedef hakkında çok ayrıntılı bilgiye gereksinim duyması gibi birçok dezavantajları bulunan bu silahların tek avantajı tehdide karşı kesin çözüm sağlamalarıdır ki, sırf bu özellikleri yüzünden vazgeçilemezler (Huang and Kar 1994).

3. MATERYAL VE YÖNTEM

3.1 Tehdit Değerlendirmede Kullanılan Algoritmaların Temelleri

Bu çalışmada Tehdit Değerlendirme ve Silah Atama sisteminin tehdit değerlendirme kısmında çalışma şekilleri birbirinden farklı üç değişik algoritma incelenmiştir. Bu algoritmalar Bayes Çıkarımı (*Bayesian Inference*), Dempster – Shafer Teorisi (*Dempster – Shafer Theory*), ve Transfer Edilebilir İnanış Modeli (*Transferable Belief Model*) olarak sıralanabilir. Bu algoritmaların Tehdit Değerlendirme ve Silah Atama Sistemi içerisinde nasıl görev yaptıklarının anlaşılabilmesi için öncelikle bu algoritmaların temellerinin bilinmesi gerekmektedir. Bu bölümde, bu algoritmalarla ilgili temel bilgiler, örnekler ve bu algoritmaların Tehdit Değerlendirme ve Silah Atama Sisteminde kullanılış şekilleri detaylı olarak ele alınmıştır.

3.1.1 Bayes çıkarımı

Bir olasılığı; kanıtlar veya gözlemler kullanarak güncelleyen istatistiksel çıkarım metoduna Bayes Çıkarımı denir. Bayes Çıkarımı, ismini, çıkarım süreci boyunca Bayes Kuralının (3.1.1.1) çok sık olarak kullanılmasından almıştır. En büyük avantajı, olasılık değerlerini, operasyon süreci boyunca elde edilen veriler ışığında, gerçek zamanlı olarak güncelleyebilmesidir. Bayes Çıkarımına dahil olan değişkenler arasındaki ilişki grafiksel olarak ifade edilebilir; ve bu grafik ifade sonucunda da Bayes Ağı (*Bayesian Network*) (3.1.1.2) elde edilmiş olur.

3.1.1.1 Bayes Kuralı (*Bayes Rule*)

Bayes Kuralı, olasılık teorisi içinde, rasgele değişkenlerin marjinal olasılıklarıyla koşullu olasılıkları arasındaki bağlantıyı sağlayan bir araçtır. Bayes Kuralı Denklem 3.1'deki gibi gösterilir. Bu denklemdeki öğelerin özel isimleri vardır; $P(A)$, A'nın önsel olasılığıdır (*prior probability*), B değişkeni ile ilgili bir bilgi elde edilmeden önce A hakkında elde var olan bilgi olarak da nitelendirilir; $P(B)$, B'nin marjinal olasılığıdır yani B değişkeninin alabileceği değerler kümesinin herhangi bir elemanının olma olasılığıdır; $P(B|A)$, koşullu olasılık olarak isimlendirilir, A değişkeninin kesin olarak aldığı bir değer için B'nin olma olasılığıdır, bu değere aynı zamanda olabilirlik

(*likelihood*) fonksiyonu da denir; $P(A|B)$, B'nin kesin olduğu durumda A'nın sonsal olasılığıdır (*posterior probability*).

$$P(A|B) = \frac{P(B|A) \times P(A)}{P(B)} = \frac{P(A, B)}{P(B)}$$

Bayes Kuralı

Denklem (3.1)

3.1.1.2 Bayes ağı (*Bayesian network*)

Bayes ağı, Bayes çıkarımına dahil olan değişkenler arasındaki ilişkiyi gösteren grafik modeldir. Bu grafikte, değişkenler arası ilişkiler için yapılan varsayımlar, değişkenlerin marjinal ve koşullu olasılıkları gibi bilgiler açıkça belirtilir. Ağ içinde A değişkeninden B değişkenine doğru bir ok var ise “B, A’ya bağlıdır” veya “A, B’nin atasıdır” denir.

Bayes ağı’nı oluşturabilmek için ilk önce bir hipotez değişkeni belirlenir. Komuta – Kontrol sistemlerinde bu hipotez değişkeni genellikle, algılanan tehdit unsurunun “niyetidir”. Daha sonra bu “niyetin” belirlenmesinde etkin rol oynayacak olan kanıt/gözlem değişkenleri belirlenir. Eğer gerekliyse, kanıt/gözlem değişkenleriyle, hipotez değişkeninin bağlantısını sağlayan ara seviye değişkenlerin belirlenmesinin ardından, değişkenlerin marjinal ve koşullu olasılıkları kararlaştırılır. Bu koşullu olasılık değerlerine karar verilirken, ölçülebilir/gözlemlenebilir (objektif) veriler kadar, geçmiş tecrübeler ve sezgiler gibi sübjektif veriler de göz önüne alınır. Herhangi bir Bayes Ağında, değişkenlerin birleşik olasılıkları (*joint probability*), Denklem 3.2’de de görüldüğü üzere, her bir değişkenin, atalarına bağlı olan koşullu olasılıklarının çarpımıdır. Hipotez değişkeninin bir atası bulunmadığı için koşullu yerine koşulsuz olasılığı dikkate alınır.

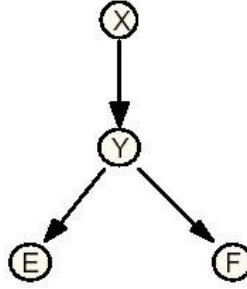
$$P(X_1, \dots, X_n) = \prod_{i=1}^n P(X_i | ATA(X_i))$$

Bayes Ağında Değişkenlerin Birleşik Olasılıkları

Denklem (3.2)

3.1.1.3 Bayes çıkarımı (örnek – 1)

Şekil 3.1’deki gibi oluşturulmuş bir Bayes ağında; E kanıt/gözlem değişkeninin e_1 ve F kanıt/gözlem değişkeninin f_1 değerlerini aldığı durumda; bu bilgilerin X hipotez değişkeni üzerindeki etkileri Bayes Çıkarımı metoduyla incelenebilir.



Şekil 3.1 Bayes Ağı: örnek – 1 (Das 1999)

Burada X değişkeni tehdidin niyeti, Y değişkeni tehdidin aktivitesi, E ve F değişkenleri de sırasıyla tehlide ait konum ve hareket gözlemleri olarak düşünülebilir. X değişkeninin spesifik bir değerinin, E ve F değişkenlerinin sırasıyla e_1 ve f_1 değerlerine göre koşullu olasılığı bulunurken, e_1 , f_1 ve x_i değerleri sabit kabul edilip, sadece Y’nin değişken olduğu düşünülerek değişkenlerin birleşik olasılığı hesaplanır. Daha sonra e_1 ve f_1 değerleri sabit, hem X hem de Y değişken kabul edilerek, değişkenlerin birleşik olasılığı tekrar hesaplanır. Bu bulunan değerlerden ilkinin, ikincisine oranı, X değişkeninin spesifik bir değerinin koşullu olasılığını verir. Bu sürecin formül olarak ifadesi Denklem 3.3’teki gibidir.

$$P(x|e_1, f_1) = \frac{\sum_y P(f_1|y) \times P(e_1|y) \times P(y|x) \times P(x)}{\sum_{x,y} P(f_1|y) \times P(e_1|y) \times P(y|x) \times P(x)}$$

X Değişkeninin, e_1 ve f_1 'e Bağlı Koşullu Olasılık Fonksiyonu

Denklem (3.3)

3.1.1.4 Bayes çıkarımı (örnek – 2)

Bayes Ağları ile ilgili araştırma yapıldığı zaman, birçok kaynakta aynı örneklerle karşılaşılmaktadır; bu örnekte yağmur, fıskiye, çimen örneğidir. Kısaca açıklamak gerekirse, çimenlerin ıslak olduğu şeklinde bir gözlem yapılabilmesi için üç seçenek vardır; sadece yağmur yağabilir, sadece fıskiye çalışabilir veya yağmur yağıyorken fıskiye çalışabilir. Bu problemde 3 adet değişken vardır. Bu değişkenlerin marjinal ve koşullu olasılık değerleri, Çizelge 3.1, Çizelge 3.2 ve Çizelge 3.3'teki gibidir ve bu değerler kısmen ölçülmüş (objektif), kısmen de geçmiş tecrübelerle dayanarak (sübjektif) belirlenmiştir.

Çizelge 3.1 Yağmur Yağmasının Marjinal olasılığı

Yağmur Yağıyor	
Doğru	Yanlış
0.20	0.80

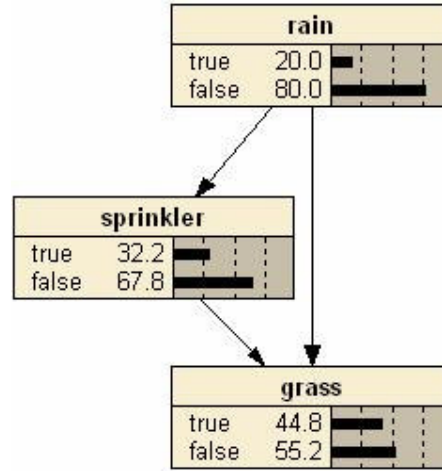
Çizelge 3.2 Fıskiyenin Çalışmasının Yağmura Koşullu Olasılığı

		Fıskiye Çalışıyor	Fıskiye Çalışmıyor
Yağmur Yağıyor	Doğru	0.01	0.99
	Yanlış	0.40	0.60

Çizelge 3.3 Çimenlerin Islak Olmasının Yağmura ve Fıskiyeye Koşullu Olasılığı

				Çimenler Islak	Çimenler Kuru
Yağmur Yağıyor	Doğru	Fıskiye Çalışıyor	Yanlış	0.80	0.20
	Yanlış			0.00	1.00
	Doğru	Fıskiye Çalışmıyor	Doğru	0.99	0.01
	Yanlış			0.90	0.10

Herhangi bir gözlem yapılmadan önce, tablolarda verilen dağılımlara göre, değişkenlerin olasılıkları Şekil 3.2’deki gibidir. Şekil 3.2’deki değerler, genel formülün (Denklem 3.2) bu probleme uyarlanması ve tablolarda verilen değerlerin, uyarlanmış formülde yerine koyulmasıyla elde edilir. Genel formülün bu probleme uygulanmış hali Denklem 3.4’te görülebilir.



Şekil 3.2 Gözlemlerden Önce Değişkenlerin Olasılıkları (rain = yağmur, sprinkler = fiskiye, grass = çimen)

$$P(\zeta, f, y) = P(\zeta|f, y) \times P(f|y) \times P(y)$$

Genel Formülün Örnek – 2’ye Uyarlanmış Hali (y=yağmur, f=fiskiye, ç=çimen)

Denklem (3.4)

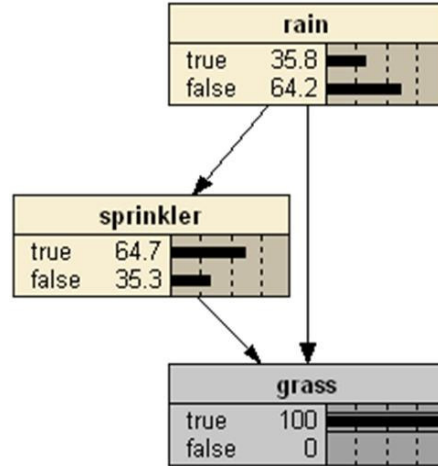
Yapılan gözlem sonucunda, çimenlerin ıslak olduğu belirlendiğine göre, bu gözlem doğrultusunda yağmurun yağıp yağmadığı hakkında nasıl bir yorum yapılabilir. Bayes ağlarının genel formülünde elde edilen veriler yerine koyulur. Bu örnekte çimlerin ıslak olduğu kesin olarak gözlemlendiğine göre “çimenler” değişkeninin her zaman “doğru (*true*)” olduğu bellidir. Üzerinde yorum yapılması istenen ise “yağmur” değişkeninin “doğru (*true*)” olup olmadığıdır. Verilen ve istenen, bir araya getirildiğinde Denklem 3.5 elde edilir.

$$P(y = \text{dogru} | \zeta = \text{dogru}) = \frac{P(y = \text{dogru}, \zeta = \text{dogru})}{P(\zeta = \text{dogru})} = \frac{\sum_{fiskiy e} P(\zeta = \text{dogru}, f = ?, y = \text{dogru})}{\sum_{fiskiy e, yagmur} P(\zeta = \text{dogru}, f = ?, y = ?)}$$

Elde edilen Gözlemin Genel Formülde Kullanılışı (y=yağmur, f=fıskiye, ç=çimen)

Denklem (3.5)

Denklem 3.4, Denklem 3.5'te yerine koyulur; ve tablolardaki koşullu olasılık değerleri de yeni formülde yerine koyulmak suretiyle değişkenlerin güncellemeleri tamamlanır ve yeni olasılık değerleri Şekil 3.3'teki gibi elde edilir.



Şekil 3.3 Gözlemlerle Güncellenmiş Olasılıklar

Gelinen son durum yorumlanırsa; başlangıçta hiçbir gözlem yapılmamışken %20 olan yağmurun yağıyor olma olasılığı, çimlerin ıslak olduğu şeklinde bir gözlem yapıldıktan sonra %35.8 değerine ulaştığı hesaplanıyor, ki; zaten çimlerin ıslak olduğu bir durumda yağmur yağıyor olması, beklenen sonuçlardan biridir.

3.1.2 Dempster – Shafer teorisi

Dempster – Shafer teorisi (DST), temelde Bayes çıkarımı ile ortak özelliklere sahiptir. Her iki algoritmada da, ilk olarak, sistemdeki değişkenlere/durumlara ağırlık değerleri

atanır. Bayes çıkarımında bu ağırlıklar, klasik anlamda “olasılık” olarak; Dempster – Shafer Teorisinde ise “kütle” (*mass*) olarak adlandırılırlar. Dempster – Shafer teorisinin, Bayes çıkarımından en büyük farkı değişkenlere kesin bir değer verilmesi gerekliliğinin olmamasıdır. Örnek olarak, Bayes çıkarımında bir odanın kapısı için sadece “açık” ve “kapalı” değerleri verilebilirken, Dempster – Shafer Teorisinde, aynı değişken için “açık”, “kapalı”, ve “belirsiz” değerleri verilebilir.

Dempster – Shafer Teorisinde bir değişkenin alabileceği değerlerin kümesine ait bütün alt kümelere bir kütle değeri atanır. Eğer bir değişken S farklı değer alabiliyorsa, bu değişkene ait 2^S adet alt küme olmalıdır, ve bu alt kümelerin her birine, genel toplam 1 olacak şekilde kütle değerleri atanmalıdır. Bu durumun açıklamasına, yukarıdaki kapı örneğinden devam edersek; bir odanın kapısının ne durumda olduğunu karar değişkeni olarak kabul edersek, DST’de bu değişken “açık”, “kapalı”, ve “belirsiz” gibi 3 farklı değer alabiliyor olsun. Bu tanım kümesine uygun “altküme” - “kütle” ikilileri Çizelge 3.4’teki gibi olabilir.

Çizelge 3.4 Alt Küme – Kütle değerleri (örnek – 1)

alt küme	kütle
belirsiz	0.12
kapalı	0.38
açık	0.34
belirsiz – kapalı	0.10
belirsiz – açık	0.06
kapalı – açık	0.00
belirsiz – kapalı – açık	0.00
$\emptyset$	0.00

Bu çizelgede “kapalı – açık”, “belirsiz – kapalı – açık”, ve “ $\emptyset$ ” altkümelerine mantıklı olmadıkları için sıfır (0.00) kütle verilmiştir.

3.1.2.1 Dempster Birleştirme Kuralı

Sistemdeki değişkenler için “kütle” değerleri gözlemlendikten sonra, bu değişkenlerin birbirleriyle ilişkileri ve önceki gözlemlerle aralarındaki ilişkileri Dempster’ın birleştirme kuralı (*Dempster’s rule of combination*) kullanılarak yapılır. Bu kural birden fazla amaç için kullanılabilir. İlk olarak bir adet alıcı için önceden var olan veri ile bu

alıcının yaptığı yeni gözlemdeki veriyi birbirleriyle birleştirebilir; ikinci olarak ise, birden fazla alıcıdan gelen verilerin birbirleriyle birleştirilmelerini sağlar. Bu kuralın bir adet değişken için yapılan gözlemde elde edilen veri ile önceden elde edilmiş olan verinin ilişkilendirilmesini sağlayan biçimi Denklem 3.6'daki gibidir.

$$m(X) = \frac{\sum_{A \cap B = X} m_s(A) \times m_o(B)}{1 - \sum_{A \cap B = \emptyset} m_s(A) \times m_o(B)}$$

Dempster Birleştirme Kuralı

Denklem (3.6)

Denklem 3.6'da m_s alıcıdan gelen yeni veriye ait kütle değerini, m_o ise gözlem yapılmadan önce var olan kütle değerini ifade etmektedir. Koks (2003) tarafından bildirildiğine göre, Dempster – Shafer teorisinin ve Dempster birleştirme kuralı'nın en açıklayıcı örneklerinden biri Zou *et al.* (2000) tarafından verilmiştir.

3.1.2.2 Dempster – Shafer teorisi (örnek – 1)

Zou *et al* (2000)'in örneğinde bulunduğu odayı hücreler olarak gören ve her bir hücreyi “dolu”, “boş” ve “belirsiz” şeklinde nitelendirebilen bir robot bulunuyor. Robot, herhangi bir hücre için 3 farklı değer üretebildiğinden dolayı, boş kümeyle birlikte toplam sekiz adet altküme elde edilir. Elde edilen bu sekiz altkümeden “boş küme”, “belirsiz – dolu”, “belirsiz – boş”, “dolu – boş” ve “belirsiz – dolu – boş” kümeleri mantıklı olmadıkları için 0.00 kütle değerine sahiptirler. Bu örnekte, odadaki her bir hücre için “dolu” kütlesi bulunmak istendiğinde ve Dempster birleştirme kuralı (Denklem 3.6) uygulandığında Denklem 3.7 elde edilir.

$$m(dolu) = \frac{m_s(dolu) \times m_o(dolu) + m_s(dolu) \times m_o(belirsiz) + m_s(belirsiz) \times m_o(dolu)}{1 - m_s(dolu) \times m_o(boş) - m_s(dolu) \times m_o(boş)}$$

Dempster Birleştirme Kuralı (örnek – 1)

Denklem (3.7)

3.1.2.3 Dempster – Shafer teorisi (örnek – 2)

Dempster birleştirme kuralı ve Dempster – Shafer teorisi birden fazla alıcıdan gelen verilerin birleştirilmesi amacı ile kullanılabilir. Buna örnek olarak algılanan bir hava aracının tipini belirleyen birbirinden bağımsız iki alıcıdan gelen verilerin birleştirilmesi ve hava aracının tipinin belirlenmesini verebiliriz (Koks 2003). Bu alıcılar tasarımları gereği algıladıkları hava aracını {F111, F/A18, P3C, Hızlı, Belirsiz} olarak tanımlayabilmektedir (Koks 2003). Bu sınıflandırmada “Hızlı” “F111 veya F/A18” anlamında; “Belirsiz” ise “F111 veya F/A18 veya P3C” anlamında kullanılmıştır (Koks 2003). Her iki alıcıdan gelen veriler Çizelge 3.5’in 2. ve 3. sütunlarındaki gibidir.

Çizelge 3.5 Alıcılardan Gelen Kütle Verileri (Koks 2003)

Hava Aracı Tipi	Alıcı 1 (kütle)	Alıcı 2 (kütle)	Birleştirilmiş Kütle
F111	30%	40%	55%
F/A18	15%	10%	16%
P3C	3%	2%	0.4%
Hızlı	42%	45%	29%
Belirsiz	10%	3%	0.3%

$$m^{1,2}(X) \propto \sum_{A \cap B = X} m^1(A) \times m^2(B)$$

İki bağımsız alıcıdan gelen verilerin birleştirilmesi

Denklem (3.8)

Çizelge 3.5’in 2. ve 3. sütunundaki veriler Denklem 3.8 kullanılarak birleştirilir³. F111 için birleştirilmiş kütle hesaplaması Denklem 3.9’daki gibidir, diğer değerlere ait birleştirilmiş kütleler de benzer şekilde hesaplanır.

³ Birleştirilmiş kütlelerin hesaplanmasında Denklem 3.6 yerine Denklem 3.8’in kullanılmasının sebebi hesaplama yükünü hafifletmek içindir. Her bir alıcının alabileceği değerlerin kütleleri toplamı 1 olduğu için Denklem 3.8 kullanılarak hesaplanan değerlerin toplamı da aynı şekilde 1 olmalıdır. Bunu elde etmek için Denklem 3.6’nın paydasındaki işlemi gerçekleştirmek yerine Denklem 3.8’de hesaplanan kütlelerin hepsini kütle toplamına bölerek normalleştirmek işlem yükünü hafifletmektedir (Koks 2003)

$$\begin{aligned}
& m^{1,2}(F111) \propto m^1(F111) \times m^2(F111) + m^1(F111) \times m^2(Hizli) + \\
& m^1(F111) \times m^2(Belirsiz) + m^1(Hizli) \times m^2(F111) + \\
& m^1(Belirsiz) \times m^2(F111) \\
& = 0.30 \times 0.40 + 0.30 \times 0.45 + 0.30 \times 0.03 + 0.42 \times 0.40 + 0.10 \times 0.40 = 0.47
\end{aligned}$$

Veri birleştirmesi için örnek hesaplama

Denklemler (3.9)

Her bir değer için birleştirilmiş kütle değeri hesaplandıktan sonra bu değerlerin normalleştirilmesi gerekir; bu amaçla, hesaplanan değerlerin toplamı bulunur, ve her değer bulunan bu toplama bölünür. Bu işlemin sonucunda Çizelge 3.5'in 4. sütununda bulunan birleştirilmiş kütle değerleri elde edilir; böylece 2 farklı alıcıdan gelen veriler DST kullanılarak birleştirilmiş olur. Alıcı sayısı daha fazla olan durumlarda Denklem 3.8 alıcı sayısına uygun şekilde uygulanır.

3.1.3 Transfer Edilebilir İnanış Modeli

Transfer edilebilir inanış modeli (*Transferable Belief Model - TBM*) temelinde Dempster – Shafer teoremiyle benzer yönleri sahiptir. TBM'in de avantajı alıcılardan doğru veri gelmediği durumlarda da hesaplama yapabilmesidir. Bu hesaplama yapılırken DST'de olduğu gibi Dempster birleştirme kuralından (Denklem 3.8) faydalanır. Ayrıca; yine Dempster – Shafer teorisinde olduğu gibi, bir değişkenin alabileceği değerlerin kümesine ait bütün alt kümelerle bir “temel inanış kümesi” (*basic belief assignment*) değeri atanır. Eğer bir değişken S farklı değer alabiliyorsa, bu değişkene ait 2^S adet alt küme olmalıdır, ve bu alt kümelerin her birine, genel toplam 1 olacak şekilde “inanış kümesi” değerleri atanmalıdır. TBM'i DST'den ayıran en önemli özelliği çift seviyeli bir algoritma olmasıdır. İlk seviyede alıcıdan gelen veri bir “inanış fonksiyonu” (*belief function*) ile temsil edilir, bu inanış fonksiyonu “inanış kümesi” ile tanımlanır. İkinci seviyeye geçiş sürecinde TBM'in bir diğer çok önemli özelliği ortaya çıkar. Bu özellik, alıcıların güvenilirliğinin dikkate alınmasıdır. Burada “indirgeme faktörü” (*discounting factor - α*) olarak isimlendirebileceğimiz bir değişken bulunur ve değeri, alıcıların güvenilirliği ile ters orantılıdır. Bir alıcının güvenilirliği ne kadar yüksek ise “indirgeme faktörü” o derece düşük değere sahip olur. İlk seviyedeki “inanış fonksiyonu”na indirgeme faktörünün etkisi Denklem 3.10'a göre eklendiğinde ikinci seviyeye geçilir.

$$m^{\theta,\alpha}(A) = (1 - \alpha)m^{\theta}(A), A \neq \theta$$

$$m^{\theta,\alpha}(\theta) = \alpha + (1 - \alpha)m^{\theta}(\theta)$$

İndirgeme faktörünün Etkisi (θ =alıcının tanım kümesi, A =alıcıdan gelen rastgele değer) (Elouedi *et al.* 2004) Denklem (3.10)

İndirgeme faktörünün hesaplamaya katıldığı inanış kütesi (m) değerleri hesaplandıktan sonra; ikinci seviyede, bir karar fonksiyonu oluşturulur. Bu karar fonksiyonu “bahis olasılığı fonksiyonu” olarak adlandırılır. Bu fonksiyon oluşturulurken bahis dönüşümü (Denklem 3.11) (*Pignistic Transformation*) kullanılır; Pignus Latince, bahis anlamına gelmektedir ve fonksiyonun ismi buradan kaynaklanır. Bu fonksiyon *BetP* ile gösterilir.

$$BetP = \sum_{B \subseteq \theta} \frac{|A \cap B|}{|A|} \frac{m(B)}{1 - m(\emptyset)}, A \subseteq \theta$$

Bahis Dönüşümü (Pignistic Transformation) (Elouedi *et al.* 2004) Denklem (3.11)

Transfer Edilebilir İnanış Modeli'nin çalışma şeklinin anlaşılabilmesi için 3.1.3.1'deki örneğin incelenmesi faydalıdır.

3.1.3.1 Transfer edilebilir inanış modeli (örnek) (Elouedi *et al.* 2004)

Algılanan hava aracının tipini belirleyebilen iki adet alıcı bulunuyor (S_1 ve S_2). Bu alıcıların belirleyebildiği araç tipleri $\theta = \{Airplane, Helicopter, Rocket\}$ şeklindedir. Toplam dört adet birbirinden farklı hava aracı algılanmış durumdadır; bunlar $\{o_1, o_2, o_3, o_4\}$ olarak isimlendirilmişlerdir. Bu dört hava aracının tipleri için S_1 ve S_2 alıcılarının kullanacağı “inanış kütesi” değerleri sırasıyla Çizelge 3.6 ve Çizelge 3.7’de görüldüğü gibidir ve bu çizelgelerde yer alan değerler önceden tanımlanmıştır.

Çizelge 3.6 S_1 alıcısının inanış kütleleri değerleri (Elouedi *et al.* 2004)

Aracın gerçek tipi	Airplane	Helicopter	Airplane	Rocket
S_1	o_1	o_2	o_3	o_4
$\emptyset$	0	0	0	0
Airplane	0	0	0	0
Helicopter	0	0.5	0.4	0
Rocket	0.5	0.2	0	0
Airplane U Helicopter	0	0	0	0
Airplane U Rocket	0	0	0.6	0.6
Helicopter U Rocket	0.3	0	0	0.4
θ	0.2	0.3	0	0

Çizelge 3.7 S_2 alıcısının inanış kütleleri değerleri (Elouedi *et al.* 2004)

Aracın gerçek tipi	Airplane	Helicopter	Airplane	Rocket
S_2	o_1	o_2	o_3	o_4
$\emptyset$	0	0	0	0
Airplane	0	0.3	0.2	0
Helicopter	0	0	0	0
Rocket	0	0	0	0
Airplane U Helicopter	0.7	0.4	0	0
Airplane U Rocket	0	0	0	0
Helicopter U Rocket	0	0	0.6	1
θ	0.3	0.3	0.2	0

S_1 alıcısının indirgeme faktörü α_1 ve S_2 alıcısının α_2 olarak belirlenir. Daha sonra Denklem 3.10 kullanılarak Denklem 3.11’de kullanılacak olan m değerleri bulunur (örnek hesaplama Denklem 3.12’de görülebilir). S_1 alıcısı için hesaplanan bu m değerleri Çizelge 3.8’de görülebilir. Aynı hesaplamalar S_2 alıcısı için de yapılır ve $BetP$ değerlerinin hesaplanmasına başlanır (örnek hesaplama Denklem 3.12’de görülebilir).

$$m_{S_1}^{\theta, \alpha_1} \{o_1\} (Rocket) = 0.5 \times (1 - \alpha_1) = 0.5 - 0.5\alpha_1$$

$$m_{S_1}^{\theta, \alpha_1} \{o_1\} (Helicopter \cup Rocket) = 0.3 \times (1 - \alpha_1) = 0.3 - 0.3\alpha_1$$

$$m_{S_1}^{\theta, \alpha_1} \{o_1\} (\theta) = \alpha_1 + (1 - \alpha_1) \times 0.2 = 0.2 + 0.8\alpha_1$$

$$BetP_{S_1}^{\theta, \alpha_1} \{o_1\} (Rocket) = 0.5 - 0.5\alpha_1 + \frac{0.3 - 0.3\alpha_1}{2} + \frac{0.2 + 0.8\alpha_1}{3} = 0.72 - 0.38\alpha_1$$

Örnek indirgenmiş m değeri ve BetP hesaplaması (Elouedi *et al.* 2004) Denklem (3.12)

Denklem 3.12’de anlatıldığı şekilde bütün *BetP* değerleri hesaplanır ve Çizelge 3.8’deki tablo ortaya çıkar.

Çizelge 3.8 S_1 alıcısı için hesaplanan BetP değerleri (Elouedi *et al.* 2004)

S_1	o_1	o_2	o_3	o_4
Airplane	$0.06 + 0.26 \alpha_1$	$0.1 + 0.24 \alpha_1$	$0.3 + 0.03 \alpha_1$	$0.3 + 0.03 \alpha_1$
Helicopter	$0.22 + 0.12 \alpha_1$	$0.6 - 0.27 \alpha_1$	$0.4 - 0.06 \alpha_1$	$0.2 + 0.13 \alpha_1$
Rocket	$0.72 - 0.38 \alpha_1$	$0.3 + 0.03 \alpha_1$	$0.3 + 0.03 \alpha_1$	$0.5 - 0.16 \alpha_1$

Bütün bu hesaplamalar S_2 alıcısı için, indirgenme faktörü α_2 kullanılarak tekrarlanır, ve S_2 alıcısı için de benzer bir çizelge hazırlanır. α indirgenme faktörleri için bir en iyi değer hesaplama metodu olsa da, kullanıcının belirlediği bir değer de kullanılabilir. α değerleri çizelgelerde yerlerine koyulup gerekli hesaplama yapıldıktan sonra elde edilen veriler Dempster birleştirme kuralı (Denklem 3.8) kullanılarak birleştirilir ve sonuca ulaşılır.

3.2 Değerlendirme Algoritmalarının Silah Atama Sisteminde Kullanımı ve Sistemin Çalışma Prensipleri

3.2.1 Tehdit değerlendirme ve silah atama sisteminin çalışma prensipleri

Bayes çıkarımı, Dempster – Shafer teorisi veya Transfer edilebilir inanış modeli algoritmalarının sistemde, öldürücülük değerinin hesaplanmasında kullanılabilmesi için öncelikle, öldürücülük değerini belirleyecek olan sistem değişkenleri tanımlanır. Bu değişkenlerin her biri için sistemde bir alıcı bulunmaktadır ve alıcılardan gelen veriler doğrultusunda seçilen algoritma kullanılarak öldürücülük değeri hesaplanır.

Algılanan tehdide ait veriler yani sistem değişkenleri hareket tipi (*mobility*), platform tipi (*platform*), pozisyon (*position*), IFF (*Identification Friend Or Foe*) bilgisi (*IFF*), tehdit seviyesi (*threat level*), birincil silah (*primary weapon*), ikincil silah (*secondary weapon*), üçüncül silah (*tertiary weapon*) olarak listelenebilir. Seçilen algoritmanın çalışabilmesi için algılanan tehdide ait bu değişkenler hakkında verilerin alıcılardan sisteme gelmesi gerekmektedir. Alıcılardan sisteme ulaşan veriler, her bir tehdit için ayrı hafıza yapılarında tutulur. Bu yapıların içeriği Çizelge 3.9'daki gibidir. Bayes çıkarımı ya da Transfer edilebilir inanış modeli kullanılacaksa “detectedPlatform” yapısı; Dempster – Shafer Teorisi kullanılacaksa “detectedPlatformDS” yapısı kullanılır. Bu farklılığın sebebi Dempster – Shafer teorisinde değişkenlerin “Belirsiz” değerini alabilmesinden kaynaklanır.

Çizelge 3.9 Algılanan tehdide ait verilerin saklandığı hafıza yapısı

detectedPlatform	detectedPlatformDS
mobility	mobility
position	position
air platform type	air platform type
surface platform type	surface platform type
iff response	iff response
threat level	threat level
primary weapon	primary weapon
secondary weapon	secondary weapon
tertiary weapon	tertiary weapon

Daha sonra operatörün algılanan tehdit sayısını (*numberOfDetections*) ve kullanılmasını istediği algoritma modelini (*userAlgorithmChoice*) sisteme girdi olarak vermesi gerekir. Bu noktadan sonra sistem kullanıcıdan girdiği tehdit sayısı kadar tehdidin özelliklerini elle girmesini veya öntanımlı dosyalardan birini yüklemesini veya daha önceden kullanıcının yarattığı ve kayıt altına aldığı dosyalardan birini yüklemesini bekler ve her tehdit için yukarıda açıklanmış olan hafıza yapılarında bu özelliklere ait değerleri saklar ve bu hafıza yapısına bir indeks numarası verir. Bu noktada kullanıcı her bir değişkenin alabileceği değerleri bilmelidir. Kullanıcı geçersiz bir değer girmek isterse sistem tarafından uyarılır ve girmeye çalıştığı değeri düzeltmesi istenir. Değişkenlerin alabileceği değerler Çizelge 3.10 ve Çizelge 3.11'deki gibidir.

Çizelge 3.10 Bayes Çıkarımı ve TBM’de değişken değerleri

değişken	değer
mobility	1 : slow [surface] 2 : fast [air] 3 : noMotion [surface]
position	1 : inRange 2 : outRange
air platform type (tehdit hava kaynaklı ise)	1 : fighter 2 : bomber 3 : helicopter 4 : civilian transportation
surface platform type (tehdit satıh kaynaklı ise)	1 : cruiser 2 : frigate 3 : destroyer 4 : civilian transportation
iff response	1 : friend 2 : hostile 3 : noResponse 4 : suspect
threat level	1 : noThreat 2 : lowThreat 3 : highThreat 4 : unknown
primary weapon secondary weapon tertiary weapon (tehdit satıh kaynaklı ise)	1 : surface to surface missile [SSM] 2 : close-in weapon system [CIWS] 3 : naval artillery [deck gun] 4 : machine gun 5 : noWeapon
primary weapon secondary weapon tertiary weapon (tehdit hava kaynaklı ise)	1 : air to surface missile [ASM] 2 : drop bomb 3 : machine gun 4 : noWeapon

Çizelge 3.11 Dempster – Shafer Teorisinde değişken değerleri

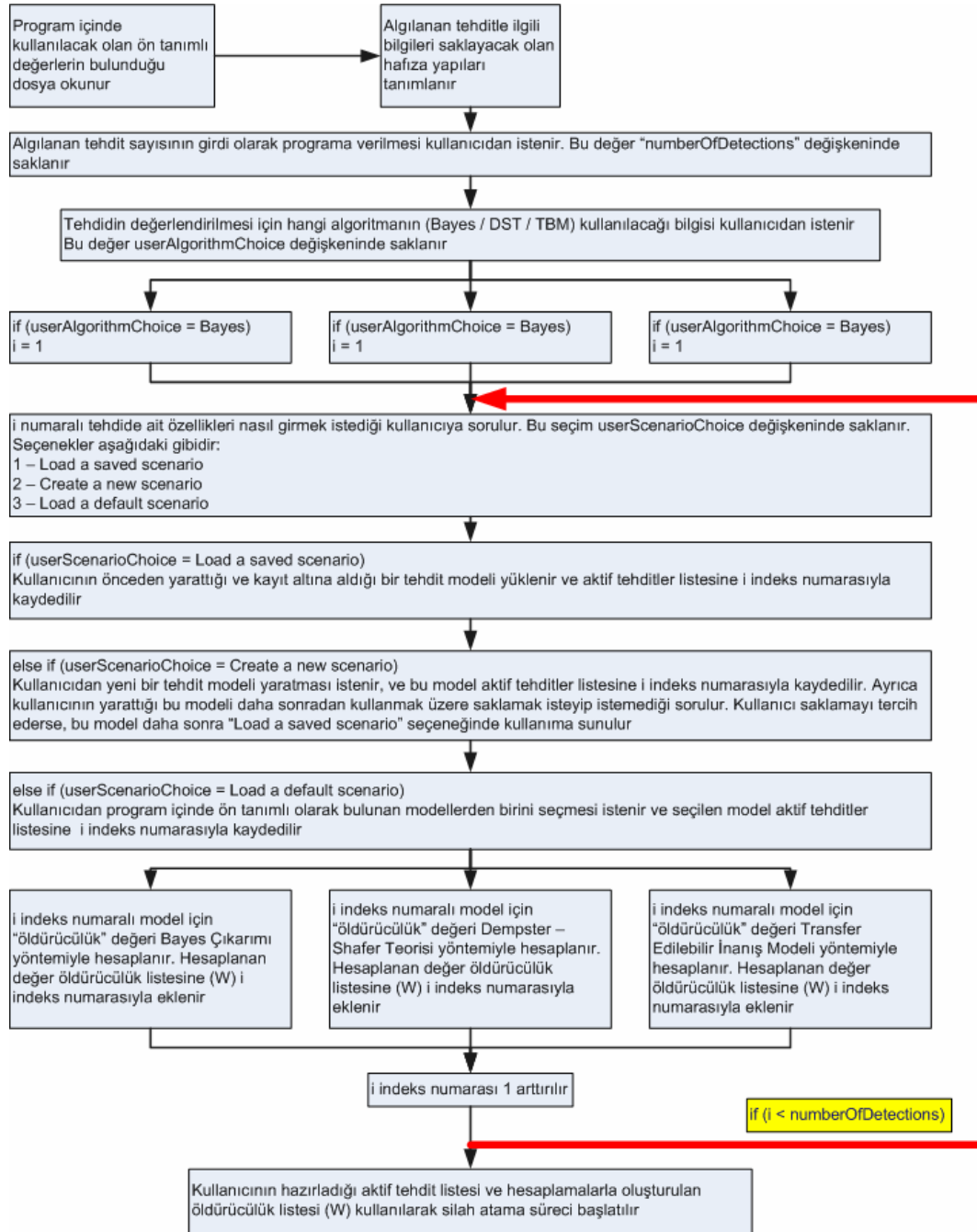
değişken	değer
mobility	1 : slow [surface] 2 : fast [air] 3 : noMotion [surface] 4 : unknown
position	1 : inRange 2 : outRange 3 : unknown
air platform type (tehdit hava kaynaklı ise)	1 : fighter 2 : bomber 3 : helicopter 4 : civilian transportation

Çizelge 3.11 Dempster – Shafer Teorisinde değişken değerleri (devam)

değişken	değer
	5 : unknown
surface platform type (tehdit satıh kaynaklı ise)	1 : cruiser 2 : frigate 3 : destroyer 4 : civilian transportation 5 : unknown
iff response	1 : friend 2 : hostile 3 : noResponse 4 : suspect 5 : unknown
threat level	1 : noThreat 2 : lowThreat 3 : highThreat 4 : unknown
primary weapon secondary weapon tertiary weapon (tehdit satıh kaynaklı ise)	1 : surface to surface missile [SSM] 2 : close-in weapon system [CIWS] 3 : naval artillery [deck gun] 4 : machine gun 5 : noWeapon 6 : unknown
primary weapon secondary weapon tertiary weapon (tehdit hava kaynaklı ise)	1 : air to surface missile [ASM] 2 : drop bomb 3 : machine gun 4 : noWeapon 5 : unknown

Her bir tehdit için bilgi girişi tamamlandığında girilen bilgiler özet olarak ekrana yansıtılır. Operatör önceden belirttiği sayıda tehdit için bilgi girişini tamamladıktan sonra, bu tehdit modelleri kullanıcının uygulanmasını istediği algoritma tipi kullanılarak değerlendirilir ve her biri için bir öldürücülük değeri hesaplanır. Tehdit modelleri, sahip oldukları öldürücülük değerlerine göre büyükten küçüğe sıralanır. Öldürücülük değeri önceden tanımlanmış bir eşik değerinden daha düşük olan tehdit modellerine bu sıralama içinde yer verilmez ve zararsız ya da aynı taraftan olduğu düşünülerek varlığı göz ardı edilir. En yüksek öldürücülük değerine sahip olan tehdit modelinden başlanarak silah atama uygulaması çalıştırılır. Sisteme ait genel akış diyagramı Şekil 3.4'teki gibidir. Tehdit değerlendirme ve silah atama sisteminin, tehdit değerlendirme kısmında kullanılabilecek olan Bayes çıkarımı 3.2.2'de, Dempster – Shafer teorisi 3.2.3'te, Transfer edilebilir inanış modeli ise 3.2.4'te ayrıntılı olarak ele alınmıştır;

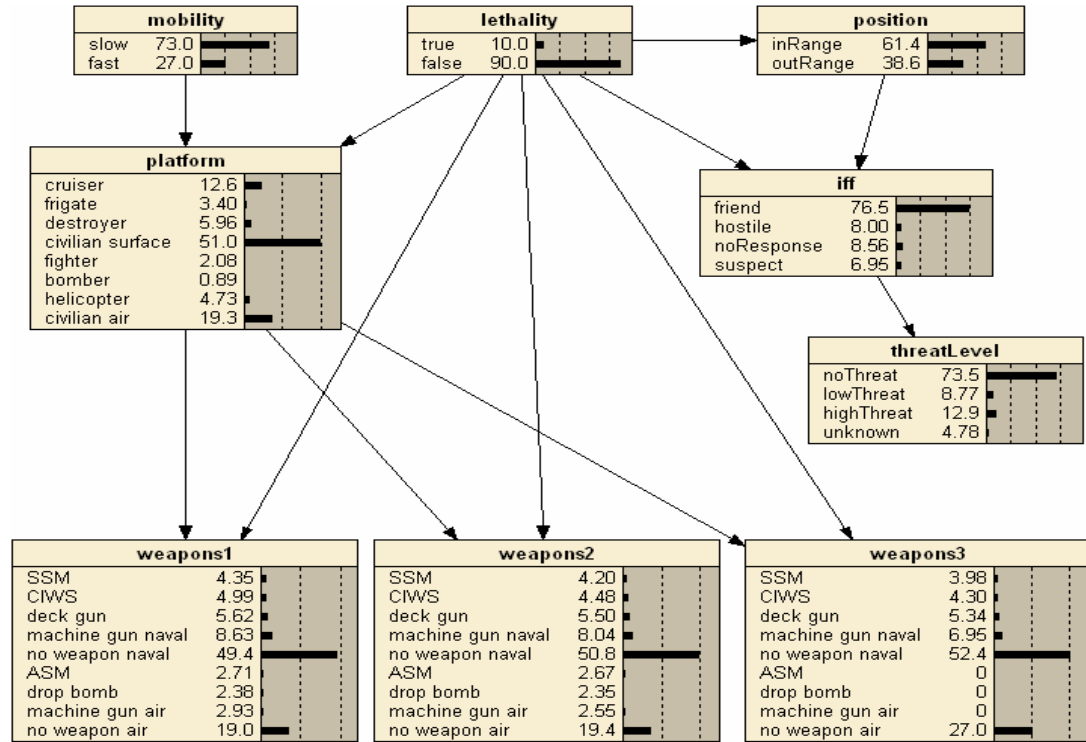
bunların yanı sıra silah atama algoritmasının temelleri ise 3.2.5'te ayrıntılı olarak açıklanmıştır.



Şekil 3.4 Sistemin genel akış diyagramı

3.2.2 Bayes çıkarımı yöntemiyle öldürücülük değeri hesaplanması

Öldürücülük değerinin Bayes çıkarımı yöntemiyle hesaplanmasında temel olarak Denklem 3.2 kullanılır. Denklem 3.2'nin kullanılabilmesi için öncelikle sistemdeki değişkenlerin arasındaki ilişkiyi modelleyen, Şekil 3.1'deki yapıya benzer bir Bayes ağı oluşturulur. Öldürücülük, Bayes ağının hipotez değişkeni olarak belirlenir. Tehdidin niyetini ve tehdidin yeteneklerini oluşturan değişkenler gözlem/kanıt değişkenleri olarak ağda yerlerini alırlar. Gereken hallerde, hipotez değişkeni ile gözlem değişkenlerinin arasında köprü kurulması amacıyla ara seviye değişkenler tanımlanır. Çizelge 3.9'da içeriği açıklanmış olan hafıza yapısındaki bütün değişkenleri ve aralarındaki ilişkileri içeren Bayes ağı Şekil 3.5'deki gibi tasarlanmıştır.



Şekil 3.5 Algılanan tehdidin özelliklerine göre oluşturulan Bayes Ağı⁴

Denklem 3.2, Şekil 3.5'teki Bayes Ağına uygulandığında Denklem 3.13 elde edilir.

⁴ Şekil 3.5'te görülen Bayes Ağı görüntüsü, Norsys Software Corp. Firmasının bir ürünü olan Netica isimli program ile hazırlanmıştır.

$$P(lethal|position,iff,threat,mobility,platform,Weapon1,Weapon2,Weapon3)=$$

$$P(Weapon1|platform,lethal) \times P(Weapon2|platform,lethal) \times P(Weapon3|platform,lethal) \times$$

$$P(platform|mobility,lethal) \times P(threat|iff) \times P(iff|position,lethal) \times P(position|lethal) \times P(lethal)$$

Genel denklemin tasarlanan Bayes Ağı'na uyarlanması

Denklem (3.13)

Denklem 3.13'te hesaplanması gereken değişken “lethal” olarak isimlendirilmiş olan öldürücülük değişkenidir. Denklemden kullanılan pozisyon (position), IFF bilgisi (iff), tehdit seviyesi (threat), devinim (mobility), platform tipi (platform), birincil silah (Weapon1), ikincil silah (Weapon2) ve üçüncül silah (Weapon3) değişkenlerinin değerlerinin kendilerine atanmış olan alıcılardan doğru ve eksiksiz olarak geldiği kabul edilir; eksik bilgi gelen durumlarda Bayes çıkarımı yanlış sonuçlar üretir ve operatörün hata yapmasını sağlar; bu tip durumlarda, değerlendirme için Dempster –Shafer teorisi'nin ya da Transfer edilebilir inanış modeli'nin kullanılması gerekir. Öldürücülük değişkeni yapısı gereği sadece iki değer alabilmektedir; bu değerler öldürücü (yes) ve öldürücü değil (no) şeklinde sıralanabilir. Bu değişkenin öldürücü ($P(lethal = yes)$) değerini alma olasılığı, silah atama bölümünde kullanılacak olan değerdir. Bu değer hesaplanırken önce $lethal = yes$ için Denklem 3.13 hesaplanır (Denklem 3.14), daha sonra ise $lethal = no$ için aynı hesaplama (Denklem 3.15) yapılır. Her iki hesaplamada da “lethal” değişkeni dışında kalan değişkenler için alıcıdan gelen değerler yerlerine koyulur ve hesaplama yapılır. Hesaplanan ilk değer, iki değer toplamına oranı (Denklem 3.16), algılanan tehdidin öldürücülük değerini verir.

$$A = P(lethal = yes|position = AD,iff = AD,threat = AD,mobility = AD,platform = AD,Weapon1 = AD,Weapon2 = AD,Weapon3 = AD) =$$

$$P(Weapon1 = AD|platform = AD,lethal = yes) \times P(Weapon2 = AD|platform = AD,lethal = yes) \times$$

$$P(Weapon3 = AD|platform = AD,lethal = yes) \times P(platform = AD|mobility = AD,lethal = yes) \times P(threat = AD|iff = AD) \times$$

$$P(iff = AD|position = AD,lethal = yes) \times P(position = AD|lethal = yes) \times P(lethal = yes)$$

$lethal = yes$ için olasılık hesaplanması

Denklem (3.14)

$$\begin{aligned}
B &= P(\textit{lethal} = \textit{no} | \textit{position} = \textit{AD}, \textit{iff} = \textit{AD}, \textit{threat} = \textit{AD}, \textit{mobility} = \textit{AD}, \textit{platform} = \textit{AD}, \textit{Weapon1} = \textit{AD}, \textit{Weapon2} = \textit{AD}, \textit{Weapon3} = \textit{AD}) = \\
&P(\textit{Weapon1} = \textit{AD} | \textit{platform} = \textit{AD}, \textit{lethal} = \textit{no}) \times P(\textit{Weapon2} = \textit{AD} | \textit{platform} = \textit{AD}, \textit{lethal} = \textit{no}) \times \\
&P(\textit{Weapon3} = \textit{AD} | \textit{platform} = \textit{AD}, \textit{lethal} = \textit{no}) \times P(\textit{platform} = \textit{AD} | \textit{mobility} = \textit{AD}, \textit{lethal} = \textit{no}) \times P(\textit{threat} = \textit{AD} | \textit{iff} = \textit{AD}) \times \\
&P(\textit{iff} = \textit{AD} | \textit{position} = \textit{AD}, \textit{lethal} = \textit{no}) \times P(\textit{position} = \textit{AD} | \textit{lethal} = \textit{no}) \times P(\textit{lethal} = \textit{no})
\end{aligned}$$

lethal = *no* için olasılık hesaplanması

Denklem (3.15)

$$P(\textit{lethal} = \textit{yes}) = \frac{A}{A + B}$$

Öldürücülük değerinin hesaplanması

Denklem (3.16)

Denklem 3.14 ve Denklem 3.15'te “AD” alıcıdan gelen değer anlamında kullanılmıştır. Öldürücülük değeri hesaplanırken, “*Lethal*” değişkeni dışında kalan bütün değişkenlerde alıcıdan gelen değere ait olasılık değeri yerine koyulur. Alıcıdan gelen değer diğer değişkenleri etkileme oranları sistem içerisinde gömülü olan ön tanımlı bir dosyada yer alır. Ağda yer alan bütün değişkenler için marjinal ve koşullu olasılık değerleri geçmiş tecrübeler ve önseziye bağlı olarak, sübjektif bir şekilde belirlenir ve bu ön tanımlı dosyada tanımlanır (bu işlem sistem çalışmaya başlamadan önce yapılmalıdır). Örnek vermek gerekirse; Denklem 3.13, *lethal* değerini hesaplarken $P(\textit{position} | \textit{lethal})$ fonksiyonu için (ve aynı denklemde kullanılan diğer fonksiyonlar için) bir değere ihtiyaç duyar. Çizelge 3.10'da görüldüğü üzere *position* değişkeni {*inRange*, *outRange*} gibi iki değer alabilmektedir. Pozisyon alıcısından bu değişken için hangi değer geldiği ve *lethal* değişkeninin hangi değerinin {*yes*, *no*} hesaplanmasının istendiği bilindiğine göre $P(\textit{position} | \textit{lethal})$ değerinin ön tanımlı dosyada bulunan ilgili eşleme tablosundan okunması ve gerekli yerde kullanılması gerekir. Bu hesaplama için sistemde kullanılan eşleme tablosu Çizelge 3.12'de görülebilir. Bu dosya sistemde şu şekilde yorumlanır; *position* alıcısından {*inRange*} değeri geldiğinde ve *lethal* değişkeninin {*yes*} olduğu durum hesaplanmak istendiğinde $P(\textit{position} | \textit{lethal})$ fonksiyonu için 0.887 değeri kullanılır.

Çizelge 3.12 $P(\textit{position} | \textit{lethal})$ için eşleştirme tablosu

	<i>lethal</i>	
<i>position</i>	<i>yes</i>	<i>no</i>
<i>inRange</i>	0.887	0.113
<i>outRange</i>	0.584	0.416

Benzer şekilde Denklem 3.13, Denklem 3.14 ve Denklem 3.15 için gerekli olan tüm fonksiyonlara ait eşleme tabloları ön tanımlı dosyada bulunur. Operasyon başladığı andan itibaren elde edilen veriler doğrultusunda değişkenlerin dağılımları güncellenir. Bu güncellemeler sonunda hipotez değişkeni olan “*lethal*” için bir W_i değeri elde edilir. W_i , $[0,1]$ aralığında tanımlıdır. $W_i = 0$ ise algılanan unsur herhangi bir tehdit yaratmamaktadır; $W_i = 1$ ise algılanan unsur maksimum derecede tehdit arz etmektedir. Operasyonun amacı doğrultusunda bu dosyadaki tablolar operatör tarafından operasyon öncesinde yeniden düzenlenebilir. Bu tarz düzenlemelere örnek olarak; sistem dost kuvvetlerle birlikte tatbikata çıkan bir araçta kullanılacaksa, eşleme tablolarında gerekli düzenlemeler yapılabilir ve $\{inRange\}$ olarak algılanan araçlar için, sistemin daha düşük öldürücülük değerleri hesaplaması sağlanabilir, çünkü her ne kadar algılanan tehdit normal şartlarda çok yüksek öldürücülük ihtiva etse de, ortamdaki araçların dost olduğu bilindiği için göz ardı edilebilir.

Yukarıda anlatılan çalışma prensiplerine göre sistemin çalışması iki örnekle açıklanabilir. Sistemin bulunduğu ortamda iki adet tehdit algılandığı varsayılıyor. Bu iki tehdidin özellikleri Çizelge 3.13’teki gibi olsun.

Çizelge 3.13 Algılanan tehditlerin özellikleri

özellikler	tehdit 1	tehdit 2
mobility	1 : slow [surface]	2 : fast [air]
position	1 : inRange	1 : inRange
air platform type	-	1 : fighter
surface platform type	3 : destroyer	-
iff response	2 : hostile	1 : friend
threat level	3 : highThreat	1 : noThreat
primary weapon	1 : surface to surface missile [SSM]	1 : air to surface missile [ASM]
secondary weapon	2 : close-in weapon system [CIWS]	3 : machine gun
tertiary weapon	3 : naval artillery [deck gun]	-

Tehdit 1 ve Tehdit 2 için sisteme öldürücülük değeri hesaplatıldığında sırasıyla 0.971558 ve 0.007693 değerleri üretiliyor, yani Tehdit 1 son derece ölümcüllük arz ederken, Tehdit 2, savunulan araç için ölümcüllük yaratmamaktadır.

Tehdit 1 için sistemin çıktısı

```
Command Window
-----detected platform 1-----
mobility of the detected platform      : slow [surface]
position of the detected platform      : inRange
IFF response of the detected platform  : hostile
threat level of the detected platform  : highThreat
type of the detected platform          : destroyer
primary weapon of the detected platform : surface to surface missile [SSM]
secondary weapon of the detected platform : close-in weapon system [CIWS]
tertiary weapon of the detected platform : naval artillery [deck gun]
-----
press any key to continue
-----
do you want to save this scenario? [y/n]
n
lethality of the detected platform 1   : 0.971558
```

Tehdit 2 için sistemin çıktısı

```
Command Window
-----detected platform 1-----
mobility of the detected platform      : fast [air]
position of the detected platform      : inRange
IFF response of the detected platform  : friend
threat level of the detected platform  : noThreat
type of the detected platform          : fighter
primary weapon of the detected platform : air to surface missile [ASM]
secondary weapon of the detected platform : machine gun
tertiary weapon of the detected platform : noWeapon
-----
press any key to continue
-----
do you want to save this scenario? [y/n]
n
lethality of the detected platform 1   : 0.007693
```

Gerçekleştirilen algoritmanın doğru çalışıp çalışmadığı, algılanan tehditlerin özelliklerine göre ölümcüllük değerlerini doğru üretip üretmediği NETICA⁵ kullanılarak doğrulanabilir. Tehditler için aynı özellikler NETICA'ya girdi olarak

⁵ Bayes Çıkarımının simülasyonu için kullanılan Norsys Software Corp. Firmasının bir ürünü olan bir bilgisayar programı. Bu programın deneme sürümüne <http://www.norsys.com/download.html> adresinden ulaşılabilir.

verildiğinde Tehdit 1 ve Tehdit 2 için ölümcüllük değerleri sırasıyla 0.972 ve 0.0077 olmaktadır; ki bu değerler gerçekleştirilen algoritmanın hesapladığı değerlerin bir miktar yuvarlanmış halleridir. Bu bilgiler ışığında Bayes Çıkarımı gerçekleştirmesinin doğru çalıştığı söylenebilir.

3.2.3 Dempster – Shafer teorisi uygulanarak öldürücülük değeri hesaplanması

Dempster – Shafer algoritmasının Bayes Çıkarımından en büyük farkı, uygulanabilmesi için algılanan tehditle ilgili tüm verilere ihtiyaç duymamasıdır, bunun gerçekleştirilmesi için değişkenlerin her birinin kendi değerleri haricinde “belirsiz (*unknown*)” değerini alabilmesine izin verilmiştir. Örnek olarak “*position*” değişkeni Bayes yönteminde sadece {*inRange*, *outRange*} değerlerini alabilirken, Dempster - Shafer’da bu değerlerin yanı sıra kullanıcı “*belirsiz*” değerini girebilmektedir. Bu seçenek, değerinden emin olunamayan bütün değişkenler için operatöre sunulmuştur. Algılayıcıdan “belirsiz” değeri gelirse yada operatör alıcıdan gelen veriye güvenmiyorsa, o değişken için belirsiz değerini girebilir ve öldürücülük hesabının bu şekilde yapılmasını isteyebilir.

Öldürücülük değerinin Dempster – Shafer teorisi yöntemiyle hesaplanmasının temelinde Denklem 3.6 ve Denklem 3.8’in birden fazla alıcıdan gelen verileri birleştirmek üzere güncellenmiş hali bulunur. Denklem 3.6 tasarlanan sisteme uyarlandığında Denklem 3.17 elde edilir. Tasarlanan sistem de sekiz adet alıcı bulunduğu için Denklem 3.8 sisteme uyarlandığında Denklem 3.18 elde edilir.

$$m(lethal = yes) = \frac{A}{B}$$

$$A = m_s(lethal = yes) \times m_o(lethal = yes) + m_s(lethal = yes) \times m_o(lethal = unknown) + m_s(lethal = unknown) \times m_o(lethal = yes)$$

$$B = 1 - m_s(lethal = yes) \times m_o(lethal = no) - m_s(lethal = no) \times m_o(lethal = yes)$$

Genel Denklem sisteme uyarlanmış hali Denklem (3.17)

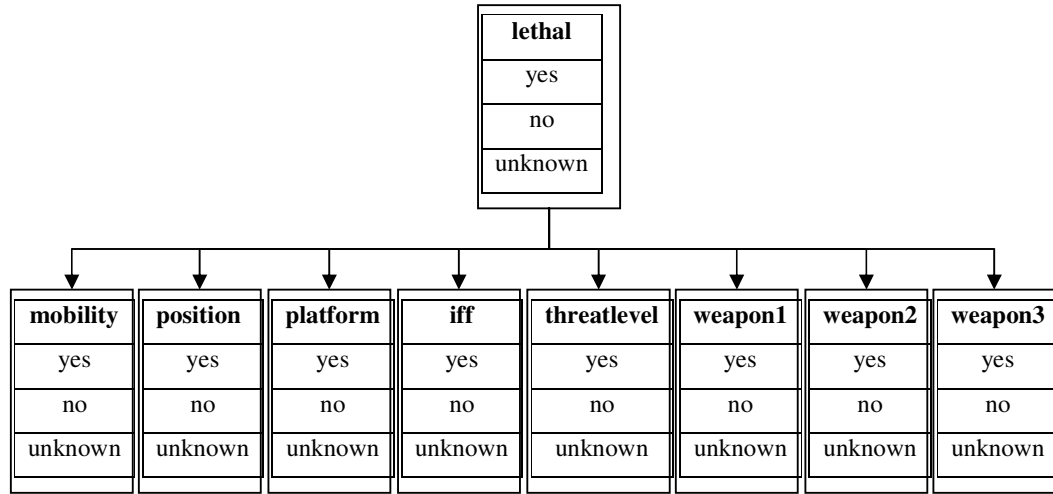
$$m^{1,2,3,4,5,6,7,8}(X) \propto \sum_{A \cap B \cap C \cap D \cap E \cap F \cap G \cap H = X} m^1(A) \times m^2(B) \times m^3(C) \times m^4(D) \times m^5(E) \times m^6(F) \times m^7(G) \times m^8(H)$$

Sekiz bağımsız alıcıdan gelen verilerin birleştirilmesi

Denklem (3.18)

Denklem 3.17 hesaplandığında $m(\text{lethal} = \text{yes})$ için elde edilecek olan değer sistemin hesaplamasının istendiği öldürücülük değerini verir. Bu denklemde m_o ile gösterilen değerler sistem çalıştırılmadan önce, geçmiş tecrübeler ve önseziyle ilgili olarak, sübjektif bir şekilde belirlenen değerlerdir. m_s değerleri ise algılanan tehdide ait algılayıcılardan gelen değerlerin Denklem 3.18 kullanılarak birleştirilmesiyle elde edilen değerlerdir.

Dempster-Shafer teorisinin kullanılabilmesi için algılanan tehdide ait değişkenler arasında Bayes Çıkarımında yapıldığı gibi bir ağ yapısı kullanılmalıdır. Bu yapı Şekil 3.6'daki gibidir.



Şekil 3.6 Dempster – Shafer Teorisinde kullanılan ağ yapısı

Oluşturulan bu ağ yapısına göre Denklem 3.18 sisteme uygulandığında, Denklem 3.19, Denklem 3.20 ve Denklem 3.21 elde edilir, ve m_s değerlerinin hesaplamalarında bu denklemler kullanılır.

$$m^{position, mobility, platform, iff, threat, weapon 1, weapon 2, weapon 3}(lethal = yes) = \sum_{X=yes / unknown} m^{position}(X) \times m^{mobility}(X) \times m^{platform}(X) \times m^{iff}(X) \times m^{threat}(X) \times m^{w1}(X) \times m^{w2}(X) \times m^{w3}(X)$$

$lethal = yes$ değerinin hesaplanması Denklem (3.19)

$$m^{position, mobility, platform, iff, threat, weapon 1, weapon 2, weapon 3}(lethal = no) = \sum_{X=no / unknown} m^{position}(X) \times m^{mobility}(X) \times m^{platform}(X) \times m^{iff}(X) \times m^{threat}(X) \times m^{w1}(X) \times m^{w2}(X) \times m^{w3}(X)$$

$lethal = no$ değerinin hesaplanması Denklem (3.20)

$$m^{position, mobility, platform, iff, threat, weapon 1, weapon 2, weapon 3}(lethal = unknown) = \sum_{X=unknown} m^{position}(X) \times m^{mobility}(X) \times m^{platform}(X) \times m^{iff}(X) \times m^{threat}(X) \times m^{w1}(X) \times m^{w2}(X) \times m^{w3}(X)$$

$lethal = unknown$ değerinin hesaplanması Denklem (3.21)

Dempster – Shafer teorisinde, Bayes çıkarımında kullanılan farklı bir yapı kullanılmasının en büyük sebebi, Denklem 3.18’in (dolayısıyla Denklem 3.19, Denklem 3.20, ve Denklem 3.21’in) alıcılardan gelen verileri birleştirip, öldürücülük değerini hesaplayabilmesi için, bütün alıcılardan gelen verilerin aynı tanım kümesine ait olması gerekmektedir. Ama Çizelge 3.11’de görüldüğü üzere alıcılardan gelen verilerin tanım kümeleri birbirinden farklıdır. Mesela; pozisyon alıcısından $\{inRange, outRange, unknown\}$ değerleri gelebilirken, devinim alıcısından $\{slow [surface], fast [air], noMotion [surface], unknown\}$ değerleri gelebilmektedir. Benzer uyumsuzluklar sekiz adet alıcının tamamı için geçerlidir ve Dempster – Shafer teorisinin kullanılabilmesi için bu uyumsuzluğun düzeltilmesi ilk koşuldur. Bu uyumsuzluğun düzeltilmesi için sistem içerisinde eşleme fonksiyonları kullanılmıştır. Bu eşleme fonksiyonlarının amacı alıcıdan gelen, farklı tanım kümesine ait değerleri, Dempster – Shafer Algoritmasının anlayacağı ortak bir tanım kümesine $\{lethal = yes (evet) / no (hayır) / unknown$

(belirsiz)} eşlemektir. Bu eşleme fonksiyonları için açıklayıcı bir örnek Çizelge 3.14'te görülebilir. Bu eşleme fonksiyonları, aynen Bayes çıkarımı'nda olduğu gibi sistem içerisinde bulunan ve sistem başlatıldığında okunan ön tanımlı bir dosyada bulunmaktadır.

Çizelge 3.14 Pozisyon değişkeni için alıcı değeri – DST tanım değeri eşleme fonksiyonu

alıcı değerleri / demspster-shafer tanım degerleri	yes	No	unknown
inRange	0.348	0.614	0.038
outRange	0.095	0.889	0.016
unknown	0.230	0.170	0.600

Bu çizelgede, alıcıdan gelebilecek olan her bir değerin, DST tanım kümesindeki değerlere hangi oranlarla etki ettiği tanımlanmıştır. Örnek olarak algılanan tehdidin, savunulan aracın yakınında olduğu ve alıcıdan {inRange} değeri geldiği varsayıldığında; Denklem 3.19, Denklem 3.20, ve Denklem 3.21'de $m^{position}(X)$ değişkeninin değeri, $lethal = yes$ hesaplanırken 0.348, $lethal = no$ hesaplanırken 0.614, $lethal = unknown$ hesaplanırken 0.038 olarak kullanılır, ve hesaplamalar bu doğrultuda yapılır. Bu durum diğer yedi adet alıcı değişkeni için de geçerlidir; ve her bir alıcı değişkeni için eşleme fonksiyonları tanımlanmıştır. Operasyonun amacı doğrultusunda bu eşleme fonksiyonlarındaki değerler operatör tarafından operasyon öncesinde yeniden düzenlenebilir. Bu tarz düzenlemelere örnek olarak; sistem dost kuvvetlerle birlikte tatbikata çıkan bir araçta kullanılacaksa, eşleme tablolarında gerekli düzenlemeler yapılabilir; böylece sistem üzerinde ölümcül silahlar taşıyan bir tehdit algılandığında, bu tehdidin kendi tarafında olduğunu bilir ve çok düşük bir öldürücülük değeri hesaplayarak sistemin yanlış karar vermesi engellenmiş olur.

Operasyon başladığı andan itibaren alıcıdan gelen veriler doğrultusunda hangi değişkenin sisteme öldürücülük, zararsızlık, belirsizlik eklediği belirlenir. Bu belirlenen bilgilerle de, önceden sistemde “öldürücülük” değişkeni için belirlenmiş olan değer Denklem 3.17 kullanılarak güncellenir ve “öldürücülük” için bir W_i değeri elde edilir. Bu W_i değeri silah atama algoritmasında kullanılacak olan değerdir. W_i , [0,1]

aralığında tanımlıdır. $W_i = 0$ ise algılanan unsur herhangi bir tehdit yaratmamaktadır; $W_i = 1$ ise algılanan unsur maksimum derecede tehdit arz etmektedir.

Yukarıda anlatılan çalışma prensiplerine göre sistemin çalışması, Bayes Çıkarımında kullanılanlara benzer iki tehdit modeliyle açıklanabilir; aradaki fark olarak bazı alıcı değerlerinin $\{unknown\}$ olmasını gösterebiliriz. Sistemin bulunduğu ortamda iki adet tehdit algılandığı varsayılıyor. Bu iki tehdidin özellikleri Çizelge 3.15'teki gibi olsun.

Çizelge 3.15 Algılanan tehditlerin özellikleri

özellikler	tehdit 1	tehdit 2
mobility	1 : slow [surface]	2 : fast [air]
position	3 : unknown	1 : inRange
air platform type	-	1 : fighter
surface platform type	3 : destroyer	-
iff response	2 : hostile	5 : unknown
threat level	3 : highThreat	4 : unknown
primary weapon	1 : surface to surface missile [SSM]	1 : air to surface missile [ASM]
secondary weapon	2 : close-in weapon system [CIWS]	3 : machine gun
tertiary weapon	3 : naval artillery [deck gun]	-

Tehdit 1 ve Tehdit 2 için sisteme öldürücülük değeri hesaplatırıldığında sırasıyla 0.991591 ve 0.002073 değerleri üretiliyor, yani Tehdit 1 son derece ölümcüllük arz ederken, Tehdit 2, savunulan araç için ölümcüllük yaratmamaktadır.

Tehdit 1 için sistemin çıktısı

```

Command Window
-----detected platform 1-----
mobility of the detected platform      : slow [surface]
position of the detected platform      : unknown
IFF response of the detected platform  : hostile
threat level of the detected platform  : highThreat
type of the detected platform          : destroyer
primary weapon of the detected platform : surface to surface missile [SSM]
secondary weapon of the detected platform : close-in weapon system [CIWS]
tertiary weapon of the detected platform : naval artillery [deck gun]
-----
press any key to continue
-----
do you want to save this scenario? [y/n]
n
lethality of the detected platform 1   : 0.991591

```

Tehdit 2 için sistemin çıktısı

```
Command Window
-----detected platform 1-----
mobility of the detected platform      : fast [air]
position of the detected platform      : inRange
IFF response of the detected platform  : unknown
threat level of the detected platform  : unknown
type of the detected platform          : fighter
primary weapon of the detected platform : air to surface missile [ASM]
secondary weapon of the detected platform : machine gun
tertiary weapon of the detected platform : noWeapon
-----
press any key to continue
-----
do you want to save this scenario? [y/n]
n
lethality of the detected platform 1   : 0.002073
```

3.2.4 Transfer edilebilir inanış modeli uygulanarak öldürücülük değeri hesaplanması

Transfer Edilebilir İnanış Modeli başlığında açıklandığı gibi bu algoritmanın temelinde de DST’de olduğu gibi Denklem 3.6 Dempster Birleştirme Kuralı ve Denklem 3.8 bulunur. Ayrıca; yine Dempster – Shafer Teorisinde olduğu gibi, bir değişkenin alabileceği değerlerin kümesine ait bütün alt kümelerle bir “temel inanış kütesi” (basic belief assignment) değeri atanır. Eğer bir değişken θ farklı değer alabiliyorsa, bu değişkene ait 2^θ adet alt küme olmalıdır, ve bu alt kümelerin her birine, genel toplam 1 olacak şekilde “inanış kütesi” değerleri atanmalıdır (Denklem 3.22). θ , sözü edilen değişken için tanım kümesidir ve “*Frame of Discernment*” olarak adlandırılır.

$$\sum_{A \in \theta} m(A) = 1$$

İnanış kütlelerinin toplamı

Denklem (3.22)

Örnek olarak tehdit modeli değişkenlerinden devinim ele alınırsa; devinimin alabileceği değerler, yani $\theta = \{1:slow, 2:fast, 3:noMotion\}$ şeklinde oluşur. Bu durumda altküme sayısı $2^3 = 8$ şeklindedir, ve oluşan bu altkümeler Çizelge 3.16’daki gibidir.

Çizelge 3.16 Devinim değişkeninin altkümeleri

$\emptyset$
slow
fast
noMotion
slow U fast
slow U noMotion
fast U noMotion
θ

TBM’i DST’den ayıran en önemli özelliği çift seviyeli bir algoritma olmasıdır. İlk seviyede alıcıdan gelen veri bir “inanış fonksiyonu” (*belief function*) ile temsil edilir, bu inanış fonksiyonunda “temel inanış kütesi” ve “indirgeme faktörü” kullanılır. Algılanan tehditle ilgili tehdit modeli yaratılırken, herhangi bir değişken için sadece bir adet değer girilebildiği göz önüne alındığında (bu değerler Çizelge 3.10’da tanımlanmıştır), girilebilen bu değerle, değişkenin oluşturabileceği tüm altkümeler arasında bir eşleme yapılması ihtiyacı ortaya çıkar. Dempster-Shafer algoritmasında yapıldığı gibi, TBM’de de tehdit modelinde bulunan değerlerle TBM’de kullanılacak yapı arasında eşlemeler yapılmıştır. Bu eşlemeler Bayes Çıkarımı ve DST’de olduğu gibi TBM için de ön tanımlı bir dosyada tanımlanmışlardır ve sistem başlatıldığında okunarak sistem içerisinde kullanılırlar. Devinim örneğinden devam edilirse alıcıdan $\{1:slow, 2:fast, 3:noMotion\}$ değerlerinden sadece bir tanesi tehdit modelinin devinim değişkeninin değeri olabilir; bu değer “slow” olduğunu varsayalım; bu durumda Çizelge 3.16’daki olasılıklardan içinde “slow” geçmeyen, ‘ $\emptyset$ ’, ‘fast’, ‘noMotion’ ve ‘fast U noMotion’ a 0 (sıfır) olasılık atanır. İçinde “slow” geçen seçeneklere ($\{slow, slow U fast, slow U noMotion, \theta\}$) ise toplamı 1 (bir) olacak şekilde temel inanış kütesi değerleri belirlenir ve bu değerler öntanımlı dosyada sisteme tanıtılırlar (Denklem 3.22); bunlar arasında en yüksek temel inanış kütesine sahip değişken “slow” olarak belirlenir (Çizelge 3.17). Çizelge 3.17’de devinim için tanımlanmış olan eşleme tablosu benzeri tablolar tüm alıcılar için ayrı ayrı tanımlanmıştır.

Çizelge 3.17 Devinim için temel inanış kütleleri değer dağılımı

TBM değeri / Tehdit Model Değeri	slow	fast	noMotion
Ø	0.00	0.00	0.00
slow	0.86	0.00	0.00
fast	0.00	0.94	0.00
noMotion	0.00	0.00	0.83
slow U fast	0.04	0.03	0.00
slow U noMotion	0.08	0.00	0.12
fast U noMotion	0.00	0.02	0.01
θ	0.02	0.01	0.04

Sözü geçen indirgeme faktörü (*discounting factor* - α) alıcıların güvenilirlik derecesiyle ilgili bir parametredir. Bu parametrenin değeri alıcıların güvenilirliğiyle ters orantılıdır. İndirgeme faktörü için çeşitli kaynaklarda en iyi değer hesaplaması için yöntemler bulunsa da, sistemde her bir farklı tipteki alıcı için birbirinden farklı sabit değerler kullanılmıştır. Bu değerler operatör tarafından operasyona çıkılmadan önce ilgili dosyadan değiştirilebilir tipte değerlerdir. TBM’in ilk seviyesinin tamamlanabilmesi için, alıcılardan gelen veriler için belirlenen temel inanış kütleleriyle indirgeme faktörü birleştirilir ve inanış fonksiyonu elde edilir. Bu işlem için Denklem 3.10 kullanılır. Devinim alıcısının “*slow*” değeri algılaması örneğinden devam edersek; Çizelge 3.17 ‘deki gibi bir dağılım ve α bilinen bir ortamda Denklem 3.10 kullanılırsa, alıcıdan “*slow*” verisinin gelmesine ait inanış fonksiyonu olarak Denklem 3.23’teki gibi bir denklem seti ortaya çıkar.

$$m^{\theta,\alpha}(slow) = (1 - \alpha)m^{\theta}(slow) = (1 - \alpha) \times 0.86 = 0.86 - 0.86\alpha$$

$$m^{\theta,\alpha}(slow \cup fast) = (1 - \alpha)m^{\theta}(slow \cup fast) = (1 - \alpha) \times 0.04 = 0.04 - 0.04\alpha$$

$$m^{\theta,\alpha}(slow \cup noMotion) = (1 - \alpha)m^{\theta}(slow \cup noMotion) = (1 - \alpha) \times 0.08 = 0.08 - 0.08\alpha$$

$$m^{\theta,\alpha}(\theta) = \alpha + (1 - \alpha)m^{\theta}(\theta) = \alpha + (1 - \alpha) \times 0.02 = \alpha + 0.02 - 0.02\alpha = 0.98\alpha + 0.02$$

Devinim için inanış fonksiyonu seti

Denklem (3.23)

Tüm alıcılardan gelen verilerle ilgili olarak inanış fonksiyonu için denklem setleri elde edildikten sonra TBM'in ikinci bölümü olan bahis olasılığı fonksiyonlarının oluşturulmasına geçilir. Bahis olasılığı fonksiyonu bir karar fonksiyonudur ve oluşturulmasında bahis dönüşümü (Denklem 3.11) kullanılır. Devinim örneği (*mobility = slow*) için bahis olasılığı fonksiyonu Denklem 3.24'teki gibi oluşturulur.

$$BetP = m^{\theta, \alpha}(slow) + \frac{m^{\theta, \alpha}(slow \cup fast)}{2} + \frac{m^{\theta, \alpha}(slow \cup noMotion)}{2} + \frac{m^{\theta, \alpha}(\theta)}{3} =$$

$$0.86 - 0.86\alpha + \frac{0.04 - 0.04\alpha}{2} + \frac{0.08 - 0.08\alpha}{2} + \frac{0.98\alpha + 0.02}{3} = 0.9267 - 0.5933\alpha$$

Bahis olasılığı fonksiyonu hesaplanması

Denklem (3.24)

Denklem 3.24'te görülen fonksiyon sadece devinim değişkeni içindir. Tehdide ait diğer değişkenler için de (toplam 8 adet) benzer fonksiyonlar tanımlanır. α indirgeme faktörünün değeri her bir alıcı için farklı olarak belirlenmiştir ve belirlenen bu α değerleri oluşturulan bahis olasılığı fonksiyonlarında yerlerine koyularak toplam sekiz adet *BetP* değeri elde edilir. Her bir alıcı için bu *BetP* değerleri, önceden tanımlanmış olan bir eşik değeri ile kıyaslanır, eğer *BetP* değeri eşik değerinden yüksek ise, alıcıdan gelen veri doğru kabul edilir ve değişken değeri alıcıdan geldiği gibi kabul edilir; eğer eşik değeri daha büyük ise, alıcıdan gelen veriye güvenilmez ve alıcıdan “belirsiz” değeri gelmiş kabul edilir.

Transfer Edilebilir inanış Modeli'nin bu noktadan sonraki çalışma şekli Dempster – Shafer teorisi gerçekleşmesiyle birebir aynıdır. Bir önceki aşamada eşik değeri ile kıyaslayarak karar verilen alıcı değerleri DST'de kullanılan eşleme fonksiyonları aracılığıyla Şekil 3.6'daki yapıya uygun hale getirilir ve önceden sistemde “öldürücülük” değişkeni için belirlenmiş olan değer Denklem 3.17 kullanılarak güncellenir ve “öldürücülük” için bir W_i değeri elde edilir. Bu W_i değeri silah atama algoritmasında kullanılacak olan değerdir. W_i , [0,1] aralığında tanımlıdır. $W_i = 0$ ise algılanan unsur herhangi bir tehdit yaratmamaktadır; $W_i = 1$ ise algılanan unsur maksimum derecede tehdit arz etmektedir.

Bu çalışma prensipleri doğrultusunda Bayes çıkarımı yöntemiyle öldürücülük değeri hesaplanması bölümünde verilmiş örneği (Çizelge 3.13), Transfer edilebilir inanış modeli için uygularsak; Tehdit 1 ve Tehdit 2 için sisteme öldürücülük değeri hesaplatıldığında sırasıyla 0.985083 ve 0.000001 değerleri üretiliyor, yani Tehdit 1 son derece ölümcüllük arz ederken, Tehdit 2, savunulan araç için ölümcüllük yaratmamaktadır.

Tehdit 1 için sistemin çıktısı

```
Command Window
-----detected platform 1-----
mobility of the detected platform      : slow [surface]
position of the detected platform      : inRange
IFF response of the detected platform  : hostile
threat level of the detected platform  : highThreat
type of the detected platform          : destroyer
primary weapon of the detected platform : surface to surface missile [SSM]
secondary weapon of the detected platform : close-in weapon system [CIWS]
tertiary weapon of the detected platform : naval artillery [deck gun]
-----
press any key to continue
-----
do you want to save this scenario? [y/n]
n
lethality of the detected platform 1      : 0.985083
```

Tehdit 2 için sistemin çıktısı

```
Command Window
-----detected platform 2-----
mobility of the detected platform      : fast [air]
position of the detected platform      : inRange
IFF response of the detected platform  : friend
threat level of the detected platform  : noThreat
type of the detected platform          : fighter
primary weapon of the detected platform : air to surface missile [ASM]
secondary weapon of the detected platform : machine gun
tertiary weapon of the detected platform : noWeapon
-----
press any key to continue
-----
do you want to save this scenario? [y/n]
n
lethality of the detected platform 2      : 0.000001
```

3.2.5 Silah atama sistemi

Bir savaş gemisi sınırlı sayıda cephaneye taşıyabilir; bu cephaneleri kullanırken de iki unsur gözetilir. Bunlar kendisini savunmak ve verilen görevi tamamlamak olarak sıralanır. Bu yüzden, eldeki kaynakların en optimize biçimde kullanılması hayati önem taşır. Farklı yapıdaki silah ve bunlara ait cephanenin tamamı farklı karakteristiklere, kullanım amaçlarına ve maliyetlere sahiptir. Bu silahların kullanılması ve cephanenin harcanması, etkinlik ve verimlilik kriterleri arasında dengelenmelidir. Savunma sırasında önem arz eden bir diğer kriter de zamanlamadır; yanlış yapılan bir zamanlama ölümcül sonuçlar ortaya çıkarabilir.

Savunma sisteminde kullanılabilecek silahları, savunma amaçlı (*soft-kill*) silahlar ve öldürücü (*hard-kill*) silahlar olarak ikiye ayırabiliriz. Öldürücü silahlar isimlendirmesi yanlış anlaşılmalara yol açmamalıdır; öldürücü silahlar da savunma amaçlı kullanılırlar. Aradaki fark savunma amaçlı silahlar sadece algılanan tehdit, savunulan gemiye yönelik atış yaptığında, füzeyi yanıltma amaçlı kullanılır; diğer taraftan öldürücü silahlar tamamen algılanan tehdide zarar verip, yok etme amaçlıdır.

Chaff, *flare*, ve *decoy* savunma amaçlı (*soft-kill*) silahlardır. Bu tip silahların, kısa sürede kullanıma hazır hale gelmeleri, maliyetlerinin daha ucuz olması, çok miktarda bulundurulabilmeleri ve hataları affeder yapıda olmaları gibi avantajları vardır. Bu avantajlarının yanında, kesin sonuç sağlamamaları gibi azımsanmayacak bir dezavantajları da bulunmaktadır (Huang and Kar 1994). Sistemde *soft – kill* silah olarak sadece “*flare*” kullanılmıştır.

Güdümlü füze, top, satıhtan havaya füze, satıhtan satıha füze gibi silahlar, öldürücü (*hard-kill*) silahlar olarak adlandırılırlar. Atışa hazırlanmalarının uzun sürmesi, maliyetin yüksek olması, boyutları sebebiyle sınırlı sayıda bulundurulabilmeleri, kullanılabilmesi için hedef hakkında çok ayrıntılı bilgiye gereksinim duyması gibi birçok dezavantajları bulunan bu silahların tek avantajı tehdide karşı kesin çözüm sağlamalarıdır; ki, sırf bu özellikleri yüzünden vazgeçilemezler (Huang and Kar 1994). Sistemde *hard – kill* silah olarak satıhtan satıha füze (*surface to surface missile – SSM*),

satıhtan havaya füze (*surface to air missile – ASM*), yakın mesafe roketi (*close in weapon system – CIWS*), güverte topu (*deck gun*) ve makineli tüfek kullanılmıştır.

Silah atama, sahip olunan silahlarla algılanan tehditlerin uyumlu çiftler halinde eşleştirilmesidir. Silah atama işlemi gerçek zamanlı ve angajman kurallarına uygun olarak yapılır. Silah atama da amaç, savunulan gemi için tehlike arz eden tehditlerin, öldürücülük değerleri göz önünde bulundurularak belli bir sıra doğrultusunda bertaraf edilmelerini sağlamaktır.

Bayes çıkarımı yöntemiyle öldürücülük değeri hesaplanması, Dempster – Shafer teorisi uygulanarak öldürücülük değeri hesaplanması ve Transfer edilebilir inanış modeli uygulanarak öldürücülük değeri hesaplanması bölümlerinde ayrıntılı olarak açıklandığı gibi, algılanan tehditler belirli özelliklerine göre bu algoritmalar tarafından değerlendirilirler ve her bir tehdit için, kullanılan algoritma bir öldürücülük değeri hesaplar. Algılanan tehdit sayısı birden fazla ise, hesaplanan öldürücülük değerleri bir öldürücülük listesine eklenir. Bu liste W ile gösterilir ve listede algılanan tehdit sayısı kadar, öldürücülük değeri bulunur. Listenin her bir elemanı W_i olarak isimlendirilir. Kullanılan algoritma, oluşturduğu öldürücülük listesiyle birlikte, algıladığı tüm tehditlere özellikleri barındıran hafıza yapılarını silah atama sistemine parametre olarak gönderir.

Öldürücülük listesinin (W) yanı sıra, savunulan geminin sahip olduğu tüm silah sistemlerinin listelendiği bir tablo oluşturulur, bu tablo M olarak ve içerdiği her eleman M_j olarak adlandırılır. Ayrıca algılanan tehdiye karşı etkinlik tablosu oluşturulmalıdır. Bu tablo $W_{i,j}$ olarak adlandırılır. Bu notasyon j numaralı silahın i numaralı tehdiye karşı etkinlik derecesi olarak yorumlanır. Bu tabloda yer alacak olan değerler, operasyon öncesinde belirlenir ve ilgili dosyada gerekli değerler girilir. Operatör istediği takdirde bu değerlerde değişiklik yoluna gidebilir. Sistemde bu etkinlik tablosundan iki adet bulunur; ilki satıh tehditlerine karşı olan (Çizelge 3.18) ve diğeri hava tehditlerine karşı olan (Çizelge 3.19) etkinlik tablosudur.

Çizelge 3.18 Satış kaynaklı tehdit için örnek karşı etkinlik tablosu

sahip olunan silah	tehdide karşı etkinlik değeri
surface to surface missile [SSM]	0.72
surface to air missile [SAM]	0.00
close-in weapon system [CIWS]	0.07
naval artillery [deck gun]	0.07
machine gun	0.07
flare	0.07

Çizelge 3.19 Hava kaynaklı tehdit için örnek karşı etkinlik tablosu

sahip olunan silah	tehdide karşı etkinlik değeri
surface to surface missile [SSM]	0.00
surface to air missile [SAM]	0.79
close-in weapon system [CIWS]	0.00
naval artillery [deck gun]	0.07
machine gun	0.07
flare	0.07

Bunlara ek olarak; gereksiz cephane harcanmasını engellemek için “tahammül edilebilir minimum eşik değeri” değişkeni tanımlanır. Bu değişken e ile gösterilir. Herhangi bir tehdit için $W_i \leq e$ olduğu durumda, algılanan tehdit tehlike arz etmiyor olarak yorumlanır ve daha fazla cephane harcamaya gerek duyulmaz.

Son olarak; W_i değeri 1’e çok yakın (öldürücülük değeri çok yüksek) tehditler için de ayrı bir eşik değeri tanımlanır (öldürücülük eşiği olarak adlandırılır). Bu tarz bir tehdit algılandığında sistem soft – kill ya da düşük etkinliğe sahip hard – kill silahları kullanmakla vakit kaybetmez ve en etkin silahını bu tehdit üzerinde kullanır.

Yukarıda açıklanmış olan temeller doğrultusunda, sistem ilk önce kendisine gönderilen öldürücülük listesi W içindeki değerleri büyükten küçüğe sıralar ve en yüksek öldürücülük değerinin arz eden tehdidi listenin en üstüne yerleştirir. Sistem, listenin en üstünde bulunan tehdide ait öldürücülük değerini, öldürücülük eşik değeri ile kıyaslar, eğer tehdit eşikten daha büyük bir öldürücülüğe sahipse, en etkin silahıyla bu tehdide saldırır (tehdidin devinim özelliğine göre en etkin silah; satıhtan satıha füze ya da

satıhtan havaya füze olabilmektedir). Eğer eşik değeri, öldürücülük değerinden büyükse, sistem silah kullanımına soft – kill silahlardan başlar. Listenin ilk sırasındaki tehdide karşı ilk angajman yapıp, silah kullanıldıktan sonra, o tehdide ait “artık öldürücülük değeri” (*residual threat value*) hesaplanır. Bu hesaplama Denklem 3.25 ve Denklem 3.26 kullanılarak yapılır.

$$lethality(new) = lethality \times (1 - KullanilanSilahinTehditUzerindeYarattigiEtki)$$

Artık öldürücülük değeri hesaplanması

Denklem (3.25)

$$W_i = W_i \times (1 - W_{i,j})$$

Artık öldürücülük değeri hesaplanması (Huang and Kar 1994)

Denklem (3.26)

Denklem 3.26 kullanılarak elde edilen artık öldürücülük değeri, bu noktadan sonra o tehdidin öldürücülük değeri olarak öldürücülük listesinde (W) düzeltilir ve sistemde kullanılır.

Listenin ilk sırasındaki tehdit için angajman yapıp, artık tehdit değeri hesaplandıktan sonra, öldürücülük listesi (W) tekrar büyükten küçüğe sıralanır. Bu işlemler serisi algılanan tüm tehditlerin öldürücülük değerleri “tahammül edilebilir minimum eşik değeri” (e) değerinden daha düşük bir değere gelene kadar tekrarlanır.

Yukarıda anlatılan süreç, Çizelge 3.13’te tanımlanmış olan Tehdit 1 için gerçekleştirilebilir. Bu gerçekleşme başlatılmadan önce sistemde kullanılan sabit değerlerin biliniyor olması gerekir. Bu değerlerden ilki tahammül edilebilir minimum eşik değeridir; ve sistemde $e = 0.05$ olarak tanımlanmıştır, yani, hesaplanan öldürücülük değeri 0.05’ten büyük olan tüm tehditler sistem tarafından ciddiye alınacak ve karşı tedbirler uygulanacaktır. e değeri tamamen operasyonun amaçları doğrultusunda önceden belirlenen bir değerdir. Bu değer belirlenirken görevin icra edileceği ortamla ilgili ön bilgilerden faydalanılır. Ayrıca, öldürücülük değeri çok yüksek tehditlere, en kısa yoldan karşılık verilebilmesi için bir öldürücülük eşiği tanımlanmıştır. Öldürücülük eşik değeri 0.90 olarak belirlenmiştir; yani hesaplanan öldürücülük değeri bu eşiğin üzerinde olan tehditlere karşı *soft – kill* yada düşük güce sahip *hard – kill* silahlarla vakit ve

kaynak kaybetmek yerine, sistem en güçlü savunma silahlarını bu tehdit üzerinde kullanır (sath kaynaklı tehdit için sathıtan sathi füze, hava kaynaklı tehdit için sathıtan havaya füze). Kullanılan silah sayesinde, bu tehdidin öldürücülük değeri daha az tehlikeli arz eden değerlere düşürüldükten sonra sistem bu sefer de en değerli cephanesini daha fazla harcamamak için normal işleyişine döner ve daha düşük güce sahip silahlarla, algılanan tehdidin öldürücülük değerini $e = 0.05$ değerinin altına indirmeye çalışır.

Burada örnek olarak, kullanıcı algılanan tehdit sayısını (*numberOfDetections*) 1 girmiş (Çizelge 3.13'teki Tehdit1) ve kullanılmasını istediği algoritma modelini de (*userAlgorithmChoice*) Bayes Çıkarımı olarak belirlemiş olsun. Bu koşullarda sistem kullanıcıdan algılamayla ilgili bilgileri aldıktan sonra Bayes Çıkarımı yöntemiyle öldürücülük değerini hesaplar ve hesaplanan değeri kullanıcıya gösterir (Tehdit1 için hesaplanan değer $W = 0.971558$ olur). Bu noktadan sonra, elde edilen bu değer silah atama sistemine gönderilir, ve gerekli görülen karşı tedbirler algılanan tehdit üzerinde uygulanır. $W = 0.971558$ değeri, öldürücülük eşik değeri olan 0.90'dan daha yüksek olduğu için, bu tehdit öncelikli tehdit sınıfına girer ve sistem düşük güce sahip silahları kullanmakla vakit kaybetmez. Algılanan tehdit sath kaynaklı olduğu için (*mobility = slow*), silah atamanın ilk yinelemesinde sathıtan sathi füze kullanılır. İlk yinelemenin ardından kullanılan silaha bağlı olarak tehdide ait öldürücülük değeri yeniden hesaplanır ve o tehdidin yeni öldürücülük değeri (W), bu hesaplanan değer olur. İlk yinelemenin çıktısı kullanıcıya gösterilir ve bu çıktı aşağıdaki gibidir.

İlk yinelemeye ait sistem çıktısı

```
lethality of the detected platform 1      : 0.971558
-----
press any key to continue
-----
detection 1 residual threat before weapon assignment: 0.971558
detection 1 residual threat after weapon assignment: 0.310899
detection 1 used weapon: surface to surface missile [SSM]
detection 1 used weapon cost: 74
detection is still lethal!!!
```

Sistem ilk yinelemeden sonra, indirgenmiş olan öldürücülük değerini (bu örnek için $W = 0.310899$) hem e değeriyle hem de öldürücülük eşik değeri ile kıyaslar. Bu

örnekte elde edilmiş olan W değeri, e değerinden büyük olmasına rağmen öldürücülük eşiğinden daha düşük hale gelmiştir. Bu durumda sistem tehdit için karşı tedbirler kullanmaya devam eder ama bunu en güçlü silahıyla değil, daha düşük maliyetli silahlarını sırayla kullanarak devam ettirir.

Ardışık yinelemeler sonrası sistemin çıktısı

```
detection 1 residual threat before weapon assignment: 0.310899
detection 1 residual threat after weapon assignment: 0.286027
detection 1 used weapon: machine gun
detection 1 used weapon cost: 8
detection is still lethal!!!
-----
press any key to continue
-----
detection 1 residual threat before weapon assignment: 0.286027
detection 1 residual threat after weapon assignment: 0.257424
detection 1 used weapon: naval artillery [deck gun]
detection 1 used weapon cost: 17
detection is still lethal!!!
-----
press any key to continue
-----
detection 1 residual threat before weapon assignment: 0.257424
detection 1 residual threat after weapon assignment: 0.223959
detection 1 used weapon: close-in weapon system [CIWS]
detection 1 used weapon cost: 29
detection is still lethal!!!
-----
press any key to continue
-----
detection 1 residual threat before weapon assignment: 0.223959
detection 1 residual threat after weapon assignment: 0.071667
detection 1 used weapon: surface to surface missile [SSM]
detection 1 used weapon cost: 74
detection is still lethal!!!
-----
press any key to continue
-----
detection 1 residual threat before weapon assignment: 0.071667
detection 1 residual threat after weapon assignment: 0.022933
detection 1 used weapon: surface to surface missile [SSM]
detection 1 used weapon cost: 74
```

Yukarıda görüldüğü üzere sistem toplam altı adet karşı tedbir amaçlı silah kullanarak tehdidin öldürücülük değerini $e = 0.05$ değerinin altına düşürür ve bu noktadan itibaren algılanan tehdit, savunulan araç için tehlike yaratmıyor kabul edilerek silah atama uygulaması durdurulur.

3.2.6 Tehdit değerlendirme algoritmalarının karşılaştırılması

Tehdit değerlendirme ve silah atama sisteminde en önemli kriterlerden biri, kullanılan tehdit değerlendirme algoritmalarının verimliliğidir. Bu sebeple aralarında karşılaştırma yapılması ve en verimli algoritmanın hangisi olduğuna karar verilmesi gerekir. Karşılaştırma kriteri olarak zaman kullanımı ve silah kullanımı açısından sisteme maliyeti göz önüne alınmıştır. Zaman kullanımından kasıt, kullanılan algoritmanın, algılanan tehdide ait öldürücülük değerini hesaplayabildiği zaman dilimidir. Daha önceden de belirtildiği gibi, herhangi bir tehdit altındayken, karşı tedbirlerin kullanılmasında zaman yönetimi çok önemlidir. Karşılaştırmanın diğer kriteri olan sisteme maliyet ise kullanılan silah sınıfı ve miktarlarının karşılaştırılmasıdır. Bilindiği üzere Bayes çıkarımı, Dempster – Shafer teorisi ve Transfer edilebilir inanış modeli algoritmalarının hepsi farklı çalışma metotlarına sahiptir; bu sebeple, birebir aynı özelliklere sahip tehditler algıladıklarında, farklı öldürücülük değerleri üretebilmektedirler. Silah atama algoritması da, kendi tasarımı doğrultusunda farklı öldürücülük değerleri için farklı silah atamaları yapabilmektedir. Savunma amaçlı kullanılabilen silahlar için bir maliyet fonksiyonu tanımlanmıştır (Çizelge 3.20). Bu fonksiyon ön tanımlı dosyada bulunur ve sistemin ilk çalıştırılmasında okunur.

Çizelge 3.20 Kullanılan silahlara ait maliyet tablosu

kullanılan silah	maliyet
surface to surface missile [SSM]	74
surface to air missile [SAM]	85
close-in weapon system [CIWS]	29
naval artillery [deck gun]	17
machine gun	8
flare	3

Silah atama sistemi, algılanan ve karşı tedbir kullanılması gereken tüm tehditler için kullanılan silahları ayrı ayrı hafızasında tutar ve silah atama uygulaması bittikten sonra kullanıcıya, hangi tehdit için ne kadar silah kullanıldığının maliyetini gösterir. Tehdit değerlendirme algoritmalarının karşılaştırılması ile ilgili ayrıntılı örnekler BULGULAR başlığı altında görülebilir.

4. BULGULAR

Tasarlanan tehdit değerlendirme ve silah atama sistemi çerçevesinde bulgular bölümünde, iki farklı inceleme yapılmıştır. İlk bölümde, sistemin dört adet tehdit algılanan durumda (her üç algoritma için de girdi olarak aynı tehdit modelleri kullanıldığı durumda), hangi algoritma kullanıldığında nasıl sonuçlar ürettiği incelenmiştir, ikinci bölümde ise her bir algoritmanın kendi üstün yönlerinin ortaya çıkartan tehdit modelleri girdi olarak kullanılmıştır.

4.1 Algoritmalarda Aynı Tipte Tehdit Modellerinin Kullanılması

Sistemde kullanılan üç algoritmanın birbirleriyle karşılaştırılabilmesi için, her üç algoritmanın aynı tip tehdit modelleriyle karşılaştığı durum ele alınmıştır. Sözü geçen karşılaştırma için dört adet tehdit modeli tanımlanmış ve bu modeller sisteme girdi olarak verilmiştir. Bu tehdit modellerinin özellikleri Çizelge 4.1'deki gibidir.

Çizelge 4.1 Algılanan tehditlerin özellikleri

özellikler	tehdit 1	tehdit 2	tehdit 3	tehdit 4
mobility	1 : slow [surface]	1 : slow [surface]	2 : fast [air]	2 : fast [air]
position	1 : inRange	1 : inRange	1 : inRange	1 : inRange
air platform type	-	-	4 : civilian	1 : fighter
surface platform type	4 : civilian	2 : frigate	-	-
iff response	1 : friend	2 : hostile	1 : friend	2 : hostile
threat level	1 : noThreat	3 : highThreat	1 : noThreat	3 : highThreat
primary weapon	5 : noWeapon	1 : [SSM]	4 : noWeapon	1 : [ASM]
secondary weapon	5 : noWeapon	2 : [CIWS]	4 : noWeapon	3 : machine gun
tertiary weapon	5 : noWeapon	4 : machine gun	4 : noWeapon	4 : noWeapon

Özelliklerinden anlaşıldığı üzere Tehdit 1 satıl kaynaklı ve zararsız, Tehdit 2 satıl kaynaklı ve son derece tehlikeli, Tehdit 3 hava kaynaklı ve zararsız, Tehdit 4 ise hava kaynaklı ve öldürücülüğünün yüksek olması beklenen tehditlerdir.

Bu bölümde; her üç algoritma için de aynı tehdit modelleri sisteme girdi olarak verilmiştir. Böylece aralarında karşılaştırma yapılabilecektir.

4.1.1 Bayes Çıkarımı kullanıldığında sistemin çıktısı

Çizelge 4.1’de özellikleri görülen tehditler ilk olarak Bayes çıkarımı kullanılarak değerlendirilmiştir. Tehdit değerlendirme algoritması olarak Bayes Çıkarımı kullanıldığında Tehdit 1, Tehdit 2, Tehdit 3, Tehdit 4 için sırasıyla 0.000014, 0.960327, 0.000007 ve 0.979389 değerleri hesaplanmıştır. Bu çıktı “Bayes Çıkarımı’nın hesapladığı öldürücülük değerleri”ndeki gibidir. Hesaplanan bu değerler beklenildiği gibidir; yani, Tehdit 2 ve Tehdit 4 savunulan araç için çok yüksek tehlike oluştururken, Tehdit 1 ve Tehdit 3 düşük öldürücülük değerleri sayesinde göz ardı edilirler (bu iki tehdidin de öldürücülük değerleri $e = 0.05$ değerinden düşüktür) ve karşı tedbir uygulanmasına gerek kalmaz.

Algoritmaların karşılaştırma kriterlerinden zaman yönetimi konusunda yapılan ölçümlerde, bu dört tehdide ait öldürücülük değerlerinin her birinin hesaplanması konusunda MATLAB⁶ yeterli çözünürlükte ölçüm alamadığı için hep 0.000000 olarak ölçülmüştür. Buradan Bayes Çıkarımı algoritmasının sistem gerekleri doğrultusunda, yeterince hızlı çalıştığı sonucuna varılabilir.

Bayes Çıkarımı’nın hesapladığı öldürücülük değerleri

lethality of the detected platform 1	: 0.000014
lethality of the detected platform 2	: 0.960327
lethality of the detected platform 3	: 0.000007
lethality of the detected platform 4	: 0.979389

Öldürücülük değerlerinin hesaplanmasından sonra, yukarıda içeriği görülen liste silah atama sistemine gönderilir. Silah atama sistemi, bu listedeki değerleri ilgili platform numaralarıyla birlikte büyükten küçüğe sıralar. Bu sıralama Tehdit 4, Tehdit 2, Tehdit 1, Tehdit 3 şeklinde oluşur. Daha önce belirtildiği gibi Tehdit 1 ve Tehdit 3, silah atama sistemi içinde hiçbir işleme tabi tutulmazlar. Sistemin asıl üzerinde çalıştıkları Tehdit 2 ve Tehdit 4’tür. Tehlike arz eden bu iki tehdit için sistemin çıktısı “Bayes Çıkarımına göre silah atama sisteminin çıktısı” bölümündeki gibi olur.

⁶ Mathworks şirketine ait bir bilgisayar programı

Bayes Çıkarımına göre silah atama sisteminin çıktısı

```
detection 4 residual threat before weapon assignmen: 0.979389
detection 4 residual threat after weapon assignmen: 0.293817
detection 4 used weapon: surface to air missile [SAM]
detection 4 used weapon cost: 85
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.960327
detection 2 residual threat after weapon assignment: 0.307305
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.307305
detection 2 residual threat after weapon assignment: 0.282720
detection 2 used weapon: machine gun
detection 2 used weapon cost: 8
detection is still lethal!!!
-----
press any key to continue
-----
detection 4 residual threat before weapon assignmen: 0.293817
detection 4 residual threat after weapon assignmen: 0.270311
detection 4 used weapon: machine gun
detection 4 used weapon cost: 8
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.282720
detection 2 residual threat after weapon assignment: 0.254448
detection 2 used weapon: naval artillery [deck gun]
detection 2 used weapon cost: 17
detection is still lethal!!!
-----
press any key to continue
-----
detection 4 residual threat before weapon assignmen: 0.270311
detection 4 residual threat after weapon assignmen: 0.213546
detection 4 used weapon: naval artillery [deck gun]
detection 4 used weapon cost: 17
detection is still lethal!!!
-----
press any key to continue
-----
```

Bayes Çıkarımına göre silah atama sisteminin çıktısı (devam)

```
detection 2 residual threat before weapon assignment: 0.254448
detection 2 residual threat after weapon assignment: 0.221370
detection 2 used weapon: close-in weapon system [CIWS]
detection 2 used weapon cost: 29
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.221370
detection 2 residual threat after weapon assignment: 0.070838
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74
detection is still lethal!!!
-----
press any key to continue
-----
detection 4 residual threat before weapon assignmen: 0.213546
detection 4 residual threat after weapon assignmen: 0.064064
detection 4 used weapon: surface to air missile [SAM]
detection 4 used weapon cost: 85
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.070838
detection 2 residual threat after weapon assignment: 0.022668
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74
detection 4 residual threat before weapon assignmen: 0.064064
detection 4 residual threat after weapon assignmen: 0.019219
detection 4 used weapon: surface to air missile [SAM]
detection 4 used weapon cost: 85

-----cost report-----
detection 1 total weapon cost: 0
detection 2 total weapon cost: 276
detection 3 total weapon cost: 0
detection 4 total weapon cost: 280
-----
```

Yukarıdaki çıktılarda görülebildiği gibi silah atama sistemi sadece Tehdit 2 ve Tehdit 4'ü işlemeye almıştır. Sözü geçen tehditlerin ikisinde sahip oldukları öldürücülük değerleri, öldürücülük eşik değerinden yüksek olduğu için ilk aşamada düşük güce sahip silahlar yerine en güçlü silahlar kullanılmıştır (Tehdit 4 için SAM ve Tehdit 2 için SSM). Her iki tehdit için de ilk yinelemeden önce 0.95'in üzerinde olan öldürücülük değerleri, ilk yinelemede en güçlü silahlarla savunma yapılmasının ardından 0.30

civarında değerlere düşmüştür. Bu noktadan sonra daha düşük güçte silahlar kullanılarak bu tehditlerin öldürücülük değerleri düşürülmeye çalışılmıştır ama yeterli başarı sağlanamadığı için her iki tehdit için de tekrardan SSM ve SAM kullanılarak öldürücülük değerleri $e = 0.05$ değerinin altına çekilmiştir.

Sistem tüm tehditler bertaraf edildikten sonra, tüm süreç içerisinde tehditlere karşı yapılan eylemlerin sisteme maliyetini operatöre sunmuştur. Tehdit 2'nin sisteme maliyeti 276 birimken, Tehdit 4'ün maliyeti 280 birime ulaşmıştır.

4.1.2 Dempster – Shafer teorisi kullanıldığında sistemin çıktısı

Çizelge 4.1'de özellikleri görülen tehditler, Dempster – Shafer teorisi kullanılarak değerlendirildiklerinde; Tehdit 1, Tehdit 2, Tehdit 3, Tehdit 4 için sırasıyla 0.000000, 0.980136, 0.000000 ve 0.772346⁷ değerleri hesaplanmıştır. Bayes Çıkarımı hesaplamasında olduğu gibi; DST'de de, Tehdit 2 ve Tehdit 4 savunulan araç için çok yüksek tehlike oluştururken, Tehdit 1 ve Tehdit 3 düşük öldürücülük değerleri sayesinde göz ardı edilirler (bu iki tehdidin de öldürücülük değerleri $e = 0.05$ değerinden düşüktür) ve karşı tedbir uygulanmasına gerek kalmaz.

Zaman yönetimi konusunda da DST, Bayes çıkarımıyla benzer şekilde çıktılar üretmiştir. Yapılan ölçümlerde, bu dört tehdide ait öldürücülük değerlerinin her birinin hesaplanması konusunda MATLAB yeterli çözünürlükte ölçüm alamadığı için hep 0.000000 olarak ölçülmüştür. Buradan Dempster – Shafer teorisinde yeteri kadar hızlı çalıştığı sonucuna varılabilir.

Dempster – Shafer Teorisi'nin hesapladığı öldürücülük değerleri

lethality of the detected platform 1	: 0.000000
lethality of the detected platform 2	: 0.980136
lethality of the detected platform 3	: 0.000000
lethality of the detected platform 4	: 0.772346

⁷ DST algoritmasının, Bayes Çıkarımına göre daha düşük öldürücülük değeri hesaplaması TARTIŞMA ve SONUÇ bölümünde yorumlanmıştır.

Dempster – Shafer teorisine göre hesaplanan bu öldürücülük değerleri silah atama sistemine gönderilir. Silah atama sistemi, bu listedeki değerleri ilgili platform numaralarıyla birlikte büyükten küçüğe sıralar. Bu sıralama Tehdit 2, Tehdit 4, Tehdit 1, Tehdit 3 şeklinde oluşur. Algılanan tehditler için sistemin çıktısı, “Dempster – Shafer Teorisine göre silah atama sisteminin çıktısı” bölümündeki gibi olur.

Dempster – Shafer Teorisine göre silah atama sisteminin çıktısı

```
detection 2 residual threat before weapon assignment: 0.980136
detection 2 residual threat after weapon assignment: 0.313644
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74
detection is still lethal!!!
```

```
-----
press any key to continue
```

```
-----
detection 4 residual threat before weapon assignment: 0.772346
detection 4 residual threat after weapon assignment: 0.710558
detection 4 used weapon: machine gun
detection 4 used weapon cost: 8
detection is still lethal!!!
```

```
-----
press any key to continue
```

```
-----
detection 4 residual threat before weapon assignment: 0.710558
detection 4 residual threat after weapon assignment: 0.653714
detection 4 used weapon: machine gun
detection 4 used weapon cost: 8
detection is still lethal!!!
```

```
-----
press any key to continue
```

```
-----
detection 4 residual threat before weapon assignment: 0.653714
detection 4 residual threat after weapon assignment: 0.601417
detection 4 used weapon: machine gun
detection 4 used weapon cost: 8
detection is still lethal!!!
```

```
-----
press any key to continue
```

```
-----
detection 4 residual threat before weapon assignment: 0.601417
detection 4 residual threat after weapon assignment: 0.475119
detection 4 used weapon: naval artillery [deck gun]
detection 4 used weapon cost: 17
detection is still lethal!!!
```

```
-----
press any key to continue
```

Dempster – Shafer Teorisine göre silah atama sisteminin çıktısı (devam)

```
detection 4 residual threat before weapon assignment: 0.475119
detection 4 residual threat after weapon assignment: 0.142536
detection 4 used weapon: surface to air missile [SAM]
detection 4 used weapon cost: 85
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.313644
detection 2 residual threat after weapon assignment: 0.288552
detection 2 used weapon: machine gun
detection 2 used weapon cost: 8
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.288552
detection 2 residual threat after weapon assignment: 0.259697
detection 2 used weapon: naval artillery [deck gun]
detection 2 used weapon cost: 17
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.259697
detection 2 residual threat after weapon assignment: 0.225936
detection 2 used weapon: close-in weapon system [CIWS]
detection 2 used weapon cost: 29
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.225936
detection 2 residual threat after weapon assignment: 0.072300
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74
detection is still lethal!!!
-----
press any key to continue
-----
detection 4 residual threat before weapon assignment: 0.142536
detection 4 residual threat after weapon assignment: 0.042761
detection 4 used weapon: surface to air missile [SAM]
detection 4 used weapon cost: 85
detection 2 residual threat before weapon assignment: 0.072300
detection 2 residual threat after weapon assignment: 0.023136
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74

-----cost report-----
detection 1 total weapon cost: 0
detection 2 total weapon cost: 276
detection 3 total weapon cost: 0
detection 4 total weapon cost: 211
-----
```

“Dempster – Shafer Teorisine göre silah atama sisteminin çıktısı” bölümünde görüldüğü üzere, silah atama sistemi sadece Tehdit 2 ve Tehdit 4’ü işlemeye almıştır. Sözü geçen tehditlerden sadece Tehdit 2’nin öldürücülük değeri, öldürücülük eşik değerinden yüksek olduğu için ilk aşamada düşük güce sahip silahlar yerine en güçlü silahlar kullanılmıştır (Tehdit 2 için SSM). Tehdit 2 için, ilk yinelemede en güçlü silahlarla savunma yapılmasının ardından öldürücülük değeri 0.31 civarına düşürülmüştür. Bu noktadan sonra daha düşük güçte silahlar kullanılarak bu tehditlerin öldürücülük değerleri düşürülmeye çalışılmıştır ama yeterli başarı sağlanamadığı için her iki tehdit için de tekrardan SSM ve SAM kullanılarak öldürücülük değerleri $e = 0.05$ değerinin altına çekilmiştir.

Sistem tüm tehditler bertaraf edildikten sonra, tüm süreç içerisinde tehditlere karşı yapılan eylemlerin sisteme maliyetini operatöre sunmuştur. Tehdit 2’nin sisteme maliyeti 276 birimken, Tehdit 4’ün maliyeti 211 birimde kalmıştır. Algoritmaların farklılıkları bu sonuçtan görülebilir. Bayes Çıkarımında aynı özelliklere sahip Tehdit 4’ün sisteme maliyeti 280 birimken, Dempster – Shafer teorisi kullanıldığında aynı tehdidin maliyeti 211 birime düşmüştür; ki bu değişim 25% anlamına gelmektedir ve sistemin Bayes çıkarımı yerine DST kullanması silah kullanımı açısından sistemin tasarruf etmesini sağlamıştır.

4.1.3 Transfer edilebilir inanış modeli kullanıldığında sistemin çıktısı

Bayes çıkarımı ve Dempster – Shafer teorisi testlerinde olduğu gibi Transfer edilebilir inanış modeli testleri için de Çizelge 4.1’de özellikleri görülen tehdit modelleri kullanılmıştır. Transfer edilebilir inanış modeli kullanılarak yapılan hesaplamalara göre; Tehdit 1, Tehdit 2, Tehdit 3, Tehdit 4 için sırasıyla 0.000000, 0.980136, 0.000000 ve 0.772346⁸ değerleri hesaplanmıştır. Önceki iki algortmada olduğu gibi TBM’de de, Tehdit 2 ve Tehdit 4 savunulan araç için çok yüksek tehlike oluştururken, Tehdit 1 ve Tehdit 3 düşük öldürücülük değerleri sayesinde göz ardı edilirler (bu iki tehdidin de

⁸ TBM algoritmasının, Bayes Çıkarımına göre daha düşük öldürücülük değeri hesaplaması TARTIŞMA ve SONUÇ bölümünde yorumlanmıştır.

öldürücülük değerleri $e = 0.05$ değerinden düşüktür) ve karşı tedbir uygulanmasına gerek kalmaz.

Zaman yönetimi konusunda da TBM, kullanılan diğer algoritmalarından aşağı kalmamış ve yapılan ölçümlerde, bu dört tehdide ait öldürücülük değerlerinin her birinin hesaplanması konusunda MATLAB yeterli çözünürlükte ölçüm alamadığı için hep 0.000000 olarak ölçülmüştür. Buradan Transfer edilebilir inanış modeli algoritmasının da en az diğer iki algoritma kadar hızlı çalıştığı sonucuna varılabilir.

Transfer Edilebilir İnanış Modeli'nin hesapladığı öldürücülük değerleri

lethality of the detected platform 1	: 0.000000
lethality of the detected platform 2	: 0.980136
lethality of the detected platform 3	: 0.000000
lethality of the detected platform 4	: 0.772346

Transfer edilebilir inanış modeli'ne göre hesaplanan bu öldürücülük değerleri silah atama sistemine gönderilir. Silah atama sistemi, bu listedeki değerleri ilgili platform numaralarıyla birlikte büyükten küçüğe sıralar. Bu sıralama Tehdit 2, Tehdit 4, Tehdit 1, Tehdit 3 şeklinde oluşur. Algılanan tehditler için sistemin çıktısı, "Transfer Edilebilir İnanış Modeli'ne göre silah atama sisteminin çıktısı" bölümündeki gibi olur.

Transfer Edilebilir İnanış Modeli'ne göre silah atama sisteminin çıktısı

```
detection 2 residual threat before weapon assignment: 0.980136
detection 2 residual threat after weapon assignment: 0.313644
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74
detection is still lethal!!!
-----
press any key to continue
-----
detection 4 residual threat before weapon assignmen: 0.772346
detection 4 residual threat after weapon assignmen: 0.710558
detection 4 used weapon: machine gun
detection 4 used weapon cost: 8
detection is still lethal!!!
-----
press any key to continue
-----
```

Transfer Edilebilir İnanış Modeli'ne göre silah atama sisteminin çıktısı (devam)

```
detection 4 residual threat before weapon assignmen: 0.710558
detection 4 residual threat after weapon assignmen: 0.653714
detection 4 used weapon: machine gun
detection 4 used weapon cost: 8
detection is still lethal!!!
```

```
-----
press any key to continue
-----
```

```
detection 4 residual threat before weapon assignmen: 0.653714
detection 4 residual threat after weapon assignmen: 0.601417
detection 4 used weapon: machine gun
detection 4 used weapon cost: 8
detection is still lethal!!!
```

```
-----
press any key to continue
-----
```

```
detection 4 residual threat before weapon assignmen: 0.601417
detection 4 residual threat after weapon assignmen: 0.475119
detection 4 used weapon: naval artillery [deck gun]
detection 4 used weapon cost: 17
detection is still lethal!!!
```

```
-----
press any key to continue
-----
```

```
detection 4 residual threat before weapon assignmen: 0.475119
detection 4 residual threat after weapon assignmen: 0.142536
detection 4 used weapon: surface to air missile [SAM]
detection 4 used weapon cost: 85
detection is still lethal!!!
```

```
-----
press any key to continue
-----
```

```
detection 2 residual threat before weapon assignment: 0.313644
detection 2 residual threat after weapon assignment: 0.288552
detection 2 used weapon: machine gun
detection 2 used weapon cost: 8
detection is still lethal!!!
```

```
-----
press any key to continue
-----
```

```
detection 2 residual threat before weapon assignment: 0.288552
detection 2 residual threat after weapon assignment: 0.259697
detection 2 used weapon: naval artillery [deck gun]
detection 2 used weapon cost: 17
detection is still lethal!!!
```

```
-----
press any key to continue
-----
```

Transfer Edilebilir İnanış Modeli'ne göre silah atama sisteminin çıktısı (devam)

```
detection 2 residual threat before weapon assignment: 0.259697
detection 2 residual threat after weapon assignment: 0.225936
detection 2 used weapon: close-in weapon system [CIWS]
detection 2 used weapon cost: 29
detection is still lethal!!!
-----
press any key to continue
-----
detection 2 residual threat before weapon assignment: 0.225936
detection 2 residual threat after weapon assignment: 0.072300
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74
detection is still lethal!!!
-----
press any key to continue
-----
detection 4 residual threat before weapon assignmen: 0.142536
detection 4 residual threat after weapon assignmen: 0.042761
detection 4 used weapon: surface to air missile [SAM]
detection 4 used weapon cost: 85
detection 2 residual threat before weapon assignment: 0.072300
detection 2 residual threat after weapon assignment: 0.023136
detection 2 used weapon: surface to surface missile [SSM]
detection 2 used weapon cost: 74

-----cost report-----
detection 1 total weapon cost: 0
detection 2 total weapon cost: 276
detection 3 total weapon cost: 0
detection 4 total weapon cost: 211
-----
```

“Transfer Edilebilir İnanış Modeli'ne göre silah atama sisteminin çıktısı” bölümünde görüldüğü üzere, silah atama sistemi sadece Tehdit 2 ve Tehdit 4'ü işlemeye almıştır. Sözü geçen tehditlerden sadece Tehdit 2'nin öldürücülük değeri, öldürücülük eşik değerinden yüksek olduğu için ilk aşamada düşük güce sahip silahlar yerine en güçlü silahlar kullanılmıştır (Tehdit 2 için SSM). Tehdit 2 için, ilk yinelemede en güçlü silahlarla savunma yapılmasının ardından öldürücülük değeri 0.31 civarına düşürülmüştür. Bu noktadan sonra daha düşük güçte silahlar kullanılarak bu tehditlerin öldürücülük değerleri düşürülmeye çalışılmıştır ama yeterli başarı sağlanamadığı için her iki tehdit için de tekrardan SSM ve SAM kullanılarak öldürücülük değerleri $e = 0.05$ değerinin altına çekilmiştir.

Sistem tüm tehditler bertaraf edildikten sonra, tüm süreç içerisinde tehditlere karşı yapılan eylemlerin sisteme maliyetini operatöre sunmuştur. Tehdit 2'nin sisteme maliyeti 276 birimken, Tehdit 4'ün maliyeti 211 birimde kalmıştır. Algoritmaların farklılıkları bu sonuçtan görülebilir. Bayes Çıkarımında aynı özelliklere sahip Tehdit 4'ün sisteme maliyeti 280 birimken, Transfer edilebilir inanış modeli kullanıldığında aynı tehdidin maliyeti 211 birime düşmüştür; ki bu değişim 25% anlamına gelmektedir ve sistemin TBM algoritmasını kullanması DST ile kıyaslandığında bir yarar sağlamasa da, Bayes Çıkarımına göre daha avantajlı olduğu ortadadır.

4.2 Algoritmalarda Farklı Tipte Tehdit Modellerinin Kullanılması

Algoritmalarda Aynı Tipte Tehdit Modellerinin Kullanılması bölümünde, sistemin aynı ortamda verdiği sonuçlar incelendikten sonra; sistemdeki herbir algoritmanın kendi üstünlüklerini ortaya koyabilmeleri için farklı tehdit modellerinin kullanıldığı testler gerçekleştirilmiştir. Bayes çıkarımı yöntemi, kendisine verilen olasılık değerlerini, hiçbir ekleme yapmadan, standart olasılık değerleri gibi kullanarak, sisteme herhangi bir esneklik getirmediği için Bayes çıkarımı algoritması için herhangi bir özel durum oluşturmak gerekmemektedir. Diğer taraftan Dempster – Shafer teorisi ve Transfer edilebilir inanış modeli algoritmaları, sistemdeki belirsizlikleri dikkate alarak öldürücülük değerleri hesaplayabildikleri için, bu iki algoritmanın üstünlüklerini ortaya koyan örnek tehdit modelleri ile testler yapılması uygun olacaktır.

4.2.1 Dempster – Shafer teorisinin avantajları

Önceki bölümlerde de belirtildiği gibi, Dempster – Shafer teorisinin en önemli özelliği, sistemdeki alıcılardan kesin veriler gelmediği durumlarda da öldürücülük değerini hesaplayabilmesidir. Bu durumu örnekleyebilmek için Çizelge 3.11'de tanımlanmış olan tüm alıcılardan “belirsiz” değerinin geldiği bir tehdit modelinin gerçekleştiği durumu inceleyebiliriz.

Çizelge 4.2 Dempster – Shafer teorisi için belirsizlik örneği

özellikler	tehdit
mobility	1 : unknown
position	4 : unknown
air platform type	3 :unknown

surface platform type	5 : unknown
iff response	5 : unknown
threat level	5 : unknown
primary weapon	4 : unknown
secondary weapon	6 : unknown
tertiary weapon	5 : unknown

Çizelge 4.2’deki veriler doğrultusunda sistem çalıştırıldığı zaman, sistem 0.013436 gibi bir öldürücülük değeri üretmektedir.

Belirsiz verilere göre DST öldürücülük değeri

```

Command Window
lethality of the detected platform 1      : 0.013436
-----
press any key to continue
-----

-----cost report-----
detection 1 total weapon cost: 0
-----

```

Bu değer, eşik değerinden daha düşük olduğu için, sistem bu tehdidi, tehditle ilgili daha sağlıklı veriler elde edilene kadar gözardı eder. Aynı tehditle ilgili kesin veriler, alıcılardan gelmeye başladığı zaman, sistem tehdidi tekrar değerlendirir, ve daha sağlıklı bir öldürücülük üreterek, tehdide karşı savunma yapıp yapılmayacağına karar verir. Sistemin; belirsiz tehditler için düşük öldürücülük değerleri üretmesi tamamen tasarımsal bir sonuçtur. Eğer operatör, belirsiz tehditlerin düşman olarak algılanmasını, ve sistemin bu tip tehditler için yüksek öldürücülük değerleri hesaplamasını isterse, sistemdeki ön tanımlı dosyayı, operasyondan önce bu şekilde düzenleyerek arzu ettiği sonuca ulaşabilir.

4.2.2 Transfer edilebilir inanış modeli algoritmasının avantajları

Transfer edilebilir inanış modelinde de, Dempster – Shafer teorisinde olduğu gibi, sistem belirsizlik durumlarını dikkate alır ve öldürücülük değerlerini buna göre hesaplar. Sistemin tasarımında her ne kadar, Transfer edilebilir inanış modeli kullanılacak olan durumlarda sisteme “belirsiz” şeklinde veriler girilemiyor olsa da, Transfer edilebilir inanış modeli, alıcılardan gelen veriyi hiç bir zaman %100 güvenli

olarak algılamadığı için ve alıcıların herbiri için sistemde α , indirgeme faktörü kullanıldığı için, belirsizlikler sistem içerisinde ele alınmış olur. Burada önemli olan nokta, indirgeme faktörünün operasyon öncesinde, öntanımlı dosya düzenlenerek operatör tarafından belirlenebiliyor olmasıdır. Yani operatör, operasyonun gerekleri doğrultusunda, verilerdeki belirsizlik üzerinde direk etkiye sahiptir.

5. TARTIŞMA ve SONUÇ

5.1 Tartışma

BULGULAR bölümünde, sistemin belirli yapıdaki tehdit modelleri algılandığında, ve bu tehdit modelleri, Bayes çıkarımı, Dempster – Shafer teorisi ve Transfer edilebilir inanış modeli algoritmaları ayrı ayrı kullanılarak değerlendirildiğinde, elde edilen sonuçlar ayrıntılarıyla incelenmiştir. Bu bölümde ise elde edilen bu sonuçlar kullanılarak, sistemde kullanılan üç farklı tehdit değerlendirme algoritmasının birbirlerine göre avantajları ve dezavantajları ele alınacaktır.

Bu üç algoritma temel çalışma anlayışları açısından iki gruba ayrılabilir. İlk grupta Bayes çıkarımı tek başına yer alır. Dempster – Shafer teorisi ve Transfer edilebilir inanış modeli ise diğer grubu oluşturur. Bu iki grubun birbirinden farklı noktası, gerçekleştirilebilmeleri için ihtiyaç duydukları bilgi seviyesidir. Bayes çıkarımı herhangi bir hesaplama yapabilmek için, Bayes ağı'nda tanımlanmış olan tüm değişkenler için kesin değerlere ihtiyaç duyar; diğer taraftan Dempster – Shafer teorisi ve Transfer edilebilir inanış modeli algoritmaları, değişen değerleriyle ilgili sağladıkları esneklikler sayesinde bir adım öne çıkarlar. Bu konuyu biraz açarsak eğer; Boudraa *et al.* (2004)'e göre Bayes çıkarımının en temel kısıtlaması belirsizlik ölçümlerinde kesin sonuç vermekten uzak olmasıdır. Yine Boudraa *et al.* (2004)'e göre inanış derecesi belli bir değer üzerinde değil, bir değerler kümesi üzerinde yoğunlaşıyorsa bu tip durumlar belirsizliği bir değer olarak kabul eden Dempster – Shafer teorisi sayesinde daha rahat ele alınabilirler. Benzer şekilde, Smets'in (2000) belirttiği üzere Transfer edilebilir inanış modelinin klasik Bayes yaklaşımına göre avantajı, içerdği esneklik ve kısmi inanışlara ait tüm durumları tasvir edebilmesidir. Koks (2003)'de Bayes çıkarımı ile Dempster – Shafer teorisi arasındaki fark için benzer görüşler öne sürmüştür. Koks (2003)'e göre; bu iki algoritma arasındaki temel fark Bayes çıkarımının klasik anlamda olasılıkları, bir deneyin birçok kez tekrarlanması sırasında bir olayın ne sıklıkla meydana gelmesini yansıtırken; diğer taraftan Dempster –Shafer teorisi bir ölçüm yapıldığı zaman, doğada olabilecek olayları değil, bizim bilgi seviyemizi yansıtır. Örnek olarak, Bayes çıkarımı değişken değeri olarak “*unknown emitter type*” gibi bir durumu kullanmaz; ama, Dempster – Shafer teorisinde “*unknown emitter type*” değişkenin

gerçek değeriymiş gibi değerlendirilebilir. Koks (2003), Bayes çıkarımının tersine, Dempster – Shafer teorisi karar verilemeyen durumların oluşmasına izin verir şeklinde algoritmalar arasındaki farkı açıklar. Bu söylemlerden de anlaşıldığı üzere Bayes çıkarımı klasik anlamda olasılıklardan oluşur ve tehdit değerlendirme işlemini yapabilmesi için sistemdeki tüm alıcılardan kesin veriler gelmesi gerekir; diğer taraftan Dempster – Shafer teorisi ve Transfer edilebilir inanış modeli algoritmaları, esneklikleriyle öne çıkarlar ve tehdit değerlendirmesi yapabilmeleri için kesin verilere ihtiyaç duymazlar. DST algoritmasının bu özelliğini, sistem gerçekleşmesi sırasında ön plana çıkarabilmek için alıcılardan DST’ye gelebilecek veri kümelerinin her birine “belirsiz” seçeneği eklenmiştir. Yani, DST algoritmasına kesin veriler gelebileceği gibi, algılanan tehditle ilgili emin olunamayan durumlarda “belirsiz” verisi de gelebilir; ve DST algoritması bu durumda çalışmaya devam eder. Diğer taraftan, aynı özelliğe sahip TBM’in gerçekleşmesinde “belirsiz” seçeneği kullanılmamıştır; ama bir tanım kümesine ait tüm verilere ait tüm kombinasyonlara gerekli kütle değerleri atanmıştır. Yani iki opsiyon arasında kalındığı bir durumda, opsiyonlardan birini seçmek yerine, ikisinin kombinasyonuna gerekli değer verilmiştir, ve bu şekilde bir belirsizlik / karar verilememesi durumu oluştuğunda sistemin sorunsuz çalışmaya devam etmesi sağlanmıştır. Bu bilgiler doğrultusunda, Bayes çıkarımı algoritmasının gerçek verilerle çalışması dolayısıyla en güvenilir öldürücülük değerini hesapladığı söylenebilir. Dempster – Shafer teorisi ve Transfer edilebilir inanış mmodeli algoritmalarında ise, hem belirsizlik dikkate alındığı, hem de alıcılardan gelen verilerden öldürücülük değeri hesaplanması sırasında tanım kümelerinin eşlenebilmesi için bir eşleme ara katmanı kullanılması sebebiyle, veri kaybı meydana gelmektedir. Bu yüzden bu iki algoritmanın, Bayes çıkarımına göre daha az güvenilir olduğu söylenebilir.

Sistemde kullanılan üç farklı algoritmanın birbirleriyle kıyaslanabilmeleri için 2 farklı yol izlenmiştir. İlki, kullanılan algoritmanın, algılanan tehdide ait öldürücülük değerini ne kadar hızlı hesaplayabildiğidir. Bu kıyaslama için MATLAB programında, tehditle ilgili bilgiler alındıktan, öldürücülük değeri hesaplanıp ekrana yansıtılana kadar geçen süre ölçülmüştür. Elde edilen sonuçlar üç algoritma için de birbiriyle aynıdır. MATLAB’da yapılan ölçümlerde üç algoritma için de öldürücülük değeri hesaplama süresi 0.000000 olarak ölçülmüştür. Bu sonuç, ölçümlerin yeterli çözünürlükte

yapılmamasına rağmen, tüm algoritmaların saniyenin milyonda birinden daha kısa sürede öldürücülük değerini hesaplayabildiğini göstermektedir. Gemi savunma sistemi gibi zaman yönetiminin hayati önem taşıdığı bir sistemde, elde edilen bu sonuç tatmin edicidir.

Algoritmaların birbirleriyle kıyaslanmalarında kullanılan diğer kriter ise, kullanılan algoritmanın hesapladığı öldürücülük değerinin sisteme maliyetidir. BULGULAR bölümünde elde edilen çıktılar incelendiğinde, aynı özelliklere sahip tehditler için en yüksek maliyetin Bayes çıkarımı algoritması kullanıldığında ortaya çıktığı gözlenebilir. Bunun sebebi Bayes çıkarımı kullanılarak öldürücülük değeri hesaplanmasında veri kaybı bulunmamasıdır. Bayes Çıkarımı'nın 0.90 civarında öldürücülük değeri hesapladığı bir tehdit için, DST ve TBM 0.70'li değerlerde öldürücülük hesaplayabilmektedir. Aynı bölümde dikkat çeken bir başka nokta ise DST ve TBM'in aynı özelliklere sahip tehditler için birebir aynı öldürücülük değerlerini ve dolayısıyla aynı maliyetleri ortaya çıkarmalarıdır. Bu durumun sebebi, TBM'in, her ne kadar çift seviyeli, bahis dönüşümü kullanan bir algoritma olsa da, son aşamada alıcılardan gelen verileri aynen DST'de olduğu gibi Dempster birleştirme kuralı kullanarak birleştirmesinden kaynaklanır.

5.2 Sonuç

Günümüzde savaş teknolojilerinin geldiği nokta, birçok kişinin sadece on yıl önce bile hayal edemedikleri kadar ileridedir. Bu teknolojiler bir taraf için büyük avantaj sağlarken diğer taraf için de ölümcül tehlikeler yaratmaktadır. Bu çalışma da, gemi savunma sistemlerinde, algılanan tehdidin değerlendirilmesi ve eğer gerekiyorsa bu tehdiye karşı gerekli tedbirlerin alınması üzerine yoğunlaşmıştır. Tehdidin değerlendirilmesinde üç farklı algoritma (Bayes çıkarımı, Dempster – Shafer teorisi, Transfer edilebilir inanış modeli) kullanılmıştır. Farklı kriterlere göre, kullanılan bu algoritmalar birbirleriyle karşılaştırılmış ve okuyucuya bir bakış açısı kazandırılmaya çalışılmıştır. Karşı tedbirlerle ilgili olan silah atama sistemi içinse genel bir algoritma kullanılmıştır. Genel olarak bakıldığında silah atama sistemi zaten her türlü savunma durumunda kullanılmaktadır. Burada önemli olan ise algılanan tehditlerin doğru olarak değerlendirilebilmesi ve bu tehditlere karşı uygulanacak tedbirlerin doğru sıralama ve

zaman yönetimiyle kullanılmasıdır. Yapılacak en ufak bir hata ölümcül sonuçlar ortaya çıkmasına sebep olabilir.

KAYNAKLAR

- Boudraa, A., Bentabet, A., Salzenstein, F. and Guillon, L. 2004. Dempster-Shafer's Basic Probability Assignment Based on Fuzzy Membership Functions. *Electronic Letters on Computer Vision and Image Analysis* 4(1):1-9.
- Chalmers, B.A. 1993. A Planning Model for Real-Time Defence Resource Allocation and Scheduling in a Naval Command and Control System. *Canadian Conference on Electrical and Computer Engineering*, 1993, vol.1; pages 341-344.
- Das, B. 1999. Representing Uncertainties Using Bayesian Networks. DSTO Publications, 66, Australia.
- Elouedi, Z., Mellouli, K. and Smets, Ph. 2004, Assessing sensor reliability for multisensor data fusion within the Transferable Belief Model. *IEEE Transactions on Systems, Man and Cybernetics B*. v34 i1. 782-787.
- Huang, P. and Kar, P. 1994. An Autonomous Optimal Weapon Assignment Algorithm For Ship Self Defense. *IEEE International Conference on Systems, Man, and Cybernetics*, 1994, Volume 3; pages 2544-2549.
- Koks, D. 2003. An Introduction to Bayesian and Dempster – Shafer Data Fusion. DSTO Systems Sciences Laboratory, 44, Australia.
- Smets, P. 2000. Belief Functions and the Transferable Belief Model.
- Zou Yi, Ho Yeong Khing, Chua Chin Seng and Zhou Xiao Wei, 2000. Multi-ultrasonic sensor fusion for autonomous mobile robots, *Sensor Fusion: Architectures, Algorithms and Applications IV*; Proceedings of SPIE 4051, 314 – 321

USDOD. 2003. DOD Dictionary of Military and Associated Terms: NATO Only Terms. United States of America: Joint Doctrine Division, J-7, Joint Staff, Department of Defense. December 17, 2003.

ÖZGEÇMİŞ

Adı Soyadı : KEREM KALCI

Doğum Yeri : ANKARA

Doğum Tarihi : 04.06.1980

Medeni Hali : Bekar

Yabancı Dili : İngilizce

Eğitim Durumu:

Lise : Ankara Cumhuriyet Lisesi 1997

Lisans : Bilkent Üniversitesi Elektrik ve Elektronik Mühendisliği 2004

Çalıştığı Kurumlar:

HAVELSAN A.Ş 2004 - ...