Two Uncertain Things

Sari Haj Hussein[1]

APSIA Breakfast Talk
[1]Interdisciplinary Center for Security, Reliability and Trust
University of Luxembourg

2011-07-06

Sample Space (Frame of Discernment)

- A set of possible worlds/states/elementary outcomes $W = \{w_1, ..., w_n\}$
- An agent considers some subset of W possible and this subset qualitatively measures her uncertainty
- The more worlds an agent considers possible, the more uncertain she is, and the less she knows

- When throwing a dice, the sample space would be $W = \{w_1, w_2, w_3, w_4, w_5, w_6\}$, w_i means the dice lands i
- An agent can consider the dice landing on an even number possible, that is the subset $W = \{w_2, w_4, w_6\}$

Sample Space (Frame of Discernment)

- A set of possible worlds/states/elementary outcomes $W = \{w_1, ..., w_n\}$
- An agent considers some subset of W possible and this subset qualitatively measures her uncertainty
- The more worlds an agent considers possible, the more uncertain she is, and the less she knows

- When throwing a dice, the sample space would be $W = \{w_1, w_2, w_3, w_4, w_5, w_6\}$, w_i means the dice lands i
- An agent can consider the dice landing on an even number possible, that is the subset $W = \{w_2, w_4, w_6\}$

- A method for representing uncertainty
- Given a sample space $W = \{w_1, ..., w_n\}$, a probability measure assigns to each world w_i a number (a probability)
- This probability describes the likelihood that the world w_i is the actual world

Algebra

- An algebra over W is a set F of subsets of W that contains W and is closed under union and complementation
- If A and B are in F, then so are $A \cup B$ and $\overline{A}$

Probability Measure

- Given a sample space W, a probability measure is a function $\mu : F \to [0, 1]$ that satisfies the following two properties:
  - $\mu(W) = 1$
  - Finite additivity: $\mu(A \cup B) = \mu(A) + \mu(B)$ if A and B are disjoint sets in F

Algebra

- An algebra over W is a set F of subsets of W that contains W and is closed under union and complementation
- If A and B are in F, then so are $A \cup B$ and $\overline{A}$

Probability Measure

- Given a sample space W, a probability measure is a function $\mu : F \to [0, 1]$ that satisfies the following two properties:
  - $\mu(W) = 1$
  - Finite additivity: $\mu(A \cup B) = \mu(A) + \mu(B)$ if A and B are disjoint sets in F

- When flipping a coin, the sample space would be $W = \{w_H, w_T\}$
- An algebra: $F = \{\{w_H\}, \{w_T\}, \{w_H, w_T\}\}$
- A probability measure: $\mu : F \to [0, 1]$
  - $\mu(\{w_H\}) = 0.7$, $\mu(\{w_T\}) = 0.3$
  - $\mu(\{w_H, w_T\}) = \mu(\{w_H\}) + \mu(\{w_T\}) = 1$

- Probability measures are not good at representing uncertainty because of the finite additivity property
- Ignorance is difficult to express - an agent has to assign a probability to $\{w_H\}$
- An agent may not have the computational power to compute all the probabilities

Belief Measure

- Given a sample space W, a belief measure is a function $Bel : 2^W \rightarrow [0,1]$ that satisfies the following three properties:
  - $Bel(\emptyset) = 0$
  - $Bel(W) = 1$
  - Inclusion-exclusion rule:
    $Bel(A_1 \cup A_2 \cup ... \cup A_n) \geq \sum_j Bel(A_j) - \sum_{j<k} Bel(A_j \cap A_k) + ... + (-1)^{n+1} Bel(A_1 \cap A_2 \cap ... \cap A_n)$ (Ω_1)

- In (Ω_1), let $A_1 = A$ and $A_2 = \overline{A}$ for $n = 2$. Then $Bel(A \cup \overline{A}) \geq Bel(A) + Bel(\overline{A}) - Bel(A \cap \overline{A})$ which gives $Bel(A) + Bel(\overline{A}) \leq 1$

Belief Measure

- Given a sample space W, a belief measure is a function $Bel : 2^W \to [0,1]$ that satisfies the following three properties:
  - $Bel(\emptyset) = 0$
  - $Bel(W) = 1$
  - Inclusion-exclusion rule: $Bel(A_1 \cup A_2 \cup ... \cup A_n) \geq \sum_j Bel(A_j) - \sum_{j<k} Bel(A_j \cap A_k) + ... + (-1)^{n+1} Bel(A_1 \cap A_2 \cap ... \cap A_n)$ (Ω_1)

- In (Ω_1), let $A_1 = A$ and $A_2 = \overline{A}$ for $n = 2$. Then $Bel(A \cup \overline{A}) \geq Bel(A) + Bel(\overline{A}) - Bel(A \cap \overline{A})$ which gives $Bel(A) + Bel(\overline{A}) \leq 1$

Plausibility Measure

- Given a sample space W, a plausibility measure is a function $Pl : 2^W \to [0,1]$ that satisfies the following three properties:
  - $Pl(\emptyset) = 0$
  - $Pl(W) = 1$
  - Inclusion-exclusion rule: $Pl(A_1 \cap A_2 \cap \ldots \cap A_n) \leq \sum_j Pl(A_j) - \sum_{j<k} Pl(A_j \cup A_k) + \ldots + (-1)^{n+1} Bel(A_1 \cup A_2 \cup \ldots \cup A_n)$ (Ω_2)

- In (Ω_2), let $A_1 = A$ and $A_2 = \overline{A}$ for $n = 2$. Then $Pl(A \cap \overline{A}) \leq Pl(A) + Pl(\overline{A}) - Pl(A \cup \overline{A})$ which gives $Pl(A) + Pl(\overline{A}) \geq 1$

Plausibility Measure

- Given a sample space W, a plausibility measure is a function $Pl : 2^W \to [0,1]$ that satisfies the following three properties:
  - $Pl(\emptyset) = 0$
  - $Pl(W) = 1$
  - Inclusion-exclusion rule: $Pl(A_1 \cap A_2 \cap ... \cap A_n) \leq \sum_j Pl(A_j) - \sum_{j<k} Pl(A_j \cup A_k) + ... + (-1)^{n+1} Bel(A_1 \cup A_2 \cup ... \cup A_n)$ (Ω_2)

- In (Ω_2), let $A_1 = A$ and $A_2 = \overline{A}$ for $n = 2$. Then $Pl(A \cap \overline{A}) \leq Pl(A) + Pl(\overline{A}) - Pl(A \cup \overline{A})$ which gives $Pl(A) + Pl(\overline{A}) \geq 1$

Basic Belief Assignment (Mass Function) (Möbius Representation)

- Given a sample space W, a basic belief assignment is a function $m : 2^W \to [0, 1]$ that satisfies the following two properties:
  - $m(\emptyset) = 0$
  - $\sum_{A \in 2^W} m(A) = 1$

- $m(A) \geq 0$
- If $m(A) > 0$ then A is a focal set
- Let $\mathcal{F}$ be the set of all focal sets induced by m, then $\langle \mathcal{F}, m \rangle$ is a body of evidence
- It is clear that a bba resembles a probability distribution function

Basic Belief Assignment (Mass Function) (Möbius Representation)

- Given a sample space W, a basic belief assignment is a function $m : 2^W \rightarrow [0, 1]$ that satisfies the following two properties:
  - $m(\emptyset) = 0$
  - $\sum_{A \in 2^W} m(A) = 1$

- $m(A) \geq 0$
- If $m(A) > 0$ then A is a focal set
- Let $\mathcal{F}$ be the set of all focal sets induced by m, then $\langle \mathcal{F}, m \rangle$ is a body of evidence
- It is clear that a bba resembles a probability distribution function

Some Formulas

- $Pl(A) = 1 - Bel(\overline{A})$
- $Bel(A) \leq Pl(A)$
- $Bel(A) = \sum_{B|B \subseteq A} m(B)$
- $Pl(A) = \sum_{B|A \cap B \neq \emptyset} m(B)$
- $Q(A) = \sum_{B|A \subseteq B} m(B)$
- $m(A) = \sum_{B|B \subseteq A} (-1)^{|A-B|} Bel(B)$
- $m(A) = \sum_{B|B \subseteq A} (-1)^{|A-B|} [1 - Pl(\overline{B})]$

- $Bel(A)$ is the total belief that the actual world is in the set A which is obtained by adding degrees of evidence for the set itself, as well as for any of its subsets
- $Pl(A)$ is the total belief that the actual world is in the set A, and also the partial evidence for the set that is associated with any set that overlaps with A
- $m(A)$ is the degree of belief that the actual world is in the set A, but it does not take into account any additional evidence for the various subsets of A

- $Q(A)$ is the total belief that can move freely to every point of A
- The interval $[Bel(A), Pl(A)]$ describes the range of possible values of the likelihood of A
- If W is finite, then there is one-to-one correspondence between belief measures and bbas

Total Ignorance

- When no evidence is available about the actual world
- Capture it using a vacuous bba $m_{vac} : 2^W \rightarrow [0, 1]$ where $mvac(W) = 1$ and $mvac(A) = 0$ for all $A \in 2^W \backslash W$
- Capture it using a vacuous belief measure $Bel_{vac} : 2^W \rightarrow [0, 1]$ where $Bel_{vac}(W) = 1$ and $Bel_{vac}(A) = 0$ for all $A \in 2^W \backslash W$
- Capture it using a vacuous plausibility measure $Pl_{vac} : 2^W \rightarrow [0, 1]$ where $Pl_{vac}(\emptyset) = 0$ and $Pl_{vac}(A) = 1$ for all $A \neq \emptyset$

- A bag contains 100 balls; 25 are known to be red, 25 are known to be either red or blue, and 50 are known to be either blue or yellow.
- The sample space $W = \{red, blue, yellow\}$
- The bba $m : 2^W \to [0, 1]$ where $m(\{red\}) = 0.25$, $m(\{red, blue\}) = 0.25$, $m(\{blue, yellow\}) = 0.5$, and $m(\{blue\}) = m(\{yellow\}) = m(\{red, yellow\}) = m(W) = 0$

- The belief measure $Bel : 2^W \rightarrow [0,1]$ where $Bel(\{red\}) = 0.25$, $Bel(\{red, blue\}) = 0.5$, $Bel(\{blue, yellow\}) = 0.5$, $Bel(\{blue\}) = Bel(\{yellow\}) = 0$, $Bel(\{red, yellow\}) = 0.25$, and $Bel(W) = 1$
- The plausibility measure $Pl : 2^W \rightarrow [0,1]$ where $Pl(\{red\}) = 0.5$, $Pl(\{blue\}) = 0.75$, $Pl(\{yellow\}) = 0.5$, $Pl(\{red, blue\}) = 1$, $Pl(\{blue, yellow\}) = 0.75$, $Pl(\{red, yellow\}) = 1$, and $Pl(W) = 1$

Rule of Combination

- Used to combine evidence obtained from two independent sources
- Assume that the degrees of evidence 1 and 2 are captured using the bbas m_1 and m_2 respectively
- $m_{1,2}(A) = \frac{\sum_{B \cap C = A} m_1(B) m_2(C)}{1-c}$ where $A \neq \emptyset$, $m_{1,2}(\emptyset) = 0$, and $c = \sum_{B \cap C = \emptyset} m_1(B) m_2(C)$
- c is the degree of conflict between the two evidence
- The rule is commutative $m_{1,2} = m_{2,1}$
- The rule is associative $m_{1,(2,3)} = m_{(1,2),3}$
- The neutral element is m_{vac}, that is $m_{1,vac} = m_{vac,1} = m_1$

- A computing system has a number of possible states represented by the space W
- Over a time period t, the actual state of the system is in the set $A \in 2^W$
- Over the same time period t, an attacker is trying to discover this actual state

- Initially, the attacker has no evidence about the actual state
- $m_{vac} : 2^W \rightarrow [0, 1]$ where $m(W) = 1$ and $m(A) = 0$ for all $A \in 2^W \backslash W$
- The attacker obtains evidence from source src_1 that the actual state is in the set $A \in 2^W$
- $m_1 : 2^W \rightarrow [0, 1]$ where $m(A) = \alpha_1 > 0$ and $m(W) = 1 - \alpha_1$
- ...
- The attacker obtains the last evidence from source src_n that the actual state is in the set $A \in 2^W$
- $m_n : 2^W \rightarrow [0, 1]$ where $m(A) = \alpha_n > 0$ and $m(W) = 1 - \alpha_n$

- Assuming that the sources $src_1, \ldots, src_n$ are independent
- The attacker will combine to get $m_{1,\ldots,n}(W) = (1-\alpha_1) \times \ldots \times (1-\alpha_n)$ and $m_{1,\ldots,n}(A) = 1-(1-\alpha_1) \times \ldots \times (1-\alpha_n)$
- The Law of Large Numbers says that $m_{1,\ldots,n}(A)$ will eventually reach 1
- When this happens, the attacker will have full belief that the actual state is in the set $A \in 2^W$, which means that the system is compromised.
- Poisoning the values of $\alpha_1, \ldots, \alpha_n$ by minimizing them would delay the satisfaction of the Law of Large Numbers, possibly until a next time period t' by the start of which the system becomes in a different actual state

Conditioning Belief Measures to Update Knowledge

- An agent has an evidence that the actual world is in the set $A \in 2^W$
- Later she obtains another evidence that the actual world is in the set $B \in 2^W$
- How can she update her knowledge?
- $Bel(B||A) = \frac{Bel(B \cup \overline{A}) - Bel(\overline{A})}{1 - Bel(\overline{A})}$
- $Pl(B||A) = \frac{Pl(B \cap A)}{Pl(A)}$

Meaningful Measure of Uncertainty with Beliefs

A measure $\mathcal{M}$ of the uncertainty of Bel is meaningful if it satisfies the following properties:

1. Probability Consistency: If all focal sets are singletons, $\mathcal{M}$ should assume Shannon's entropy: $\mathcal{M}(Bel) = -\sum_{x \in \mathcal{W}} Bel(\{x\}) log_2 Bel(\{x\})$
2. Set Consistency: If Bel focuses on a single set $A \subseteq W$, $\mathcal{M}$ should assume Hartley's entropy: $\mathcal{M}(Bel) = log_2 |A|$
3. Expansibility: The range of $\mathcal{M}$ is $[0, log_2|W|]$ and $\mathcal{M}$ is measured in bits
4. Subadditivity: Let Bel_1, Bel_2, and Bel be bbas on W_1, W_2, and $W_1 \times W_2$, then $\mathcal{M}(Bel) \leq \mathcal{M}(Bel_1) + \mathcal{M}(Bel_2)$
5. Additivity: Let Bel_1, Bel_2, and Bel be bbas on W_1, W_2, and $W_1 \times W_2$, and assume that Bel_1 and Bel_2 are noninteractive, then $\mathcal{M}(Bel) = \mathcal{M}(Bel_1) + \mathcal{M}(Bel_2)$

Generalized Hartley's Measure (U-uncertainty)

- Given a sample space W and a body of evidence $\langle \mathcal{F}, m \rangle$ on this space, the generalized Hartley's measure is given by the formula: $GH(m) = \sum_{A \in \mathcal{F}} m(A) log_2 |A|$
- It has the Expansibility Property $GH(m) \in [0, log_2 |W|]$ and is measured in bits
  - lower bound when all focal sets are singletons
  - upper bound in total ignorance
- It has the Subadditivity Property: $GH(m) \leq GH(m_1) + GH(m_2)$
- It has the Additivity Property: $GH(m) = GH(m_1) + GH(m_2)$

Generalized Shannon's Measure with Beliefs

- A number of unsuccessful attempts to generalize Shannon's measure with beliefs.
  1. Measure of Dissonance: $E(m) = -\sum_{A \in \mathcal{F}} m(A) log_2 Pl(A)$
  2. Measure of Confusion: $C(m) = -\sum_{A \in \mathcal{F}} m(A) log_2 Bel(A)$
  3. Measure of Discord:
     $$D(m) = -\sum_{A \in \mathcal{F}} m(A) log_2 \left(1 - \sum_{B \in \mathcal{F}} m(B) \frac{|B-A|}{|B|}\right)$$
  4. Measure of Strife:
     $$ST(m) = -\sum_{A \in \mathcal{F}} m(A) log_2 \left(1 - \sum_{B \in \mathcal{F}} m(B) \frac{|A-B|}{|A|}\right)$$
- All of these measures do not have the Subadditivity Property, and are thus meaningless.
- This frustrated search was replaced with Aggregate Uncertainty

Aggregate Uncertainty

- $AU(Bel) = \max_{\mathcal{P}_{Bel}} \left\{ -\sum_{x \in W} p_x log_2 p_x \right\}$
- $\mathcal{P}_{Bel}$ is a set of probability distributions that satisfies:
  - $p_x \in [0, 1]$ for all $x \in W$ and $\sum_{x \in W} p_x = 1$
  - $Bel(A) \leq \sum_{x \in A} p_x$ for all $A \subseteq W$
- AU is a meaningful measure of uncertainty with beliefs

Efficient Algorithm

1. Find a nonempty set $A \subseteq W$ such that $\frac{Bel(A)}{|A|}$ is maximal
2. For $x \in A$, let $p_x = \frac{Bel(A)}{|A|}$
3. For each $B \subseteq W - A$, let $Bel(B) = Bel(B \cup A) - Bel(A)$
4. Let $W = W - A$
5. If $W \neq \emptyset$ and $Bel(W) > 0$, go to 1
6. If $W \neq \emptyset$ and $Bel(W) = 0$, let $p_x = 0$ for all $x \in W$
7. Compute $AU(Bel) = -\sum_{x \in W} p_x log_2 p_x$

- A sample space $W = \{x_1, x_2, x_3\}$ of three confidential bank balances
- An attacker would like to learn the highest bank balance by monitoring the execution of the following program:

```
int i = 1;
bool f = true;
while (i <= 3) {
  if (x[i] > g) {
    f = false
  }
  i++;
}
cout << f << endl;
```

- $g \in \{x_1, x_2, x_3\}$ is the attacker's guess and f is a flag that tells whether this guess is correct or not

- $m : 2^W \rightarrow [0,1]$ where $m(\{x_1, x_2\}) = 0.8$ and $m(\{x_2, x_3\}) = 0.2$

A	$Bel(A)$	$\frac{Bel(A)}{\|A\|}$
$\{x_1, x_2\}$	0.8	0.4
$\{x_2, x_3\}$	0.2	0.1

- $p_{x_1} = p_{x_2} = 0.4$
- $W - A = \{x_1, x_2, x_3\} - \{x_1, x_2\} = \{x_3\}$
- $Bel(\{x_3\}) = Bel(\{x_1, x_2, x_3\}) - Bel(\{x_1, x_2\}) = 1 - 0.4 = 0.6$
- $W = W - A = \{x_1, x_2, x_3\} - \{x_1, x_2\} = \{x_3\}$

- Since $W \neq \emptyset$ and $Bel(W) > 0$, we repeat the process

A	$Bel(A)$	$\frac{Bel(A)}{\lvert A \rvert}$
$\{x_3\}$	0.6	0.6

- $p_{x_3} = 0.6$
- $W - A = \{x_3\} - \{x_3\} = \{\}$ we stop here!
- $AU(Bel) = -0.4 log 0.4 - 0.4 log 0.4 - 0.6 log 0.6 = 0.528 + 0.528 + 0.442 = 1.498$ bits

- The attacker has a higher degree of belief that the highest bank balance is in the set $\{x_1, x_2\}$ $\rightsquigarrow$ she feeds the program with x_1
- Suppose she gets a *true* flag
- The attacker will update her beliefs and get: $Bel(\{x_1, x_2\}||\{x_1\}) = 1.0$ and $Bel(\{x_2, x_3\}||\{x_1\}) = 0.0$
- $AU(Bel)$ would be 1.5 bits $\rightsquigarrow$ 0.002 increase in uncertainty

- The attacker has a higher degree of belief that the highest bank balance is in the set $\{x_1, x_2\}$ $\rightsquigarrow$ she feeds the program with x_1
- Suppose she gets a *flase* flag
- The attacker will update her beliefs and get: $Bel(\{x_1, x_2\} || \{x_2, x_3\}) = 0.8$ and $Bel(\{x_2, x_3\} || \{x_2, x_3\}) = 1.0$
- Again (!!!) $AU(Bel)$ would be 1.5 bits $\rightsquigarrow$ 0.002 increase in uncertainty

Thank You!