(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2005 (29.12.2005)

PCT

(10) International Publication Number
WO 2005/124580 A1

(51) International Patent Classification[7]: G06F 17/00, G06N 5/00

(21) International Application Number: PCT/AU2005/000857

(22) International Filing Date: 15 June 2005 (15.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2004903251 15 June 2004 (15.06.2004) AU

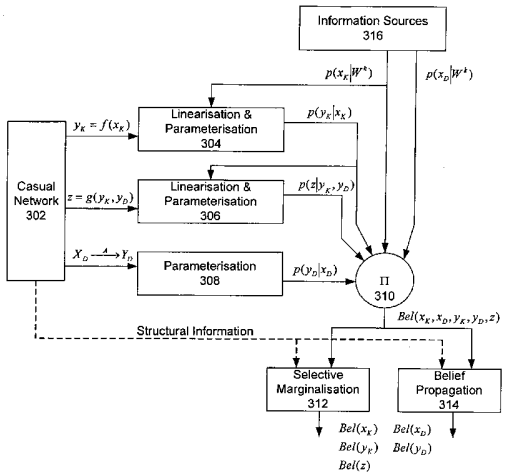
(71) Applicants *(for all designated States except US)*: **THE UNIVERSITY OF MELBOURNE** [AU/AU]; Grattan Street, Parkville, Victoria 3052 (AU). **THE UNIVERSITY OF ADELAIDE** [AU/AU]; North Terrace, Adelaide, South Australia 5000 (AU). **THE UNIVERSITY OF SOUTH AUSTRALIA** [AU/AU]; North Terrace, Adelaide, South Australia 5000 (AU). **THE FLINDERS UNIVERSITY OF SOUTH AUSTRALIA** [AU/AU]; Sturt Road, Bedford Park, Adelaide, South Australia 5042 (AU). **THE UNIVERSITY OF QUEENSLAND** [AU/AU]; Cumbrae Stewart Building, Research Road, St Lucia, Brisbane, Queensland 4067 (AU). **COMMONWEALTH OF AUSTRALIA REPRESENTED BY THE DEFENCE DEPARTMENT'S DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION** [AU/AU]; Building R1, Russell Offices, Canberra, Australian Capital Territory 2601 (AU). **TELSTRA CORPORATION LIMITED** [AU/AU]; A.C.N. 051 775 556, Level 41, 242 Exhibition Street, Melbourne, Victoria 3000 (AU). **COMPAQ COMPUTER AUSTRALIA PTY. LIMITED** [AU/AU]; 410 Concord Road, Rhodes, New South Wales 2138 (AU). **RLM SYSTEMS PTY LIMITED** [AU/AU]; A.C.N. 050 753 403, 4 Wesley Court, 23 Lakeside Drive, Burwood East, Victoria 3151 (AU). **CEA TECHNOLOGIES PTY LIMITED** [AU/AU]; A.C.N. 059 951 183, 59-65 Gladstone Street, Fyshwick, Australian Capital Territory 2609 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **OKELLO, Nickens** [AU/AU]; 2/3 Hillcrest Avenue, Chadstone, Victoria 3148 (AU). **THOMS, Gavin, Alfred** [AU/AU]; 13 Rivoli Place, Taylors Lakes, Victoria 3038 (AU). **MUSICKI, Darko** [AU/AU]; 20/29 King Street, Enfield, New South Wales 2136 (AU). **CHALLA, Subhash** [AU/AU]; Unit 6, 54 The Avenue, Coburg, Victoria 3058 (AU). **PHAM, Tuyet**

[Continued on next page]

(54) Title: A THREAT ASSESSMENT SYSTEM AND PROCESS



(57) Abstract: A threat assessment system, including one or more linearisation modules for generating by linear approximation a conditional probability distribution of a first continuous variable on the basis of a non-linear causal relationship between the first continuous variable and a continuous state variable representing a state of a threatening entity, and for generating by linear approximation a conditional probability distribution of a second continuous variable representing a threat posed by the threatening entity to an asset on the basis of a non-linear causal relationship between the second continuous variable, the first continuous variable, and a discrete state variable representing a state of the threatening entity. The system includes a multiplier module for generating, on the basis of the conditional probability distributions, a joint belief function for assessing the threat, and a belief function generator for generating a belief function for the second continuous variable on the basis of the joint belief function.

WO 2005/124580 A1

[AU/AU]; 7 Pridham Street, Maidstone, Victoria 3012 (AU). **MAREELS, Iven** [AU/AU]; 13 Heathdale Road, Narre Warren, Victoria 3804 (AU). **EVANS, Robin, John** [AU/AU]; 5 Bayview Lane, Aspendale, Victoria 3195 (AU). **WANG, Xuezhi** [AU/AU]; 21 Reynolds Parade, Pascoe Vale South, Victoria 3046 (AU).

(74) Agents: BROWN, Richard, Alan et al.; Davies Collison Cave, 1 Nicholson Street, Melbourne, Victoria 3000 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A THREAT ASSESSMENT SYSTEM AND PROCESS

FIELD OF THE INVENTION

The present invention relates to a threat assessment system and process.

BACKGROUND

As described in Pearl, Judea, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann, San Mateo, CA, 1988 ("Pearl"), Bayesian networks can be used to predict or infer outcomes in the physical world represented by one or more variables whose values are unknown (referred to herein as 'unknown variables') based on observations of other variables having some causal relationship with the unknown variables. In this context, inference is a process of generating probabilities for the unknown variables based upon predetermined causal relationships between those variables and other variables whose values are known or at least estimated with some uncertainty.

Prior art processes for inferring outcomes have used Bayesian belief functions with causal networks, junction tree algorithms, and Pearl's belief propagation, as described in Pearl. However, the resulting inferred outcomes are analytically cumbersome and typically require considerable human interpretation to be used in practical context. For example, in a military context, Bayesian networks have been used to predict the location and type of intruder aircraft detected by multiple sensors and other sources of information. However, the resulting information nevertheless requires substantial interpretation and evaluation by a suitably experienced human to determine, for example, whether any action is required in response to a perceived threat of the intruder aircraft to one or more assets such as ground targets.

Furthermore, although Bayesian belief networks can support backward propagation of evidence, (*e.g.*, where an outcome is known and it is desired to update the causal relationships in the network), the computational requirements of prior art methods increase

exponentially with the complexity of the Bayesian network, making backward propagation infeasible in situations of practical complexity. Consequently, the Bayesian networks that have been developed are undesirably limited in the number of variables that can be included.

It is desired, therefore, to provide a threat assessment system and process and a causal network that alleviate one or more of the above difficulties, or at least provide a useful alternative.

SUMMARY OF THE INVENTION

In accordance with the present invention, there is provided a threat assessment system, including:

one or more linearisation modules for generating by linear approximation a conditional probability distribution of a first continuous variable on the basis of a non-linear causal relationship between said first continuous variable and a continuous state variable representing a state of a threatening entity, and for generating by linear approximation a conditional probability distribution of a second continuous variable representing a threat posed by said threatening entity to an asset on the basis of a non-linear causal relationship between said second continuous variable, said first continuous variable, and a discrete state variable representing a state of said threatening entity;

a multiplier module for generating, on the basis of said conditional probability distributions, a joint belief function for assessing said threat; and

a belief function generator for generating a belief function for said second continuous variable on the basis of said joint belief function.

The present invention also provides a threat assessment system, including:

a causal network module representing causal relationships between variables for assessing a threat posed by a threatening entity to an asset, said causal relationships including one or more non-linear relationships;

one or more parameterisation modules for generating conditional probability distributions for said variables, including generating by linear approximation one or more conditional probability distributions representing said one or more non-linear relationships; and

a multiplier module for generating a joint belief function for assessing said threat on the basis of the conditional probability distributions for said variables.

The present invention also provides a threat assessment system for assessing at least one threat posed at least one threatening entity to at least one asset, the system including a capability generator for generating one or more capability values representing respective capabilities of one or more threatening entities to threaten one or more assets;

an intent generator for generating one or more intent values representing intent of said one or more threatening entities to threaten said one or more assets; and

a threat assessment module for generating one or more threat values representing respective threats posed by said one or more threatening entities to said one or more assets on the basis of said capability values and said intent values.

The present invention also provides a threat assessment system for assessing at least one threat posed at least one threatening entity to at least one asset, the system being adapted to generate conditional probability distributions representing relationships between nodes of a causal network representing said at least one threat, said nodes including at least one entity state node representing a state of a corresponding threatening entity, criteria nodes representing variables dependent on said state and being child nodes of said at least one entity node, and at least one threat node being a child node of said criteria nodes, said at least one threat node representing a threat posed by said at least one threatening entity to a corresponding asset.

The present invention also provides a threat assessment system for assessing at least one threat posed at least one threatening entity to at least one asset, the system being adapted to generate conditional probability distributions representing relationships between nodes of a causal network, said causal network including:

at least one entity node representing a state of a corresponding threatening entity;

a capability node for each entity-asset pair representing the capability of a corresponding threatening entity to threaten a corresponding asset, the capability node being a child node of the entity node of the corresponding threatening entity;

an intent node for each entity-asset pair representing the intent of the corresponding threatening entity to attack the corresponding asset, the intent node being a child node of the entity node of the corresponding threatening entity; and

at least one threat node representing a threat posed by a corresponding threatening entity to a corresponding asset, said at least one threat node being a child node of the corresponding capability node and the corresponding intent node.

The present invention also provides a threat assessment system, including:

a causal network module representing causal relationships between variables for assessing a threat posed by a threatening entity to an asset;

one or more parameterisation modules for generating conditional probability distributions representing linear relationships of said causal relationships

one or more linearisation modules for generating by linear approximation conditional probability distributions representing non-linear relationships of said causal relationships; and

a multiplier for generating a joint belief function for assessing said threat by multiplying the conditional probability distributions representing said relationships.

The present invention also provides a threat assessment process, including:

generating by linear approximation a conditional probability distribution of a first continuous variable on the basis of a non-linear causal relationship between said first continuous variable and a continuous state variable representing a state of a threatening entity;

generating by linear approximation a conditional probability distribution of a second continuous variable representing a threat posed by said threatening entity to an asset on the basis of a non-linear causal relationship between said second continuous variable, said first continuous variable, and a discrete state variable representing a state of said threatening entity;

generating, on the basis of said conditional probability distributions, a joint belief function for assessing said threat; and

generating a belief function for said second continuous variable on the basis of said joint belief function to assess said threat.

The present invention also provides a threat assessment process, including:

generating one or more capability values representing respective capabilities of one or more threatening entities to threaten one or more assets;

generating one or more intent values representing intent of said one or more threatening entities to threaten said one or more assets; and

generating one or more threat values representing respective threats posed by said one or more threatening entities to said one or more assets on the basis of said capability values and said intent values.

The present invention also provides a threat assessment process, including:

determining causal relationships between variables for assessing a threat posed by a threatening entity to an asset, said causal relationships including one or more non-linear relationships;

generating conditional probability distributions for said variables, including generating by linear approximation one or more conditional probability distributions representing said one or more non-linear relationships; and

generating a joint belief function for assessing said threat on the basis of the conditional probability distributions for said variables.

The present invention also provides a threat assessment process, including:

receiving tracking and identification data including conditional probability distributions of kinematic data and type data of a threatening entity, said kinematic data representing a location and velocity of the threatening entity, and said type data representing a type of said threatening entity selected from a plurality of entity types;

generating, on the basis of the conditional probability distributions of kinematic data and a location of an asset, conditional probability distributions of entity-asset data representing separation of the threatening entity and the asset and an angle between the velocity vector of the threatening entity and a vector joining the threatening entity and the asset;

generating, on the basis of the conditional probability distributions of entity-asset data, a conditional probability distribution of threat data with respect to the entity-asset data and the type data of the threatening entity;

multiplying the conditional probability distributions of entity-asset data, the conditional probability distribution of threat data, the conditional probability distributions of kinetic data, and the conditional probability distribution of type data to generate a joint belief function of said threat data, said entity-asset data, said kinetic data, and said type data; and

generating, from said joint belief function, respective belief functions for one or more of said threat data, said entity-asset data, said kinetic data, and said type data.

BRIEF DESCRIPTION OF THE DRAWINGS

Preferred embodiments of the present invention are hereinafter described, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a criteria based causal network for assessing threat in accordance with a preferred embodiment of the present invention;

Figure 2 is a Bayesian belief network for assessing threat in accordance with a preferred embodiment of the present invention, illustrating the contributions of continuous and discrete nodes to threat;

Figure 3 is a block diagram of a preferred embodiment of a threat assessment system;

Figure 4 is a flow diagram of a threat assessment process of the system;

Figure 5 is a flow diagram of a threat estimation process of the threat assessment process;

Figure 6 is a schematic diagram of a threat scenario wherein a threatening entity or intruder U_i approaches an asset A_j;

Figure 7 is a causal model used by the threat assessment system to represent the relationships between data from sensors, capabilities of one or more intruders with respect to one or more assets, intents of those intruders with respect to those assets, and the resulting threats to each asset;

Figure 8 is an image of a surveillance region containing assets, illustrating the actual paths taken by two intruder aircraft, referred to as targets 1 and 2;

Figure 9 is an image of the surveillance region of Figure 8, illustrating the paths taken by the two intruder aircraft as generated by a tracking and data fusion system and provided as input to the threat assessment system;

Figures 10 and 11 are graphs of the height and velocity estimates, respectively, for the two intruder aircraft as a function of time step, as generated by the tracking and data fusion system and provided as input to the threat assessment system;

Figure 12 includes graphs of the variances of the location and velocity components as a function of time step for target 1, as generated by the tracking and data fusion system and provided as input to the threat assessment system;

Figure 13 includes graphs of the variances of the location and velocity components as a function of time step for target 2, as generated by the tracking and data fusion system and provided as input to the threat assessment system;

Figures 14 and 5 include graphs of the aircraft type estimates for target 1 and target 2 of Figure 9, respectively, as generated by the tracking and data fusion system and provided as input to the threat assessment system;

Figure 16 includes graphs of the means of the two intermediate variable components as a function of time step, as generated by the threat assessment system; and

Figure 17 includes graphs of the means and variances of the threats posed by both intruder aircraft to each of the two assets as a function of time step, as generated by the threat assessment system.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The threat posed by an entity to one or more assets can be estimated using a causal network, as shown in Figure 1. The state of the entity, represented by node X, is determined from independent sources of information or measurement nodes $S_1, S_2, \ldots, S_m$ that are parents to node X. At the output end of the network, threat variables $z_1, z_2, \ldots, z_n$ represent the level of threat to assets $A_1, A_2, \ldots, A_n$ respectively. The threat variables are determined using criteria variables $c_1, c_2, \ldots, c_r$ applied to the entity state X. The causal relationships between the entity state, criteria, and threat variables are in general non-linear.

In general, the entity state X includes continuous and discrete components that can be represented by one or more continuous variables X_K and one or more discrete variables X_D, as shown for a single entity and asset pair in Figure 2. A continuous variable is a variable whose value is real (*i.e.*, $X_K \in \Re$) and continuous, whereas a discrete variable is a variable whose

value is restricted to one of a limited number of possible values. The continuous variables typically include one or more variables representing respective rates of change of one or more other continuous state variables. Corresponding continuous and discrete criteria nodes Y_K and Y_D are generated from X_K and X_D, respectively, and are also referred to as intermediate nodes. The threat Z posed by the entity to the asset is determined from the intermediate nodes Y_K and Y_D.

As shown in Figure 3, a threat assessment system based on the networks of Figures 1 and 2 includes threat assessment modules 302 to 314, including a causal network module 302, two linearisation modules 304, 306, a discrete parameterisation module 308, a multiplier 310, a selective marginalisation module 312, and a belief propagation module 314. A threat assessment process, as shown in Figure 4, allows the threat assessment system to generate probability distributions for one or more variables representing respective threats posed by one or more threatening entities to one or more assets from probability distributions for variables representing the state of the threatening entities received from information sources 316.

In the described embodiment, the threat assessment system is a standard computer system such as an Intel IA-32 or IA-64 based computer system executing a Windows operating system, and the processes executed by the system are implemented by software modules, being the threat assessment modules 302 to 314, stored on non-volatile (*e.g.*, magnetic disk) storage associated with the computer system and executed by one or more processors of the system. Although not shown in Figure 3, the system also includes the Matlab software application, available from http://www.mathworks.com/products/matlab/, and Murphy's Bayes Net Toolbox for Matlab (BNT), as described at http://www.ai.mit.edu/~murphyk/Software/BNT/bnt.html, and the threat assessment modules 302 to 314 are based on matrix functions provided by Matlab and BNT. However, it will be apparent that the processes can alternatively be implemented entirely by dedicated software modules written in a programming language such as Fortran and omitting the BNT and Matlab components. Moreover, it will be apparent to those skilled in the art that the

components of the threat assessment system can be distributed over a variety of locations, and that at least parts of the processes executed by the system can alternatively be implemented by dedicated hardware components, such as application-specific integrated circuits (ASICs).

The threat assessment process and system are described below with reference to application of the system and process to air defence, wherein the threat posed to one or more physical assets by one or more intruding aircraft is assessed. However, it should be understood that the threat assessment process and system are not limited to an air defence scenario, but can be applied equally to threat assessment for land and sea scenarios with minimal adaptation. Moreover, the threat assessment process and system can also be used in non-defence related fields. For example, in economics, a network with the structure represented in Figures 1 and 2 can be used to monitor the health of an economy by estimating values for economic variables such as interest rates, building activities, employment rates, currency exchange rates, cost and availability of energy and other resources, climatic factors, etc. In a manufacturing or chemical processing plant, the threat assessment process can be used to monitor specific variables that can affect the health or output capacity of the plant through the use of sensors that are deployed within the plant. In environmental monitoring, the threat assessment process can be applied to assess and control threats to the health of a vital environmental region by identifying and tracking health indicators through the use of environmental data from a wide range of sensors and/or other sources of information. Accordingly, the threat assessment system and process are described below, both in general terms, and also with reference to application.

In order to use the threat assessment process to assess the threat posed by a threatening entity, the first step is to identify the variables relevant, at step 402 of the threat assessment process, as shown in Figure 4. In an air defence scenario, a geographical area contains a distribution of assets that are to be defended against intruder aircraft of different types equipped to launch various types of weapons. An air defence commander has at his or her disposal a number of interceptors of varying capabilities that can be launched to intercept the intruding aircraft on

the basis of knowledge of the asset locations and an assessment of the level of threat posed by the intruding aircraft. The information sources 316 includes a tracking and data fusion system that continually generates track and identification data providing a comprehensive description of each aircraft in the surveillance region, based on input from a network of sensors $S_1, S_2, \ldots, S_m$ and possibly other sources of information, as described in N. N. Okello and D. W. McMichael, "Capabilities and limitations of data fusion in AEW&C," Tech. Rep. 26/98, CSSIP (The Cooperative Research Centre for Sensor Signal and Information Processing), September 1998 ("Okello1998"), and N. Okello, P. Scoullar, and S. Challa, "Association and Identity Inference for the Air Picture Compilation Problem," Tech. Rep. CR 16/00, CSSIP, July 2000 ("Okello2000"). The sensors themselves may be included in the assets being protected.

The track and identification data generated by the tracking and data fusion system includes observable kinematic and discrete state estimates and associated uncertainties. Referring to Figure 2, the kinematic estimates are provided by a continuous matrix variable $\mathbf{x}_K = [\ \xi(k), \dot{\xi}(k), \eta(k), \dot{\eta}(k), \zeta(k), \dot{\zeta}(k)\ ]^T$ that represents the kinematic component of the target (aircraft) state, with $\xi(k)$, $\eta(k)$, and $\zeta(k)$ being the three orthogonal spatial coordinates of the intruder aircraft at time step k, and $\dot{\xi}(k), \dot{\eta}(k), \dot{\zeta}(k)$ being the corresponding velocity components. The discrete variable $\mathbf{x}_D = T_q \in \{T_1, \ldots, T_{N_T}, T_{N_T+1}\}$ represents the discrete component of target state: T_q identifies the type of intruder aircraft from a list of N_T possible aircraft types, with $Tq = T_{N_T+1}$ representing all unknown aircraft types. These seven variables are associated with respective probability distributions.

In general, a surveillance region includes N_U unknown entities, referred to as intruders, and N_A assets, where U_i, $i = 1, \ldots, N_U$ is the i-th intruder, and A_j, $j = 1, \ldots, N_A$ is the j-th asset. Figure 5 is a schematic illustration of a surveillance region with an intruder U_i approaching a number of assets, illustrating the geometrical relationship between a stationary asset A_j with a known location, and the intruder U_i travelling at velocity v_i and equipped with a weapon system whose range envelope is semicircular with radius r_L. In order to evaluate the threat

posed by an intruder U_i on asset A_j, the variables that control the threat level given an intruder-asset pair (U_i, A_j) are determined.

In the described defence application, the threat assessment system uses a general inference network, as shown in Figure 7, and the inference networks in Figures 2 and 3 to infer the threat to assets A_j, $j = 1, ..., N_A$ based on separate evaluations of variables representing an intruder's capability C_{ij} and intent I_{ij} with respect to each asset, determined from track and identification data for the intruder U_i generated by the tracking and data fusion system from sensors and any other available relevant information. Returning to Figure 5, once the relevant variables have been determined, the causal relationships between these variables is determined at step 404.

The level of threat posed to the asset A_j by the intruder U_i depends on the intruder-to-asset range $\mathbf{r}_{ij}$, its rate of change $\dot{r}_{ij} \stackrel{\Delta}{=} d|r_{ij}|/dt$ and the maximum range r_L of the intruder's weapon system. This dependence is non-linear. Intuitively, the threat to an asset posed by a very distant intruder is essentially non-existent or very low, and should increase as the intruder approaches the asset. The threat level should then reach a maximum when the asset falls within the range of the intruder's weapon system, *i.e.*, when the intruder is able to overlay its weapon range envelope over the asset. Accordingly, the intruder's *capability* to threaten the asset is defined as:

$$z_C \propto g_C(r_L, \mathbf{r}_{ij}) = \begin{cases} 1, & \text{if } |\mathbf{r}_{ij}| < r_L \\ \frac{r_L}{|\mathbf{r}_{ij}|}, & \text{if } |\mathbf{r}_{ij}| \geq r_L \end{cases} \quad (1)$$

An intruder with a semi-circular frontal weapon envelope of radius r_L is deemed to pose no threat if it is receding with respect to the stationary asset, *i.e.*, if $\dot{r}_{ij} > 0$. However, when $\dot{r}_{ij} \leq 0$, the threat level is considered to be proportional to $\cos\theta_{ij}$, where θ_{ij} is the angle between the intruder velocity vector and the intruder-to-asset range vector $\mathbf{r}_{ij}$. Accordingly, the intruder's *intent* to threaten the asset A_j is defined as:

$$z_I \propto g_I(\dot{r}_{ij}, \mathbf{v}_j) = \begin{cases} \frac{|\dot{r}_{ij}|}{|\mathbf{v}_j|}, & \text{if } \dot{r}_{ij} \leq 0 \\ 0, & \text{if } \dot{r}_{ij} > 0 \end{cases} \quad (2)$$

The threat I_{ij} to an asset A_j by an intruder U_i is then defined as the product of its *intent* and *capability* components, as follows:

$$\begin{aligned} I_{ij} &= k g_C(r_L, \mathbf{r}_{ij}) g_I(\dot{r}_{ij}, \mathbf{v}_j) \\ &= \begin{cases} \frac{|\dot{r}_{ij}|}{|\mathbf{v}_j|}, & \text{if } |\mathbf{r}_{ij}| < r_L \text{ and } \dot{r}_{ij} \le 0 \\ \frac{r_L}{|\mathbf{r}_{ij}|}\left(\frac{|\dot{r}_{ij}|}{|\mathbf{v}_j|}\right), & \text{if } |\mathbf{r}_{ij}| \ge r_L \text{ and } \dot{r}_{ij} \le 0 \\ 0, & \text{if } \dot{r}_{ij} > 0 \text{ and } 0 < |\mathbf{r}_{ij}| < \infty \end{cases} \end{aligned} \tag{3}$$

or, equivalently,

$$I_{ij} = \begin{cases} \cos\ \theta_{ij}, & \text{if } |\mathbf{r}_{ij}| < r_L \text{ and } |\theta_{ij}| \le \frac{\pi}{2} \\ \frac{r_L}{|\mathbf{r}_{ij}|} \cos\ \theta_{ij}, & \text{if } |\mathbf{r}_{ij}| \ge r_L \text{ and } |\theta_{ij}| \le \frac{\pi}{2} \\ 0, & \text{if } |\theta_{ij}| > \frac{\pi}{2} \text{ and } 0 < |\mathbf{r}_{ij}| < \infty \end{cases} \tag{4}$$

where $-\pi \le \theta_{ij} \le \pi$ is the angle between the i-th intruder velocity vector $\mathbf{v}_i$ and the intruder-to-asset range vector $\mathbf{r}_{ij}$, and $k = 1$ is a constant. Thus the threat level $I_{ij} \in [0, 1]$ is a non-linear discontinuous function of the variables $\mathbf{r}_{ij}$, θ_{ij}, and r_L.

Returning to the inference network of Figure 2, the capability and intent components of threat are represented by an intermediate continuous variable or node

$$\mathbf{y}_K = [\ |\mathbf{r}_{ij}(k)|\ \theta_{ij}(k)\ ]^T \tag{5}$$

that represents the total continuous information that is required for threat assessment. In alternative embodiments, this node may be one of several possible criteria nodes, and in the general case there will be one or more continuous nodes and one or more discrete nodes.

If $\mathbf{x}_A = [\xi_A\ \eta_A\ \zeta_A]^T$ is the location of the j-th asset, then the intruder-to-asset range vector is

$$\mathbf{r}_{ij}(k) = \begin{bmatrix} \xi_A - \xi(k) \\ \eta_A - \eta(k) \\ \zeta_A - \zeta(k) \end{bmatrix}. \tag{6}$$

Furthermore, if $v_j(k) = [\dot{\xi}(k)\ \dot{\eta}(k)\ \dot{\zeta}(k)]^T$ is the velocity vector of the intruder, and θ_{ij} is the angle between the intruder velocity vector $\mathbf{v}_j(k)$ and the intruder-to-asset range vector $\mathbf{r}_{ij}$, then

$$y_K = \begin{bmatrix} |\mathbf{r}_{ij}| \\ \theta_{ij} \end{bmatrix} = \begin{bmatrix} \sqrt{(\xi_A - \xi(k))^2 + (\eta_A - \eta(k))^2 + (\zeta_A - \zeta(k))^2} \\ \cos^{-1}\left(\frac{\mathbf{v}_j^T \mathbf{r}_{ij}}{|\mathbf{v}_j||\mathbf{r}_{ij}|}\right) \end{bmatrix} \tag{7}$$

is the intermediate vector that links the kinematic component of the intruder state vector to the threat variable. The variable y_K is therefore a non-linear function of the kinematic component of the target state vector $\mathbf{x}(k) = [\mathbf{x}_K^T(k)\ \ x_D(k)]^T$ and the asset location x_A, and therefore can be written as:

$$y_K = f(\mathbf{x}_K(k), \mathbf{x}_A) \tag{8}$$

where $x_D(k)$ is the intruder type selected from the set $T = \{T_1, ..., T_{N_T}, T_{N_T+1}\}$.

The variable y_D is discrete and is another of possibly several criteria nodes. Its node Y_D represents the total discrete information that is required for threat assessment. It is related to X_D by the mapping $X_D \xrightarrow{A} Y_D$ where A is an appropriately dimensioned matrix that defines the relationship between components of X_D and those of Y_D. In the described embodiment, this relationship is deterministic in that knowledge of the intruder type gives complete information about the weapon system, including weapon envelope parameters, and A is a unitary matrix with a one in each row or column and maps the type of intruder aircraft to its weapon type. For the sake of simplicity, $A = I$, where I is the identity matrix, so that

$$P(y_D(i)|x_D(j)) = \delta(i-j), \tag{9}$$

where δ is the Dirac δ-function. The variable $z = I_{ij}$ is continuous and represents the threat posed by intruder i to asset j. It is related to the criteria variables through equation (4) above, and is a non-linear function of the discrete component, $x_D(k)$, of the intruder state vector $\mathbf{x}(k)$.

Having determined the variables relevant to threat assessment at step 402, and the relationships between those variables at step 404, the causal network 302 is configured by defining the above functions for y_K, z, and x_D at step 406. For example, in the described application of the system to air defence, $y_K = f(x_K)$ is defined as a vector function that depends on the continuous component of intruder state, of which the function components are the range of the intruder from the asset, and the angle between the intruder velocity vector and the bearing of the asset with respect to the intruder; $A: X_D \rightarrow y_D$ is a matrix that maps target type information to weapons systems; and $z = g(y_K, y_D)$ is a scalar function of the target type (the aircraft type x_D determines the weapon launch range) and the intermediate variable y_K. The intermediate variable y_K is one of two dependent variables of the threat. The second dependent variable, y_D, represents the weapon system type, which is discrete.

At step 408, any non-linear relationships (*i.e.*, the causal network functions defined at step 406) of the casual relationships determined at step 404 are identified. In this particular military application of the system, the relationships defining the continuous variables y_K and z are both non-linear. For example, the intermediate node Y_K is a child of node X_K based on a non-linear relationship. Having identified the non-linear relationships, at step 408 the system is configured to linearise those relationships by applying first-order Taylor series approximations to them, as described below. Having configured the threat assessment system, the system is now ready to generate estimates for threat by executing a threat estimation process 412, as shown in Figure 5.

The threat estimation process 412 begins at step 502 by receiving the probability distributions for the continuous variables x_K and the discrete variables x_D from the information sources 316, being in this military application, a level 1 tracking and data fusion system.

The threat assessment system approximates each continuous node by a Gaussian probability distribution, ensuring that the results will be conservative in the sense that a Gaussian distribution represents the worst possible case and will produce the least accurate results. If

more information subsequently becomes known, such as the actual probability distribution of one or more variables, then the results will be more accurate. Nodes X_K and X_D, representing the state vector of intruder U_i, have no parents and their priors are obtained from the output of the level 1 data fusion system, as described in D.L. Hall and J. Llinas, "An Introduction to Multisensor Data Fusion," Proceedings of the IEEE, vol. 85, No. 1, pp. 6-23, Jan. 1997. The output of the level 1 data fusion system is:

$$\begin{aligned} &\hat{\mathbf{x}}(k|k) = [\hat{\mathbf{x}}_K(k)^T \quad \hat{\mathbf{x}}_D(k) = T_q]^T, \\ &\text{where } T_q = \max_{T_p}\{\mathrm{P}(T_p|W^k), p = 1, ..., N_T, N_T + 1\}, \end{aligned} \tag{10}$$

then the input node priors are:

$$p(\mathbf{x}_K(k)|W^k) = \mathrm{N}\left[\mathbf{x}_K(k); \hat{\mathbf{x}}_K(k|k), P(k|k)\right] \tag{11}$$

and

$$p(\mathbf{x}_D(k)|W^k) = [\mathrm{P}(T_1|W^k) \quad \ldots \quad \mathrm{P}(T_{N_T+1}|W^k)]^T \tag{12}$$

i.e., in this case, the input node prior for X_K is a Gaussian distribution with mean $\hat{x}_K(k|k)$ and covariance matrix $P(k|k)$, where the notation $(k|k)$ indicates that the value of the corresponding variable is for time k and taking into account all known information up to time k, and the notation $N(x; \mu, \sigma)$ represents a Normal or Gaussian distribution of variable x with mean μ and standard deviation σ; and W^k denotes the set of all sensor measurements up to time k. The tracking and data fusion system provides the data, represented by equation (10), (11) and (12) as described in Okello1998 and Okello2000.

At steps 504 and 506, an approximate *conditional probability distribution* (CPD) for nodes Y and Z is determined, based on the linear Gaussian approximation. Specifically, at step 504, a first-order Taylor series approximation of equation (8) about $x_K(k) = \hat{x}_K(k|k)$ is used to generate the following conditional Gaussian distribution from $p(x_K|W^k)$: with the time index k omitted for notational convenience, yields

$$\begin{aligned} \mathbf{y}_K &\approx f(\hat{\mathbf{x}}_K, \mathbf{x}_A) + \frac{1}{1!}\frac{\partial f(\mathbf{x}_K, \mathbf{x}_A)}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}(\mathbf{x}_K - \hat{\mathbf{x}}_K) \\ &= f(\hat{\mathbf{x}}_K, \mathbf{x}_A) - \frac{1}{1!}\frac{\partial f(\mathbf{x}_K, \mathbf{x}_A)}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\hat{\mathbf{x}}_K + \frac{1}{1!}\frac{\partial f(\mathbf{x}_K, \mathbf{x}_A)}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\mathbf{x}_K. \end{aligned} \quad (13)$$

This approximation therefore transforms **y** from a deterministic to a random variable, and so

$$\begin{aligned} E_{Y_K|X_K}\left[\mathbf{y}_K|X_K = \mathbf{x}_K\right] &= E_{\hat{X}_K|X_K}\left[f(\hat{\mathbf{x}}_K, \mathbf{x}_A)|X_K = \mathbf{x}_K\right] + E_{\hat{X}_K|X_K}\left[\frac{\partial f}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\mathbf{x}_K|X_K = \mathbf{x}_K\right] \\ &\quad -E_{\hat{X}_K|X_K}\left[\frac{\partial f}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\hat{\mathbf{x}}_K|X_K = \mathbf{x}_K\right] \\ &= E_{\hat{X}_K}\left[f(\hat{\mathbf{x}}_K, \mathbf{x}_A)\right] + E_{\hat{X}_K}\left[\frac{\partial f}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\right]\mathbf{x}_K - E_{\hat{X}_K}\left[\frac{\partial f}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\hat{\mathbf{x}}_K\right] \end{aligned} \quad (14)$$

where E denotes expectation value, or

$$\begin{aligned} E_{Y_K|X_K}\left[\mathbf{y}|X_K = \mathbf{x}_K\right] &= E_{\hat{X}_K}\left[f(\hat{\mathbf{x}}_K, \mathbf{x}_A)\right] - E_{\hat{X}_K}\left[\frac{\partial f}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\hat{\mathbf{x}}_K\right] + E_{\hat{X}_K}\left[\frac{\partial f}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\right]\mathbf{x}_K \\ &= \mu_{Y_K} + W_Y\mathbf{x}_K \end{aligned} \quad (15)$$

where

$$\mu_{Y_K} = E_{\hat{X}_K}\left[f(\hat{\mathbf{x}}_K, \mathbf{x}_A)\right] - E_{\hat{X}_K}\left[\frac{\partial f}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\hat{\mathbf{x}}_K\right] \quad (16)$$

$$W_{Y_K} = E_{\hat{X}_K}\left[\frac{\partial f}{\partial \mathbf{x}_K}|_{\mathbf{x}_K=\hat{\mathbf{x}}_K}\right]. \quad (17)$$

If $\hat{x}_K$ is approximated by a Gaussian distribution, then the covariance matrix of the variable y_K is given by:

$$\Sigma_{Y_K} = A^T P(k|k)A \quad (18)$$

where

$$A = \frac{\partial \mathbf{y}_K}{\partial \mathbf{x}_K} = \begin{bmatrix} \frac{\partial y_1}{\partial \xi} & \frac{\partial y_1}{\partial \dot{\xi}} & \frac{\partial y_1}{\partial \eta} & \frac{\partial y_1}{\partial \dot{\eta}} & \frac{\partial y_1}{\partial \zeta} & \frac{\partial y_1}{\partial \dot{\zeta}} \\ \frac{\partial y_2}{\partial \xi} & \frac{\partial y_2}{\partial \dot{\xi}} & \frac{\partial y_2}{\partial \eta} & \frac{\partial y_2}{\partial \dot{\eta}} & \frac{\partial y_2}{\partial \zeta} & \frac{\partial y_2}{\partial \dot{\zeta}} \end{bmatrix} \quad (19)$$

The conditional probability density function between the continuous nodes X_K and Y_K can therefore be approximated by a conditional Gaussian distribution and takes on the form

$$p(\mathbf{y}_K|\mathbf{x}_K) = \mathrm{N}\left[\mathbf{y}_K; \mu_{Y_K} + W_{Y_K}\mathbf{x}_K, \Sigma_{Y_K}\right] \tag{20}$$

where the mean μ_{Y_K}, the regression (weight) matrix W_{Y_K}, and the covariance matrix Σ_{Y_K} are defined in equations (16), (17), and (18), respectively.

The output node Z is a child to a discrete node Y_D and a continuous node Y_K and so, at step 506, the following conditional probability density function is generated:

$$p(\mathbf{z}|\mathbf{y}_K, y_D) = \mathrm{N}\left[\mathbf{z}; \mu_Z + W_Z\mathbf{y}_K, \Sigma_Z\right] \tag{21}$$

where

$$\mu_{Z|Y_K,Y_D} = \mu_Z + W_Z\mathbf{y}_K = \begin{bmatrix} \mu_Z(1) \\ \vdots \\ \mu_Z(N_T+1) \end{bmatrix} + \begin{bmatrix} W_Z(1) \\ \vdots \\ W_Z(N_T+1) \end{bmatrix} \mathbf{y}_K \tag{22}$$

$$\Sigma_Z = \mathrm{diag}\left[\Sigma_Z(1) \quad \ldots \quad \Sigma_Z(N_T+1)\right] \tag{23}$$

Thus the components of the N_T+1 dimensional node X_D give rise to respective components of the mean μ_Z and covariance Σ_Z of the one-dimensional node Z.

At step 508, the conditional probability distribution of any discrete intermediate variables is generated. As described above, in this military application, this distribution is represented by a delta function. However, other applications of the system will in general use alternative mappings from input discrete variables to intermediate discrete variables.

In this case, the node variable Z is nonlinear and discontinuous with respect to Y_K, and so Z conditioned on Y_K has three possible modes as defined in equation (4). Consequently, the conditional probability distribution of the variable z is evaluated for each of these three modes.

For the first mode of equation (4), and for $p = 1, 2, \ldots, N_T + 1$,

$$\begin{aligned} z &= \cos\,\theta_{ij} = g_1(\mathbf{y}_K, p) \\ &= g_1(\hat{\mathbf{y}}_K, p) + \frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}(\mathbf{y}_K - \hat{\mathbf{y}}_K) + \ldots \\ &\approx g_1(\hat{\mathbf{y}}_K, p) + \frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}(\mathbf{y}_K - \hat{\mathbf{y}}_K) \\ &= g_1(\hat{\mathbf{y}}_K, p) - \frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}\hat{\mathbf{y}}_K + \frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}\mathbf{y}_K \end{aligned} \tag{24}$$

This approximation transforms z from a deterministic to a random variable, and so

$$\begin{aligned} \mu_{Z|Y_K}(p) &= \mathrm{E}_{\hat{Y}_K}\left[g_1(\hat{\mathbf{y}}_K, p) - \frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}\hat{\mathbf{y}}_K\right] + \mathrm{E}_{\hat{Y}_K}\left[\frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}\right]\mathbf{y}_K \\ &= \mu_Z(p) + W_Z(p)\mathbf{y}_K \end{aligned} \tag{25}$$

where

$$\mu_Z(p) = \mathrm{E}_{\hat{Y}_K}\left[g_1(\hat{\mathbf{y}}_K, p) - \frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}\hat{\mathbf{y}}_K\right] \tag{26}$$

$$W_Z(p) = \mathrm{E}_{\hat{Y}_K}\left[\frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{y}_K}\right] \tag{27}$$

$$\Sigma_Z(p) = AR_{r\theta}A^T, \text{ and } A = \frac{\partial g_1(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}. \tag{28}$$

Similarly, for the second mode of equation (4):

$$z = \frac{r_L}{|\mathbf{r}_{ij}|}\cos\,\theta_{ij} = g_2(\mathbf{y}_K, p) \tag{29}$$

and so

$$\begin{aligned} \mu_{Z|Y_K}(p) &= \mathrm{E}_{\hat{Y}_K}\left[g_2(\hat{\mathbf{y}}_K, p) - \frac{\partial g_2(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}\hat{\mathbf{y}}_K\right] + \mathrm{E}_{\hat{Y}}\left[\frac{\partial g_2(\mathbf{y}, p)}{\partial \mathbf{y}}|_{\mathbf{y}_K=\hat{\mathbf{y}}_K}\right]\mathbf{y}_K \\ &= \mu_Z(p) + W_Z(p)\mathbf{y}_K \end{aligned} \tag{30}$$

where

$$\mu_Z(p) = \mathrm{E}_{\hat{Y}_K}\left[g_2(\hat{\mathbf{y}}_K, p) - \frac{\partial g_2(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{y}}\hat{\mathbf{y}}_K\right] \quad (31)$$

$$W_Z(p) = \mathrm{E}_{\hat{Y}_K}\left[\frac{\partial g_2(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{y}_K}\right] \quad (32)$$

$$\Sigma_Z(p) = AR_{r\theta}A^T, \text{ and } A = \frac{\partial g_2(\mathbf{y}_K, p)}{\partial \mathbf{y}_K}|_{\mathbf{y}_K=\hat{y}_K}. \quad (33)$$

For the third mode of equation (4) however, $z = 0$ and so

$$\mu_Z(p) = 0, \quad (34)$$

$$W_Z(p) = [0 \;\; 0], \quad (35)$$

and

$$\Sigma_Z(p) = \varepsilon^2, \quad (36)$$

for $p = 1, .., N_T + 1$, where ε is a small number.

Given the conditional probability distributions of equations (9), (11), (12), (20), and (21), and the Bayesian belief network in Figure 2, at step 510 a joint belief function for threat assessment is generated by the multiplier 310 as the product of all these conditional probability distributions, as follows:

$$\begin{aligned} \mathrm{Bel}(z, y_K, y_D, x_K, x_D) &= p(z, y_K, y_D, x_K, x_D|W^k) \\ &= p(x_K|W^k)p(x_D|W^k)p(y_K|x_K)p(y_D|x_D)p(z|y_K, y_D) \end{aligned} \quad (37)$$

At step 512, belief functions for individual variables are generated from the joint belief function, as described below. The belief functions are generated by either the selective marginalisation module 312 or the belief propagation module 314, depending upon the variables in the threat assessment network.

Selective marginalisation, as described below, is preferred under all conditions. Selective marginalisation is computationally more direct and more economical than Pearl's belief propagation. Either process can be used if evidence is inserted at nodes other than the root (*i.e.*, initial continuous and discrete) nodes.

The selective marginalisation module 312 generates a closed form expression of the belief function of each node variable by summing out any other discrete variables and integrating out any other continuous variables from the joint belief function of the network given by equation (37). This process of selective marginalisation is referred to herein as the direct integration process.

The direct integration process is performed as follows. From the joint belief function of equation (37), the distribution of any node variable conditioned on the measurement set W^k is obtained by integrating and/or summing out all the other node variables, as follows:

$$\begin{aligned} \mathrm{Bel}(z) = p(z|W^k) &= \sum_{x_D, y_D} \int_{x_K, y_K} p(z, y_K, y_D, x_K, x_D|W^k) dx_K dy_K \\ &= \sum_{x_D, y_D} \int_{x_K, y_K} p(x_K|W^k) p(x_D|W^k) p(y_K|x_K) p(y_D|x_D) p(z|y_K, y_D) dx_K dy_K \end{aligned} \quad (38)$$

Following a process of substitution, completion of squares and maximization, the conditional mean and covariance of z take on the form

$$\mu_{Z|i} = A_3^{-1} B_3 = \Sigma_{Z|i} (\Sigma^{-1}_{Z|Y_K,i} W_Z(i) A_2^{-1} M_2 + \Sigma^{-1}_{Z|Y_K,i} \mu_Z(i)) \quad (39)$$

$$\Sigma_{Z|i} = A_3^{-1} = (\Sigma^{-1}_{Z|Y_K,i} - \Sigma^{-1}_{Z|Y_K,i} W_Z(i) A_2^{-1} W_Z^T(i) \Sigma^{-1}_{Z|Y_K,i})^{-1} \quad (40)$$

The belief function for the intermediate function Y can also be evaluated by integrating out all the other variables within the joint belief function, as follows:

$$\begin{aligned} \mathrm{Bel}(y_K) &= p(y_K|W^k) \\ &= \sum_{x_D, y_D} \int_{x_K, z} p(z, y_K, y_D, x_K, x_D|W^k) dx_K dy_K \\ &= \sum_{y_D} \int_{x_k, z} p(x_K|W^k) p(y_D|W^k) p(y_K|x_K) p(z|y_K, y_D) dx_K dz \\ &= \int_{x_K} p(x_K|W^k) p(y_K|x_K) dx_K \end{aligned} \quad (41)$$

Hence the mean and covariance of Y are

$$\hat{y}_K = A_2^{-1}B_2 = A_2^{-1}\left\{\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K} + \Sigma_{Y_K|X_K}^{-1}W_{Y_K}A_1^{-1}(P^{-1}\hat{x} - W_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K})\right\} \quad (42)$$

$$\Sigma_{Y_K} = A_2^{-1} = (\Sigma_{Y_K|X_K}^{-1} - \Sigma_{Y_K|X_K}^{-1}W_{Y_K}A_1^{-1}W_{Y_K}^T\Sigma_{Y_K|X_K}^{-1})^{-1} \quad (43)$$

As described above, as an alternative to the selective marginalisation or direct integration process of equations (38) to (40), the belief functions can be generated by the belief propagation module 314, which applies belief propagation, as described in Pearl, to the Bayesian belief network of Figure 2, as described below.

Consider the Bayesian belief network of Figure 2. When node Y_D receives no evidence, as in the described embodiments, then X_D and Y_D are equivalent, since $A = I$. In the derivation that follows, the variable X_D is used in place of Y_D. However, it should be understood that in the more general case Y_D should be used. The nodes X_K and X_D are root nodes with no parents, and therefore can be written as forward propagation messages π, as follows:

$$\pi(x_K) \equiv p(x_K|W^k) = N(x_K;\hat{x},P) \quad (44)$$

$$\pi(x_D) \equiv p(x_D|W^k) = [\,\mathrm{P}(T_1|W^k) \quad \mathrm{P}(T_2|W^k) \quad \ldots \quad \mathrm{P}(T_{N+1}|W^k)\,]. \quad (45)$$

The output node Z is a childless continuous node that cannot be instantiated but whose value lies in [0, 1]. Thus the backward propagation message $\lambda(z) \sim \mathrm{U}[0, 1]$ *i.e.*, has a uniform distribution over [0,1], and this appropriately expresses the level of knowledge available on the variable Z. Alternatively, the interval restriction on the variable Z can be relaxed in order to take advantage of the Gaussian distribution by assuming that $\lambda(z) \sim \mathrm{N}(z; \mu_Z, \Sigma_Z)$, where $\mu_Z = 0.5$ and Σ_Z is a large number. From equation (4.45) in Pearl,

$$\mathrm{Bel}(z) = \alpha\lambda(z)\left[\sum_{x_D}\int_{y_K} p(z|y_K,x_D)\pi_Z(y_K)\pi_Z(x_D)dy_K\right] \quad (46)$$

where $\pi_Z(y)$ and $\pi_Z(x_D)$ are messages from parents Y and X_D respectively.

Now consider the message $\pi_Z(x_D)$ that X_D sends to Z. From equation (4.45) in Pearl,

$$\pi_Z(x_D) = \alpha\pi(x_D) = [\,\mathrm{P}(T_1|W^k) \quad \mathrm{P}(T_2|W^k) \quad \ldots \quad \mathrm{P}(T_{N+1}|W^k)\,]. \tag{47}$$

Consider again the message $\pi_Y(x_K)$ that X_K sends to Y. Applying equation (4.45) in Pearl,

$$\begin{aligned} \pi_{Y_K}(x_K) &= \alpha\pi(x_K) = \pi(x_K) = N(x_K;\hat{x},P) \\ &= \frac{1}{\sqrt{2\pi P}}\exp\Big[-\frac{1}{2}(x_K-\hat{x})P^{-1}(x_K-\hat{x})\Big]. \end{aligned} \tag{48}$$

Now consider the message $\pi_Z(y_K)$ that Y sends to Z. Applying equation (4.45) in Pearl followed by the integral version of equation (4.38) in Pearl, the following equation is obtained:

$$\begin{aligned} \pi_Z(y_K) &= \alpha\pi(y_K) = \pi(y_K) = \int_{X_K} p(y_K|x_K)\pi_{Y_K}(x_K)dx_K \qquad (49) \\ &= \int_{x_K} \frac{1}{\sqrt{2\pi\Sigma_{Y_K|X}}}\frac{1}{\sqrt{2\pi\Sigma_X}}\exp\Big[-\frac{1}{2}(y_K-\mu_{Y_K|X_K})^T\Sigma^{-1}_{Y_K|X_K}(y_K-\mu_{Y_K|X_K})\Big] \\ &\qquad \exp\Big[-\frac{1}{2}(x_K-\hat{x})^T\Sigma^{-1}_{X_K}(x_K-\hat{x})\Big]dx_K \\ &= \kappa\exp\Big[-\frac{1}{2}\Big\{-B_1^TA_1^{-1}B_1 + (y_K-\mu_{Y_K})^T\Sigma^{-1}_{Y_K|X_K}(y_K-\mu_{Y_K}) + \hat{x}^T\Sigma_X^{-1}\hat{x}\Big\}\Big] \qquad (50) \end{aligned}$$

where

$$A_1 = \Sigma_X^{-1} + W_{Y_K}^T\Sigma^{-1}_{Y_K|X_K}W_{Y_K} \tag{51}$$

$$B_1 = \Sigma^{-1}_{X_K}\hat{x} + W^T_{Y_K}\Sigma^{-1}_{Y_K|X_K}(y_K-\mu_{Y_K}). \tag{52}$$

The conditional distribution $p(z|y, x_D)$ can be approximated by a linear Gaussian and written in the form:

$$p(z|y_K,i) = \mathrm{N}\big(z;\mu_Z(i) + W_Z(i)y_K, \Sigma_{Z|Y_K,i}\big) \tag{53}$$

Substituting equations (47) and (50) into (46) yields

$$\begin{aligned} \mathrm{Bel}(z) &= \alpha\exp\Big[-\frac{1}{2}(z-\mu_0)^T\Sigma_0^{-1}(z-\mu_0)\Big] \\ &\quad \Big\{\sum_{x_D}\int_{y_K}\exp\Big[-\frac{1}{2}(z-\mu_{Z|Y_K,i})^T\Sigma^{-1}_{Z|Y_K,i}(z-\mu_{Z|Y_K,i})\Big] \\ &\quad \exp\Big[-\frac{1}{2}(-B_1^TA_1^{-1}B_1 + (y_K-\mu_{Y_K})^T\Sigma^{-1}_{Y_K|X_K}(y_K-\mu_{Y_K}) + \hat{x}^T\Sigma^{-1}_{X_K}\hat{x})\Big]\mathrm{P}(T_i|W^k)dy_K\Big\} \end{aligned}$$

or

$$\begin{aligned}
\mathrm{Bel}(z) &= \alpha \exp[-\frac{1}{2}(z-\mu_0)^T\Sigma_0^{-1}(z-\mu_0)] \\
&\quad \Big\{\sum_{x_D} \exp\Big[-\frac{1}{2}\Big(-(M_2+W_Z^T(i)\Sigma^{-1}_{Z|Y_K,i}z)^T A_2^{-1}(M_2+W_Z^T(i)\Sigma^{-1}_{Z|Y_K,i}z)+(z-\mu_Z(i))^T\Sigma^{-1}_{Z|Y_K,i}(z-\mu_Z(i)) \\
&\qquad -(\Sigma_X^{-1}\hat{x}-W_{Y_K}^T\Sigma^{-1}_{Y_K|X_K}\mu_{Y_K})^T A_1^{-1}(\Sigma_{X_K}^{-1}\hat{x}-W_{Y_K}^T\Sigma^{-1}_{Y_K|X_K}\mu_{Y_K}) \\
&\qquad +\mu_{Y_K}^T\Sigma^{-1}_{Y_K|X_K}\mu_{Y_K}+\hat{x}^T\Sigma_{X_K}^{-1}\hat{x}\Big)\Big]P(T_i|W^k)\Big\} \\
&= \alpha\sum_{x_D}\exp\Big[-\frac{1}{2}\Big\{(z-A_3^{-1}B_3)^T A_3(z-A_3^{-1}B_3)-B_3^{-1}A_3^{-1}B_3 \\
&\qquad +\mu_0^T\Sigma_0^{-1}\mu_0-M_2^TA_2^{-1}M_2+\mu_Z^T(i)\Sigma^{-1}_{Z|Y_K,i}\mu_Z(i) \\
&\qquad -(\Sigma_{X_K}^{-1}\hat{x}-W_{Y_K}^T\Sigma^{-1}_{Y_K|X_K}\mu_{Y_K})^T A^{-1}(\Sigma_{X_K}^{-1}\hat{x}-W_{Y_K}^T\Sigma^{-1}_{Y_K|X_K}\mu_{Y_K}) \\
&\qquad +\mu_{Y_K}^T\Sigma^{-1}_{Y_K|X_K}\mu_{Y_K}+\hat{x}^T\Sigma_{X_K}^{-1}\hat{x}\Big\}\Big]\mathrm{P}(T_i|W^k) \qquad (54)
\end{aligned}$$

where

$$A_3 = \Big[\Sigma^{-1}_{Z|Y_K,i}-\Sigma^{-1}_{Z|Y_K,i}W_Z(i)A_2^{-1}W_Z^T(i)\Sigma^{-1}_{Z|Y_K,i}+\Sigma_0^{-1}\Big] \qquad (55)$$

$$B_3 = \Sigma^{-1}_{Z|Y_K,i}\mu_Z(i)+\Sigma^{-1}_{Z|Y_K,i}W_Z(i)A_2^{-1}M_2+\Sigma_0^{-1}\mu_0 \qquad (56)$$

The belief function in equation (54) is a Gaussian mixture whose summand densities have means and variances given by

$$\mu_{Z|i} = \Sigma_{Z|i}\Big\{\Sigma^{-1}_{Z|Y_K,i}\mu_Z(i)+\Sigma^{-1}_{Z|Y_K,i}W_Z(i)A_2^{-1}M_2+\Sigma_0^{-1}\mu_0\Big\} \qquad (57)$$

$$\Sigma_{Z|i} = A_3^{-1} = \Big[\Sigma^{-1}_{Z|Y_K,i}-\Sigma^{-1}_{Z|Y_K,i}W_Z(i)A_2^{-1}W_Z^T(i)\Sigma^{-1}_{Z|Y_K,i}+\Sigma_0^{-1}\Big]^{-1} \qquad (58)$$

and so the mean and covariance of such a mixture is given by

$$\hat{z} = \sum_{i=1}^{N_T+1}\mu_{Z|i}\mathrm{P}(T_i|W^k) \qquad (59)$$

$$\Sigma_Z = \sum_{i=1}^{N_T+1}\mathrm{P}(T_i|W^k)\Big\{\Sigma^{-1}_{Z|i}+(\mu_{Z|i}-\hat{z})(\mu_{Z|i}-\hat{z})^T\Big\} \qquad (60)$$

If Σ_0 is large, then

$$\mu_{Z|i} = \Sigma_{Z|i}\Big\{\Sigma^{-1}_{Z|Y_K,i}\mu_Z(i)+\Sigma^{-1}_{Z|Y_K,i}W_Z(i)A_2^{-1}M_2\Big\} \qquad (61)$$

$$\Sigma_{Z|i} = A_3^{-1} = \Big[\Sigma^{-1}_{Z|Y_K,i}-\Sigma^{-1}_{Z|Y_K,i}W_Z(i)A_2^{-1}W_Z^T(i)\Sigma^{-1}_{Z|Y_K,i}\Big]^{-1} \qquad (62)$$

and so the evidence at node Z does not enter the belief function for node Z.

Thus an estimate of the threat $\boldsymbol{Z}$ to one or more assets is obtained from equations (57) and (58) by substituting values from equations (11) and (12), which themselves rely on equations (20) and (21), which rely on equations (16), (17), and (18), and (22) and (23), respectively.

Repeating the above steps for node Y,

$$\mathrm{Bel}(y_K) = \alpha\lambda_Z(y_K)\Big\{\int_{X_K} p(y_K|x_K)\pi_{Y_K}(x_K)dx_K\Big\} \tag{63}$$

where $\lambda_Z(y)$ is the message that Z sends to Y. Applying equation (4.44) in Pearl,

$$\lambda_Z(y_K) = \beta\int_Z \lambda(z)\sum_{x_D} p(z|x_D, y_K)\pi_Z(x_D)dz \tag{64}$$

where $\pi_Z(x_D)$ is given in equation (47) and $\lambda(z) \sim N(z;\, \mu_Z, \Sigma_Z)$ where $\mu_Z = 0.5$ and Σ_Z is a large number to reflect the lack of knowledge on the uninitialized childless node variable Z.

The integrals in equations (63) and (64) are then integrated, after which equation (64) is substituted into equation (63). Thus:

$$\begin{aligned}
\mathrm{Bel}(y_K) &= \alpha\lambda_Z(y_K)\Big\{\int_{X_K} p(y_K|x_K)\pi_{Y_K}(x_K)dx_K\Big\} \\
&= \alpha\lambda_Z(y_K)\Big\{\int_{x_K} \exp\Big[-\frac{1}{2}(y_K - \mu_{Y_K} - W_{Y_K}x)^T\Sigma^{-1}_{Y_K|X_K}(y_K - \mu_{Y_K} - W_{Y_K}x_K)\Big] \\
&\qquad \exp\Big[-\frac{1}{2}(x_K - \hat{x})^T\Sigma^{-1}_{X_K}(x_K - \hat{x})\Big]dx_K\Big\} \\
&= \alpha\lambda_Z(y_K)\Big\{\exp\Big[-\frac{1}{2}\Big[-B_1^T A_1^{-1}B_1 + \hat{x}^T\Sigma_X^{-1}\hat{x} + (y_K - \mu_{Y_K})^T\Sigma^{-1}_{Y_K|X_K}(y_K - \mu_{Y_K})\Big]
\end{aligned} \tag{65}$$

where

$$A_1 = \Sigma^{-1}_{X_K} + W^T_{Y_K}\Sigma^T_{Y_K|X_K}W_{Y_K} \tag{66}$$

$$B_1 = \Sigma^{-1}_{X_K}\hat{x} + W^T_{Y_K}\Sigma^{-1}_{Y_K|X_K}(y_K - \mu_{Y_K}) \tag{67}$$

Now rearranging the exponent in equation (65) in order to expose the quadratic in y, the following is obtained:

$$\begin{aligned}
\mathrm{Bel}(y_K) &= \alpha\lambda_Z(y_K)\Big\{\int_{x_K}\exp\Big[-\frac{1}{2}\Big[-(\Sigma_X^{-1}\hat{x}+W_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}(y_K-\mu_{Y_K}))^T A_1^{-1}(\Sigma_{X_K}^{-1}\hat{x}+W_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}(y_K-\mu_{Y_K})) \\
&\qquad +\hat{x}^T\Sigma_X^{-1}\hat{x}+(y_K-\mu_{Y_K})^T\Sigma_{Y_K|X_K}^{-1}(y_K-\mu_{Y_K})\Big]\Big\} \\
&= \alpha\lambda_Z(y_K)\exp\Big\{-\frac{1}{2}\Big[y_K^T(\Sigma_{Y_K|X_K}^{-1}-\Sigma_{Y_K|X_K}^{-1}W_{Y_K}A_1^{-1}W_{Y_K}^T\Sigma_{Y_K|X_K}^{-1})y_K \\
&\qquad -2y_K^T(\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K}+\Sigma_{Y_K|X_K}^{-1}W_{Y_K}A_1^{-1}(\Sigma_{X_K}^{-1}\hat{x}-W_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K})) \\
&\qquad -(\Sigma_{X_K}^{-1}\hat{x}-W_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K})^T A_1^{-1}(\Sigma_{X_K}^{-1}\hat{x}-W_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K}) \\
&\qquad +\hat{x}^T\Sigma_{X_K}^{-1}\hat{x}+\mu_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K}\Big]\Big\}.
\end{aligned} \tag{68}$$

But

$$\begin{aligned}
\lambda_Z(y_K) &= \beta\int_Z\lambda(z)\sum_{i=1}^{N_T+1}p(z|y_K,x_D(i))\pi_Z(x_D(i))dz \\
&= \beta\int_Z\exp\Big[-\frac{1}{2}(z-\mu_0)^T\Sigma_0^{-1}(z-\mu_0)\Big] \\
&\qquad \sum_{i=1}^{N_T+1}\exp\Big[-\frac{1}{2}(z-\mu_Z-W_Z(i)y_K)^T\Sigma_{Z|Y_K,i}^{-1}(z-\mu_Z-W_Z(i)y_K)\Big]P(T_i|W^k)dz \\
&= \beta\sum_{i=1}^{N_T+1}\exp\Big[-\frac{1}{2}\Big\{-B_2^TA_2^{-1}B_2+(\mu_Z(i)+W_Z(i)y_K)^T\Sigma_{Z|Y_K,i}^{-1}(\mu_Z(i)+W_Z(i)y_K)+\mu_0^T\Sigma_0^{-1}\mu_0\Big\}\Big]\mathrm{P}(T_i|W^k)
\end{aligned} \tag{69}$$

where

$$A_2 = (\Sigma_{Z|Y_K,i}^{-1}+\Sigma_0^{-1}) \tag{70}$$

$$B_2 = \big(\Sigma_{Z|Y_K,i}^{-1}(\mu_Z(i)+W_Z(i)y_K)+\Sigma_0^{-1}\mu_0\big). \tag{71}$$

Now rearranging the exponent in equation (69) in order to expose the quadratic in y, provides

$$\begin{aligned}
\lambda_Z(y_K) &= \beta\sum_{i=1}^{N_T+1}\exp\Big[-\frac{1}{2}\Big\{-(\Sigma_{Z|Y_K,i}^{-1}(\mu_Z(i)+W_Z(i)y_K)+\Sigma_0^{-1}\mu_0)^TA_2^{-1}(\Sigma_{Z|Y_K,i}^{-1}(\mu_Z(i)+W_Z(i)y_K)+\Sigma_0^{-1}\mu_0) \\
&\qquad +(\mu_Z(i)+W_Z(i)y_K)^T\Sigma_{Z|Y_K,i}^{-1}(\mu_Z(i)+W_Z(i)y_K)+\mu_0^T\Sigma_0^{-1}\mu_0\Big\}\Big]P(T_i|W^k) \\
&= \beta\sum_{i=1}^{N_T+1}\exp\Big[-\frac{1}{2}\Big\{y_K^T\Big(W_Z^T(i)\Sigma_{Z|Y_K,i}^{-1}W_Z(i)-W_Z(i)^T\Sigma_{Z|Y_K,i}^{-1}A_2^{-1}\Sigma_{Z|Y_K,i}W_Z(i)\Big)y_K \\
&\qquad -2y_K^T\Big(W_Z(i)^T\Sigma_{Z|Y_K,i}^{-1}A_2^{-1}(\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i)+\Sigma_0^{-1}\mu_0)-W_Z(i)^T\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i)\Big) \\
&\qquad -(\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i)+\Sigma_0^{-1}\mu_0)^TA_2^{-1}(\Sigma_{Z|Y_K,i}\mu_Z(i)+\Sigma_0^{-1}\mu_0) \\
&\qquad +\mu_Z(i)^T\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i)+\mu_0^T\Sigma_0^{-1}\mu_0\Big\}\Big]\mathrm{P}(T_i|W^k).
\end{aligned} \tag{72}$$

Now substituting (72) into (68), and writing the exponent in the form of a quadratic in y, provides:

$$\begin{aligned}
\mathrm{Bel}(y_K) &= \alpha\beta \sum_{i=1}^{N_T+1} \exp\Big\{ -\frac{1}{2}\Big[y_K^T A_3 y_K - 2y_K^T B_3 - (\Sigma_{X_K}^{-1}\hat{x} - W_{Y_K}^T \Sigma_{Y_K|X_K}^{-1}\mu_{Y_K})^T A_1^{-1}(\Sigma_{X_K}^{-1}\hat{x} - W_{Y_K}^T \Sigma_{Y_K|X_K}^{-1}\mu_{Y_K}) \\
&\qquad + \hat{x}^T\Sigma_{X_K}^{-1}\hat{x} + \mu_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K} - (\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i) + \Sigma_0^{-1}\mu_0)^T A_2^{-1}(\Sigma_{Z|Y_K,i}\mu_Z(i) + \Sigma_0^{-1}\mu_0) \\
&\qquad + \mu_Z(i)^T\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i) + \mu_0^T\Sigma_0^{-1}\mu_0\Big]\Big\} P(T_i|W^k) \\
&= \alpha\beta \sum_{i=1}^{N_T+1} \exp\Big\{ -\frac{1}{2}\Big[(y_K - A_3^{-1}B_3)^T A_3 (y_K - A_3^{-1}B_3) - B_3^T A_3^{-1} B_3 \\
&\qquad - (\Sigma_{X_K}^{-1}\hat{x} - W_{Y_K}^T \Sigma_{Y_K|X_K}^{-1}\mu_{Y_K})^T A_1^{-1}(\Sigma_{X_K}^{-1}\hat{x} - W_{Y_K}^T \Sigma_{Y_K|X_K}^{-1}\mu_{Y_K}) \\
&\qquad + \hat{x}^T\Sigma_{X_K}^{-1}\hat{x} + \mu_{Y_K}^T\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K} - (\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i) + \Sigma_0^{-1}\mu_0)^T A_2^{-1}(\Sigma_{Z|Y_K,i}\mu_Z(i) + \Sigma_0^{-1}\mu_0) \\
&\qquad + \mu_Z(i)^T\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i) + \mu_0^T\Sigma_0^{-1}\mu_0\Big]\Big\} \mathrm{P}(T_i|W^k)
\end{aligned} \tag{73}$$

The belief function in equation (73) is a Gaussian mixture with the means and covariances of the summands given by

$$\mu_{Y_K|i} = A_3^{-1}B_3 \tag{74}$$

$$\Sigma_{Y_K|i} = A_3^{-1} \tag{75}$$

where $i = 1, \ldots, N_T + 1$, and so the mean and covariance of such a mixture is given by:

$$\hat{y}_K = \sum_{i=1}^{N_T+1} \mu_{Y_K|i}\mathrm{P}(T_i|W^k) \tag{76}$$

$$\Sigma_{Y_K} = \sum_{i=1}^{N_T+1} \mathrm{P}(T_i|W^k)\Big\{\Sigma_{Y_K|i}^{-1} + (\mu_{Y_K|i} - \hat{y})(\mu_{Y_K|i} - \hat{y})^T\Big\} \tag{77}$$

where

$$A_3 = \Big(\Sigma_{Y_K|X_K}^{-1} - \Sigma_{Y_K|X_K}^{-1} W_{Y_K} A_1^{-1} W_{Y_K}^T \Sigma_{Y_K|X_K}^{-1} + W_Z^T(i)\Sigma_{Z|Y_K,i}^{-1} W_Z(i) - W_Z(i)^T\Sigma_{Z|Y_K,i}^{-1} A_2^{-1}\Sigma_{Z|Y_K,i} W_Z(i)\Big) \tag{78}$$

$$\begin{aligned}
B_3 = \Big(&\Sigma_{Y_K|X_K}^{-1}\mu_{Y_K} + \Sigma_{Y_K|X_K}^{-1} W_{Y_K} A_1^{-1}(\Sigma_{X_K}^{-1}\hat{x} - W_{Y_K}^T \Sigma_{Y_K|X_K}^{-1}\mu_{Y_K}) \\
&+ W_Z(i)^T\Sigma_{Z|Y_K,i}^{-1} A_2^{-1}(\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i) + \Sigma_0^{-1}\mu_0) - W_Z(i)^T\Sigma_{Z|Y_K,i}^{-1}\mu_Z(i)\Big).
\end{aligned} \tag{79}$$

Backward Propagation

Any node within a Bayesian network can be instantiated with evidence. Consider the case where it becomes known that the variable Y_K has a value y_K. This piece of information can be injected as evidence $e^-_{Y_K V_1}$ by inserting an auxiliary child node V_1 that directs this evidence backwards towards node Y_K. Similarly, child nodes V_2 and V_3 can be inserted to direct evidence $e^-_{ZV_2}$ and $e^-_{Y_D V_3}$ towards nodes Z and Y_D, respectively.

For example, using selective marginalisation and taking structural information into account,

$$
\begin{aligned}
\mathrm{Bel}(y_K) &= \sum_{y_D,x_D,v_3} \int_{x_K,v_1,v_2,z} \mathrm{Bel}(x_K,x_D,y_K,y_D,z,v_1,v_2,v_3)\,dx_K\,dz\,dv_1\,dv_2 \\
&= \sum_{y_D,x_D,v_3} \int_{x_K,z,v_1,v_2,v_3} \alpha p(e^-_{Y_K V_1}|v_1)p(v_1|y_K)p(y_K|x_K)p(e^-_{ZV_2}|v_2)p(v_2|z)p(z|y_K,y_D) \\
&\qquad p(e^-_{Y_D V_3}|v_3)p(v_3|y_D)p(y_D|x_D)p(x_K|e^+_{X_K Y_K})p(x_D|e^+_{X_D Y_D})\,dx_K\,dz\,dv_1\,dv_2 \\
&= \alpha p(e^-_{Y_K V_1}|y_K) \sum_{y_D,x_D} \int_{z,x_K} p(e^-_{ZV_2}|z)p(e^-_{Y_D V_3}|y_D)p(z|y_K,y_D)p(y_K|x_K)p(y_D|x_D)p(x_K|e^+_{X_K Y_K})p(x_D|e^+_{X_D Y_D})\,dz\,dx_K \\
&= \alpha p(e^-_{Y_K V_1}|y_K) \sum_{y_D} \int_{z,x_K} p(e^-_{ZV_2}|z)p(z|y_K,y_D)p(y_K|x_K)p(x_K|e^+_{X_K Y_K})p(e^-_{Y_D V_3}|y_D)p(y_D|e^+_{X_D Y_D})\,dz\,dx_K \\
&= \alpha p(e^-_{Y_K V_1}|y_K) \sum_{y_D} \int_{z,x_K} p(e^-_{ZV_2}|z)p(z|y_K,y_D)p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(y_K|x_K)p(x_K|e^+_{X_K Y_K})\,dz\,dx_K \\
&= \alpha p(e^-_{Y_K V_1}|y_K) \sum_{y_D} p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D}) \int_{x_K} p(y_K|x_K)p(x_K|e^+_{X_K Y_K})\,dx_K \int_z p(e^-_{ZV_2}|z)p(z|y_K,y_D)\,dz \\
&= \alpha p(e^-_{Y_K V_1}|y_K) \sum_{y_D} p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(e^-_{ZV_2}|y_K,y_D) \int_{x_K} p(y_K|x_K)p(x_K|e^+_{X_K Y_K})\,dx_K \\
&= \alpha p(e^-_{Y_K V_1}|y_K) \int_{x_K} p(y_K|x_K)p(x_K|e^+_{X_K Y_K})\,dx_K \sum_{y_D} p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(e^-_{ZV_2}|y_K,y_D) \qquad (80) \\
&= \alpha p(e^-_{ZV_2}|y_K,e^-_{Y_D V_3}) \int_{x_K} p(y_K|x_K)p(x_K|e^+_{X_K Y_K})\,dx_K \qquad (81) \\
&= \alpha p(e^-_{ZV_2}|y_K,e^-_{Y_D V_3})p(y_K|e^+_{X_K Y_K}) \qquad (82)
\end{aligned}
$$

Hence the Belief function for y_K can be written as:

$$
\begin{aligned}
\mathrm{Bel}(x_K,x_D,y_K,y_D,z,v_1,v_2,v_3) &= p(x_K,x_D,y_K,y_D,z,v_1,v_2,v_3|e^+_{X_K Y_K},e^+_{X_D Y_D},e^-_{Y_K V_1},e^-_{Y_K V_2},e^-_{Y_K V_3}) \\
&= \frac{p(x_K,x_D,y_K,y_D,z,v_1,v_2,v_3,e^+_{X_K Y_K},e^+_{X_D Y_D},e^-_{Y_K V_1},e^-_{Y_K V_2},e^-_{Y_K V_3})}{p(e^+_{X_K Y_K},e^+_{X_D Y_D},e^-_{Y_K V_1},e^-_{Y_K V_2},e^-_{Y_K V_3})} \\
&= \alpha p(e^-_{Y_K V_1}|v_1)p(v_1|y_K)p(y_K|x_K)p(e^-_{ZV_2}|v_2)p(v_2|z)p(z|y_K,y_D) \\
&\qquad p(e^-_{Y_D V_3}|v_3)p(v_3|y_D)p(y_D|x_D)p(x_K|e^+_{X_K Y_K})p(x_D|e^+_{X_D Y_D})
\end{aligned}
$$

Equation (81) follows from (80) because the evidence at node Y_D is known with probability 1 and therefore forces its value onto the node variable. The second term in equation (80) drops out because evaluation of the belief function for y_K implies that no hard evidence is available for y_K; otherwise, the node variable takes on the value of the hard evidence.

Similarly, for node Z:

$$\begin{aligned}
\mathrm{Bel}(z) &= \sum_{y_D,x_D,v_3} \int_{x_K,y_K,v_1,v_2} \mathrm{Bel}(x_K,x_D,y_K,y_D,z,v_1,v_2,v_3)dx_K dy_K dv_1 dv_2 \\
&= \sum_{y_D,x_D,v_3} \int_{x_K,y_K,v_1,v_2} \alpha p(e^-_{Y_K V_1}|v_1)p(v_1|y_K)p(y_K|x_K)p(e^-_{ZV_2}|v_2)p(v_2|z)p(z|y_K,y_D) \\
&\qquad p(e^-_{Y_D V_3}|v_3)p(v_3|y_D)p(y_D|x_D)p(x_K|e^+_{X_K Y_K})p(x_D|e^+_{X_D Y_D})dx_K dy_K dv_1 dv_2 \\
&= \sum_{y_D} p(e^-_{Y_D V_3}|y_D)p(y_D|e^+_{X_D Y_D})p(e^-_{ZV_2}|z) \int_{x_K,y_K} p(e^-_{Y_K V_1}|y_K)p(y_K|x_K)p(x_K|e^+_{X_K Y_K})p(z|y_K,y_D)dx_K dy_K \\
&= \sum_{y_D} p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(e^-_{ZV_2}|z) \int_{x_K,y_K} p(e^-_{Y_K V_1}|y_K)p(y_K|x_K)p(x_K|e^+_{X_K Y_K})p(z|y_K,y_D)dx_K dy_K \\
&= \sum_{y_D} p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(e^-_{ZV_2}|z) \int_{y_K} p(e^-_{Y_K V_1}|y_K)p(z|y_K,y_D) \int_{x_K} p(y_K|x_K)p(x_K|e^+_{X_K Y_K})dx_K dy_K \\
&= \sum_{y_D} p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(e^-_{ZV_2}|z)p(z|e^-_{Y_K V_1},y_D) \int_{x_K} p(e^-_{Y_K V_1}|x_K)p(x_K|e^+_{X_K Y_K})dx_K \\
&= \sum_{y_D} p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(e^-_{ZV_2}|z)p(z|e^-_{Y_K V_1},y_D) \qquad (83) \\
&= p(z|e^-_{Y_K V_1},e^-_{Y_D V_3}) \qquad (84)
\end{aligned}$$

As above, equation (84) follows from (83) because the evidence at node Y_D is dominant and therefore forces its value onto the node variable. Furthermore, it is assumed that the evidence at node Z does not exist; otherwise, it takes on the value of the evidence.

Similarly, for node Y_D,

$$\begin{aligned}
\mathrm{Bel}(y_D) &= \sum_{x_D,v_3}\int_{x_K,y_K,z,v_1,v_2}\mathrm{Bel}(x_K,x_D,y_K,y_D,z,v_1,v_2,v_3)dx_K dy_K dv_1 dv_2 \\
&= \sum_{x_D,v_3}\int_{x_K,y_K,v_1,v_2}\alpha p(e^-_{Y_K V_1}|v_1)p(v_1|y_K)p(y_K|x_K)p(e^-_{Z V_2}|v_2)p(v_2|z)p(z|y_K,y_D) \\
&\qquad p(e^-_{Y_D V_3}|v_3)p(v_3|y_D)p(y_D|x_D)p(x_K|e^+_{X_K Y_K})p(x_D|e^+_{X_D Y_D})dx_K dy_K dv_1 dv_2 \\
&= \sum_{x_D}\int_{z,x_K,y_K} p(e^-_{Y_K V_1}|y_K)p(e^-_{Z V_2}|z)p(y_K|x_K)p(z|y_K,y_D)p(e^-_{Y_D V_3}|y_D) \\
&\qquad p(y_D|x_D)p(x_K|e^+_{X_K Y_K})p(x_D|e^+_{X_D Y_D})dz dx_K dy_K \\
&= p(y_D|e^+_{X_D Y_D})p(e^-_{Y_D V_3}|y_D)\int_{x_K,y_K} p(e^-_{Z V_1}|y_K)p(e^-_{Z V_2}|z)p(y_K|x_K)p(z|y_K,y_D)p(x_K|e^+_{X_K Y_K})dz dx_K dy_K \\
&= p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})\int_{x_K,y_K}\delta(e^-_{Y_K V_1}-y_K)p(y_K|x_K)p(x_K|e^+_{X_K Y_K})\int_z p(z|y_K,y_D)\delta(e^-_{Z V_2}-z)dz dx_K dy_K \\
&= p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})\int_{x_K,y_K}\delta(e^-_{Y_K V_1}-y_K)p(y_K|x_K)p(x_K|e^+_{X_K Y_K})p(e^-_{Z V_2}|y_K,y_D)dx_K dy_K \\
&= p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})\int_{x_K} p(e^-_{Y_K V_1}|x_K)p(x_K|e^+_{X_K Y_K})p(e^-_{Z V_2}|e^-_{Y_K V_1},y_D)dx_K \\
&= p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(e^-_{Z V_2}|e^-_{Y_K V_1},y_D)\int_{x_K} p(x_K|e^-_{Y_K V_1},e^+_{X_K Y_K})dx_K \\
&= p(y_D|e^-_{Y_D V_3},e^+_{X_D Y_D})p(e^-_{Z V_2}|e^-_{Y_K V_1},y_D) \qquad (85) \\
&= p(y_D|e^+_{X_D Y_D})p(e^-_{Z V_2}|e^-_{Y_K V_1},y_D) \qquad (86)
\end{aligned}$$

Again equation (86) follows from (85) because it is assumed that evidence at Y_D does not exist; otherwise, y_D takes on the value of the evidence. Clearly, Bel(y_D) does not depend on evidence at node X_K.

The threat assessment process described above generates inferred values that do not require further human interpretation to estimate threat, due to the inclusion of the relevant inferential criteria, including those previously reserved for 'human judgement,' in the process via the criteria based causal networks of Figures 1 and 7. In comparison to prior art processes based on junction tree methods, the threat assessment process is able to generate inferred values using both continuous and mixed nodes with greatly reduced computational complexity, particularly in back-propagation of evidence. The functions representing causal relationships can be discontinuous, as in the military applications described herein, and the distributions of input variables do not have to be Gaussian distributions.

For each potential threat observed in an operational space, the threat relationships are represented by a full Bayesian belief network that is instantiated in real time with data from a real–time data base (in the above defence scenario, populated by a level 1 tracking and data fusion system). All relationships within the operational space are represented dynamically in real–time. The processing load associated with the threat assessment process scales linearly with the number of threatening entities and assets.

EXAMPLE

A level 1 fusion surveillance picture was generated from data supplied by a network of sensors, trackers, and data fusion processes, as described in Okello1998 and Okello2000. This level 1 fusion surveillance picture was then used as input to the threat assessment system.

Figure 8 shows the actual movements or 'ground-truths' in two dimensions of two intruders (targets 1 and 2) of known type in the vicinity of two stationary assets 802, 804. The intruder of type 1 has a constant speed of 600 km/hr and maintains a constant altitude of 10000 m over a spherical earth while continuously emitting a signal that categorizes it as a type 1 target. The intruder of type 3 has a constant speed of 1000 km/hr and maintains a constant altitude of 9000 m while continuously emitting a signal that categorizes it as a type 3 target. This provides a simple multi-intruder multi-asset threat scenario. The numbers on the intruder ground-truths are target birth and death times in seconds measured from radar and electronic support measure (ESM) activation time. The target type information is related through a look-up table to the type of weapon carried by a platform of the identified type.

The scenario of Figure 8 was used to generate radar and ESM measurements at separate locations within the surveillance area. These were then processed by local trackers and the resulting sensor-level tracks were then fused to obtain a surveillance picture in which each tracked entity is comprehensively described in terms of its continuous kinematic and discrete type estimates. Figure 9 shows the resulting track estimates generated by a Cartesian-based

multitarget IMM-tracker that processes measurements from Radar 1. The Figure shows a first track 900 taken by one aircraft referred to as "target 1", and a second path taken by the other aircraft, referred to as "target 2". Figure 10 is a graph of the corresponding height estimates, with a first solid line 1002 representing the height or altitude of target 1 estimated at around 9,000 m, and a second solid line 1004 representing the height of target 2, estimated at around 10,000 m. Figure 11 is a graph of the corresponding speed estimates with the speed 1102 of target 1 estimated at 1,000 km h^{-1}, and the speed 1104 of target 2 estimated at around 600 km h^{-1}. Figures 12 and 13 are graphs of the corresponding location and speed variances for targets 1 and 2, respectively.

The discrete component of each ESM measurement is a vector of aircraft type probabilities with components given by $P(T_p|w(k))$, $p = 1, ..., N_T$, where $N_T = 3$ is the number of aircraft types in the ESM library. Aircraft of unknown types are lumped under target type probability $P(T_{N_T+1}|w(k)) = 1 - \sum_{p=1}^{N_T} P(T_p|w(k))$. In this example, target 1 is of type 1 and the ESM type measurements originating from this target are generated from a Dirichlet distribution with the parameter vector α = [5 2 2 2]. Similarly, target 2 is of type 3 and the ESM type measurements originating from this target are generated from a Dirichlet distribution with parameter vector α = [2 2 5 2]. Furthermore, any clutter measurement is generated based on the parameter vector α = [2 2 2 5]. Thus while the kinematic component of the ESM are processed using the modified polar coordinates-based bearings-only tracker, these discrete type measurements are processed using a Bayesian filter. The output of such a filter is a vector of type probabilities with components given by $P(T_p|W^k)$, $p = 1, ..., N_T + 1$ where W^k is the set of all measurements up to time k. We assume that track-to-measurement association and track-to-track association are possible. Figures 10 and 11 show target type probabilities for tracks 1 and 4, respectively. These plots were generated by a Bayesian filter following the processing of ESM type measurements, as described in Okello1998 and Okello2000. It was assumed that the target types differ only in the size of their weapon envelopes, and that the target types T_1, T_2, T_3, and T_4 have semi-circular weapon envelopes with radii of 50 km, 40 km, 60 km, and 2 km, respectively.

For comparison purposes, the same set of level 1 data described above was independently processed by the belief propagation process of the belief propagation module 314 and the direct integration process of the selective marginalisation module 312. Figures 16 and 17 show numerical results generated by the belief propagation process. However, identical results (not shown) were generated by the direct integration process.

Figure 16 includes four graphs of the two components of the intermediate node **y** for each of the two possible target types, as determined from the level 1 tracking data and fusion input data of Figures 9 to 15. The top left graph 1602 presents, as a function of time step k, the mean value of the first component of the intermediate variable **y** (refer to Equations 5 and 8), being the length of the intruder-to-asset range vector $|r_{ij}|$ for the first intruder target 1, and the top right graph 1604 presents the second component of **y**, being the angle between the intruder velocity vector and the intruder-to-asset range vector $\mathbf{r}_{ij}$. The bottom left graph 1606 and bottom right graph 1608 are equivalent graphs for the second intruder, target 2. Figure 17 includes four graphs showing the mean and covariances of the threat to each of the two stationary assets 802,804 . The top left graph shows that the threat 1702 to the first asset rises to a first peak 1700 having a value of around 0.5 near time step 80 as a consequence of target 1 approaching asset 1, the threat 1702 rapidly decreasing as target 1 passes asset 1. A second peak 1704 at around time step 500 is due to target 2 approaching and then passing asset 1. Similarly, the bottom left graph shows that the threat 1706 to asset 2 is initially high due to the close proximity and orientation of target 1, rapidly decreasing as target 1 passes asset 2. The threat due to the approach of target 2 increases gradually to a peak at around time step 300 due to the approach of target 2, and rapidly decreases to zero as target 2 heads away from asset 2.

The threat assessment process thus allows the threat posed by one or more threatening entities to one or more assets to be automatically assessed in real-time without requiring human judgement or involvement. The threat values thus generated by the threat assessment system can be used to prepare a suitable response to these threats.

The observation that the belief propagation process and the direct integration process give identical results suggests that these processes are sufficiently versatile to handle a wide range of complex problems. In particular, these processes can be used to solve Bayesian network problems having a mixture of continuous and discrete nodes; in cases where the continuous nodes are not Gaussian, conservative results based on a Gaussian approximation are easily obtainable. Furthermore, it has been demonstrated that non-linearities and discontinuities in the conditional dependence between connected nodes is not an obstacle when using any of the processes described herein.

Many modifications will be apparent to those skilled in the art without departing from the scope of the present invention as herein described with reference to the accompanying drawings.

CLAIMS:

1. A threat assessment system, including:

one or more linearisation modules for generating by linear approximation a conditional probability distribution of a first continuous variable on the basis of a non-linear causal relationship between said first continuous variable and a continuous state variable representing a state of a threatening entity, and for generating by linear approximation a conditional probability distribution of a second continuous variable representing a threat posed by said threatening entity to an asset on the basis of a non-linear causal relationship between said second continuous variable, said first continuous variable, and a discrete state variable representing a state of said threatening entity;

a multiplier module for generating, on the basis of said conditional probability distributions, a joint belief function for assessing said threat; and

a belief function generator for generating a belief function for said second continuous variable on the basis of said joint belief function.

2. A system as claimed in claim 1, wherein the multiplier module is adapted to generate the joint belief function for assessing said threat as the product of said conditional probability distributions and conditional probability distributions for the continuous and discrete state variables of said threatening entity.

3. A system as claimed in claim 2, wherein the system further includes a parameterisation module for generating a conditional probability distribution of a discrete variable with respect to the discrete state variable of said threatening entity, and the multiplier module is adapted to generate the joint belief function for assessing said threat as the product of said conditional probability distributions.

4. A threat assessment system, including:

a causal network module representing causal relationships between variables for assessing a threat posed by a threatening entity to an asset, said causal relationships including one or more non-linear relationships;

one or more parameterisation modules for generating conditional probability distributions for said variables, including generating by linear approximation one or more conditional probability distributions representing said one or more non-linear relationships; and

a multiplier module for generating a joint belief function for assessing said threat on the basis of the conditional probability distributions for said variables.

5. A threat assessment system for assessing at least one threat posed at least one threatening entity to at least one asset, the system including a capability generator for generating one or more capability values representing respective capabilities of one or more threatening entities to threaten one or more assets;

an intent generator for generating one or more intent values representing intent of said one or more threatening entities to threaten said one or more assets; and

a threat assessment module for generating one or more threat values representing respective threats posed by said one or more threatening entities to said one or more assets on the basis of said capability values and said intent values.

6. A threat assessment system for assessing at least one threat posed at least one threatening entity to at least one asset, the system being adapted to generate conditional probability distributions representing relationships between nodes of a causal network representing said at least one threat, said nodes including at least one entity state node representing a state of a corresponding threatening entity, criteria nodes representing variables dependent on said state and being child nodes of said at least one entity node, and at least one threat node being a child node of said criteria nodes, said at least one threat node representing a threat posed by said at least one threatening entity to a corresponding asset.

7. A system as claimed in claim 6, wherein said causal network includes one or more leaf nodes as children of respective child nodes of said network for backwards propagation of evidence to parent nodes of said leaf node.

8. A system as claimed in claim 6, wherein said variables include one or more discrete variables and one or more continuous variables.

9. A system as claimed in claim 6, wherein said causal network includes one or more information nodes for use in determining the states of said at least one entity node and being parent nodes to said at least one entity node.

10. A threat assessment system for assessing at least one threat posed at least one threatening entity to at least one asset, the system being adapted to generate conditional probability distributions representing relationships between nodes of a causal network, said causal network including:

at least one entity node representing a state of a corresponding threatening entity;

a capability node for each entity-asset pair representing the capability of a corresponding threatening entity to threaten a corresponding asset, the capability node being a child node of the entity node of the corresponding threatening entity;

an intent node for each entity-asset pair representing the intent of the corresponding threatening entity to attack the corresponding asset, the intent node being a child node of the entity node of the corresponding threatening entity; and

at least one threat node representing a threat posed by a corresponding threatening entity to a corresponding asset, said at least one threat node being a child node of the corresponding capability node and the corresponding intent node.

11. A system as claimed in claim 10, wherein said at least one threatening entity includes an aircraft.

12. A threat assessment system, including:

a causal network module representing causal relationships between variables for assessing a threat posed by a threatening entity to an asset;

one or more parameterisation modules for generating conditional probability distributions representing linear relationships of said causal relationships

one or more linearisation modules for generating by linear approximation conditional probability distributions representing non-linear relationships of said causal relationships; and

a multiplier for generating a joint belief function for assessing said threat by multiplying the conditional probability distributions representing said relationships.

13. A system as claimed in claim 12, including a belief function generator for generating from said joint belief function at least one belief function for at least one of said variables.

14. A system as claimed in claim 13, wherein the belief function generator is adapted to generate the at least one belief function by selective marginalisation or belief propagation.

15. A threat assessment process, including:

generating by linear approximation a conditional probability distribution of a first continuous variable on the basis of a non-linear causal relationship between said first continuous variable and a continuous state variable representing a state of a threatening entity;

generating by linear approximation a conditional probability distribution of a second continuous variable representing a threat posed by said threatening entity to an asset on the basis of a non-linear causal relationship between said second continuous variable, said first continuous variable, and a discrete state variable representing a state of said threatening entity;

generating, on the basis of said conditional probability distributions, a joint belief function for assessing said threat; and

generating a belief function for said second continuous variable on the basis of said joint belief function to assess said threat.

16. A process as claimed in claim 15, including generating a conditional probability distribution of a first discrete variable on the basis of a causal relationship between said first discrete variable and the discrete state variable representing a state of a threatening entity.

17. A process as claimed in claim 16, wherein said joint belief function is generated by multiplying the conditional probability distributions for the first and second continuous variables and the first discrete variable, and conditional probability distributions for the continuous and discrete state variables.

18. A process as claimed in claim 15, wherein the continuous state variable represents location and velocity components of a threatening entity, and the discrete state variable represents a type of said threatening entity.

19. A process as claimed in claim 18, wherein the type of said threatening entity determines a weapon type of said threatening entity.

20. A process as claimed in claim 19, wherein the weapon type of said threatening entity determines a range of said weapon type.

21. A process as claimed in claim 15, wherein the first continuous variable includes a distance from the threatening entity to the asset and an angle between the velocity of the threatening entity and a straight line joining the asset and the threatening entity.

22. A threat assessment process, including:

generating one or more capability values representing respective capabilities of one or more threatening entities to threaten one or more assets;

generating one or more intent values representing intent of said one or more threatening entities to threaten said one or more assets; and

generating one or more threat values representing respective threats posed by said one or more threatening entities to said one or more assets on the basis of said capability values and said intent values.

23. A process as claimed in claim 22, including receiving state data representing state variables of each threatening entity, said capability values and said intent values being generated on the basis of said state data.

24. A process as claimed in claim 22, wherein said state variables include location variables and velocity variables for said one or more threatening entities.

25. A process as claimed in claim 22, wherein each of said one or more threatening entities includes a weapon for firing a projectile over a predetermined range from the threatening entity.

26. A process as claimed in claim 22, including generating distance data representing distances between each threatening entity and each asset, said capability values and said intent values being generated on the basis of said distance data.

27. A process as claimed in claim 22, wherein each of said capability values is generated on the basis of a distance between a corresponding threatening entity and a corresponding asset, and a predetermined range of a weapon of the corresponding threatening entity.

28. A process as claimed in claim 22, wherein each of said capability values is proportional to a ratio of a predetermined range of a weapon of a corresponding threatening entity and a distance between the corresponding threatening entity and a corresponding asset unless said distance is less than said range.

29. A process as claimed in claim 22, wherein each of said intent values is generated on the basis of a rate of change of a distance between a corresponding threatening entity and a corresponding asset, and a velocity of the corresponding threatening entity.

30. A process as claimed in claim 22, wherein each of said intent values is equal to an absolute value of a ratio of a rate of change of a distance between a corresponding threatening entity and a corresponding asset, and a velocity of the corresponding threatening entity, if said rate of change of said distance if less than or equal to zero, and zero otherwise.

31. A process as claimed in claim 22, wherein each of said threat values is generated as a product of one or more corresponding capability values and intent values for respective threatening entities.

32. A process as claimed in claim 22, wherein said values and said state data are represented as probability distributions.

33. A process as claimed in claim 22, wherein said probability distributions are Gaussian distributions.

34. A process as claimed in claim 22, wherein each of said capability values is generated as a conditional probability distribution on the basis of a causal relationship between the capability value and a corresponding state variable.

35. A process as claimed in claim 22, wherein each of said intent values is generated as a conditional probability distribution on the basis of a causal relationship between the intent value and a corresponding state variable.

36. A process as claimed in claim 22, including generating, for each asset, a joint belief function on the basis of said conditional probability distributions; and

generating, for each asset, a probability distribution representing the threat posed by said one or more threatening entities to the corresponding asset on the basis of the corresponding joint belief function.

37. A process as claimed in claim 22, including updating one or more of said probability distributions on the basis of received evidence for one or more of said values.

38. A threat assessment process, including:

determining causal relationships between variables for assessing a threat posed by a threatening entity to an asset, said causal relationships including one or more non-linear relationships;

generating conditional probability distributions for said variables, including generating by linear approximation one or more conditional probability distributions representing said one or more non-linear relationships; and

generating a joint belief function for assessing said threat on the basis of the conditional probability distributions for said variables.

39. A process as claimed in claim 38, including generating one or more belief functions for respective ones of said variables on the basis of said joint belief function.

40. A process as claimed in claim 38, wherein each of said one or more belief functions is generated using selective marginalisation or belief propagation.

41. A process as claimed in claim 38, wherein said conditional probability distributions are Gaussian distributions.

42. A process as claimed in claim 38, wherein said joint belief function is generated as the product of said conditional probability distributions.

43. A process as claimed in claim 38, wherein said variables include one or more continuous variables and one or more discrete variables.

44. A threat assessment process, including:

receiving tracking and identification data including conditional probability distributions of kinematic data and type data of a threatening entity, said kinematic data representing a location and velocity of the threatening entity, and said type data representing a type of said threatening entity selected from a plurality of entity types;

generating, on the basis of the conditional probability distributions of kinematic data and a location of an asset, conditional probability distributions of entity-asset data representing separation of the threatening entity and the asset and an angle between the velocity vector of the threatening entity and a vector joining the threatening entity and the asset;

generating, on the basis of the conditional probability distributions of entity-asset data, a conditional probability distribution of threat data with respect to the entity-asset data and the type data of the threatening entity;

multiplying the conditional probability distributions of entity-asset data, the conditional probability distribution of threat data, the conditional probability distributions of kinetic data, and the conditional probability distribution of type data to generate a joint belief function of said threat data, said entity-asset data, said kinetic data, and said type data; and

generating, from said joint belief function, respective belief functions for one or more of said threat data, said entity-asset data, said kinetic data, and said type data.

45. A process as claim in claim 44, wherein the respective belief functions are generated by selective marginalisation or belief propagation.

46. A system having components for executing the steps of any one of claims 15 to 45.

47. A computer readable storage medium having stored thereon program instructions for executing the steps of any one of claims 15 to 45.

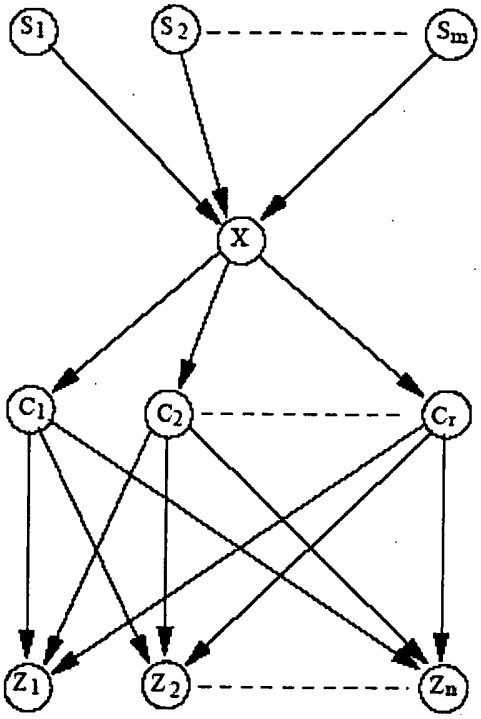


Figure 1

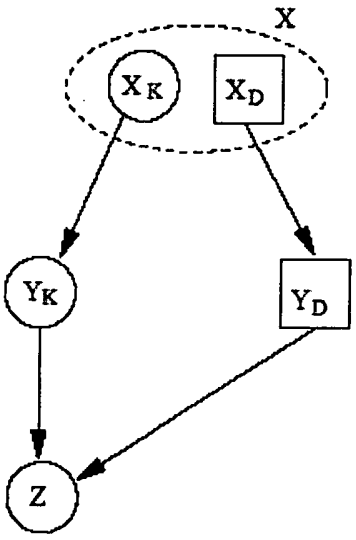


Figure 2

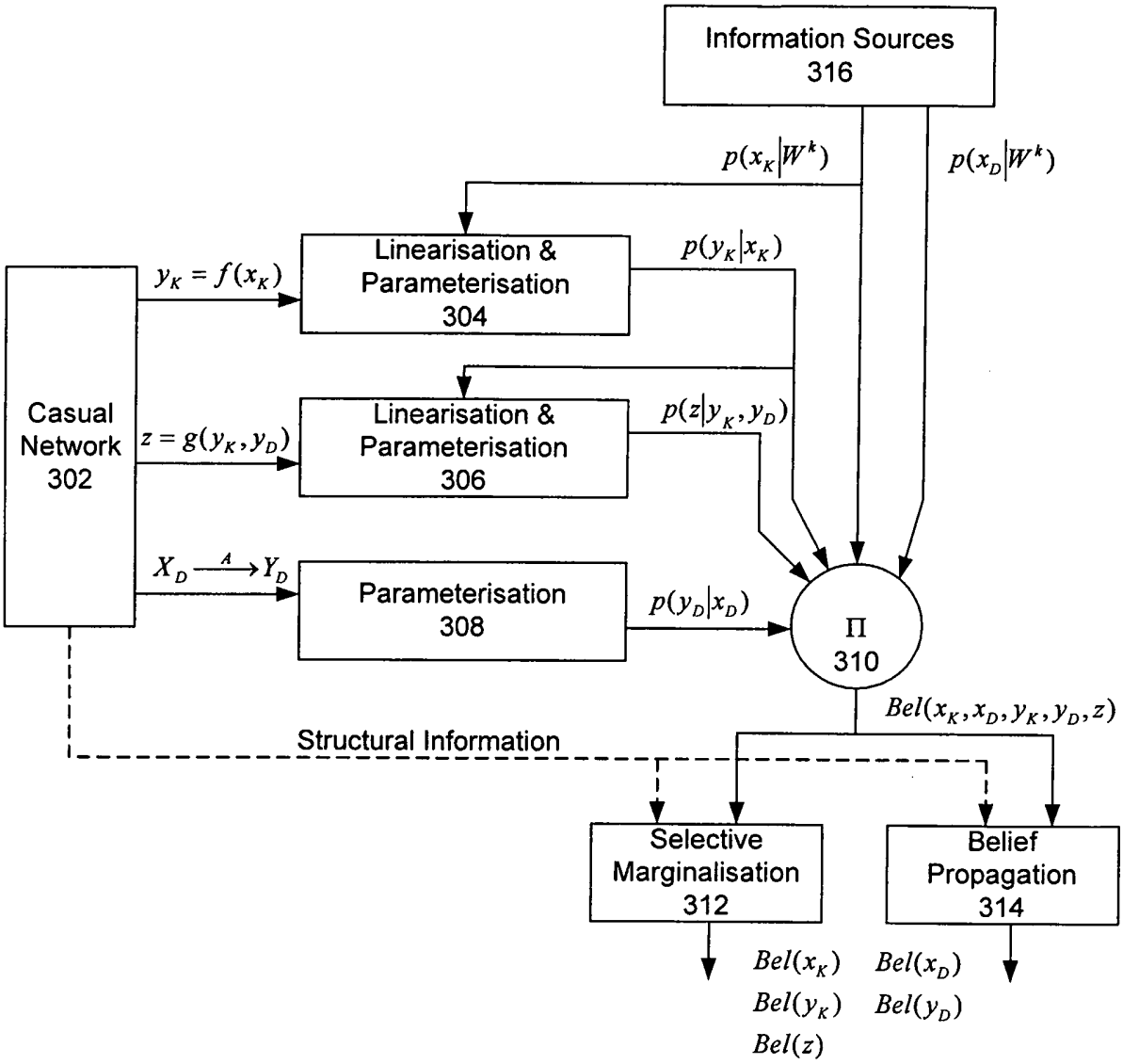

Information Sources
316
$p(x_K|W^k)$
$p(x_D|W^k)$
Linearisation &
Parameterisation
304
$p(y_K|x_K)$
$y_K = f(x_K)$
Casual
Network
302
Linearisation &
Parameterisation
306
$p(z|y_K, y_D)$
$z = g(y_K, y_D)$
$X_D \xrightarrow{A} Y_D$
Parameterisation
308
$p(y_D|x_D)$
Π
310
$Bel(x_K, x_D, y_K, y_D, z)$
Structural Information
Selective
Marginalisation
312
Belief
Propagation
314
$Bel(x_K)$
$Bel(y_K)$
$Bel(z)$
$Bel(x_D)$
$Bel(y_D)$

Figure 3

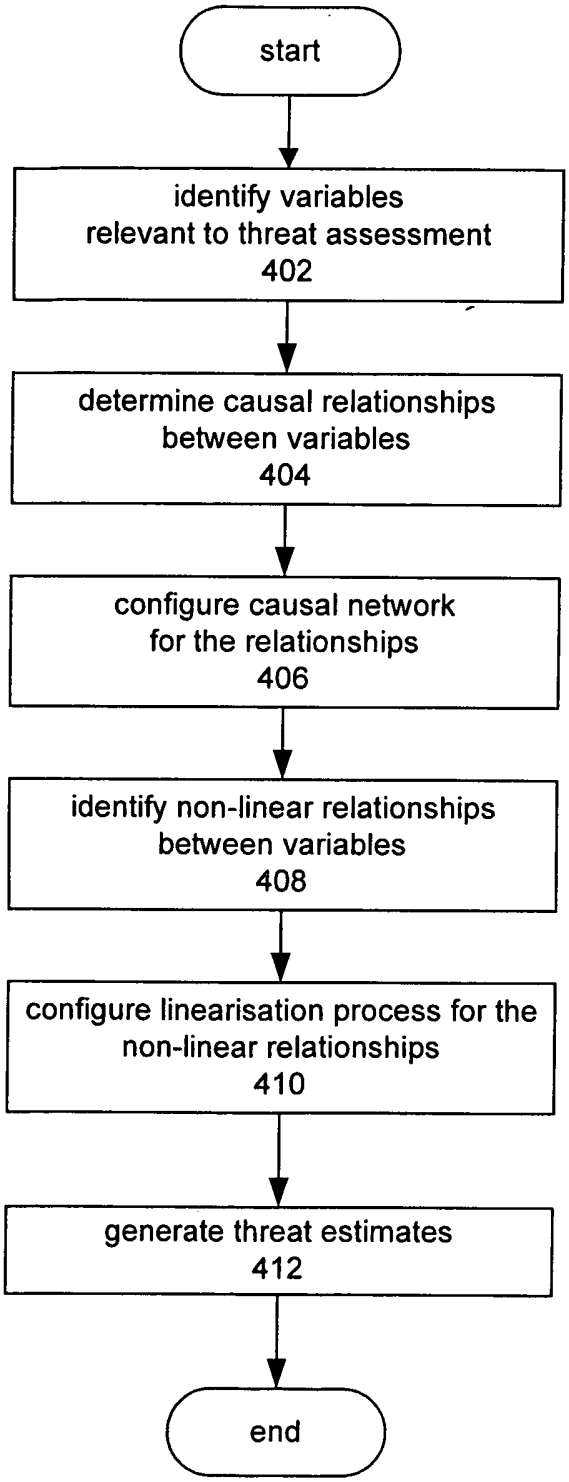

start
identify variables relevant to threat assessment 402
determine causal relationships between variables 404
configure causal network for the relationships 406
identify non-linear relationships between variables 408
configure linearisation process for the non-linear relationships 410
generate threat estimates 412
end

Figure 4

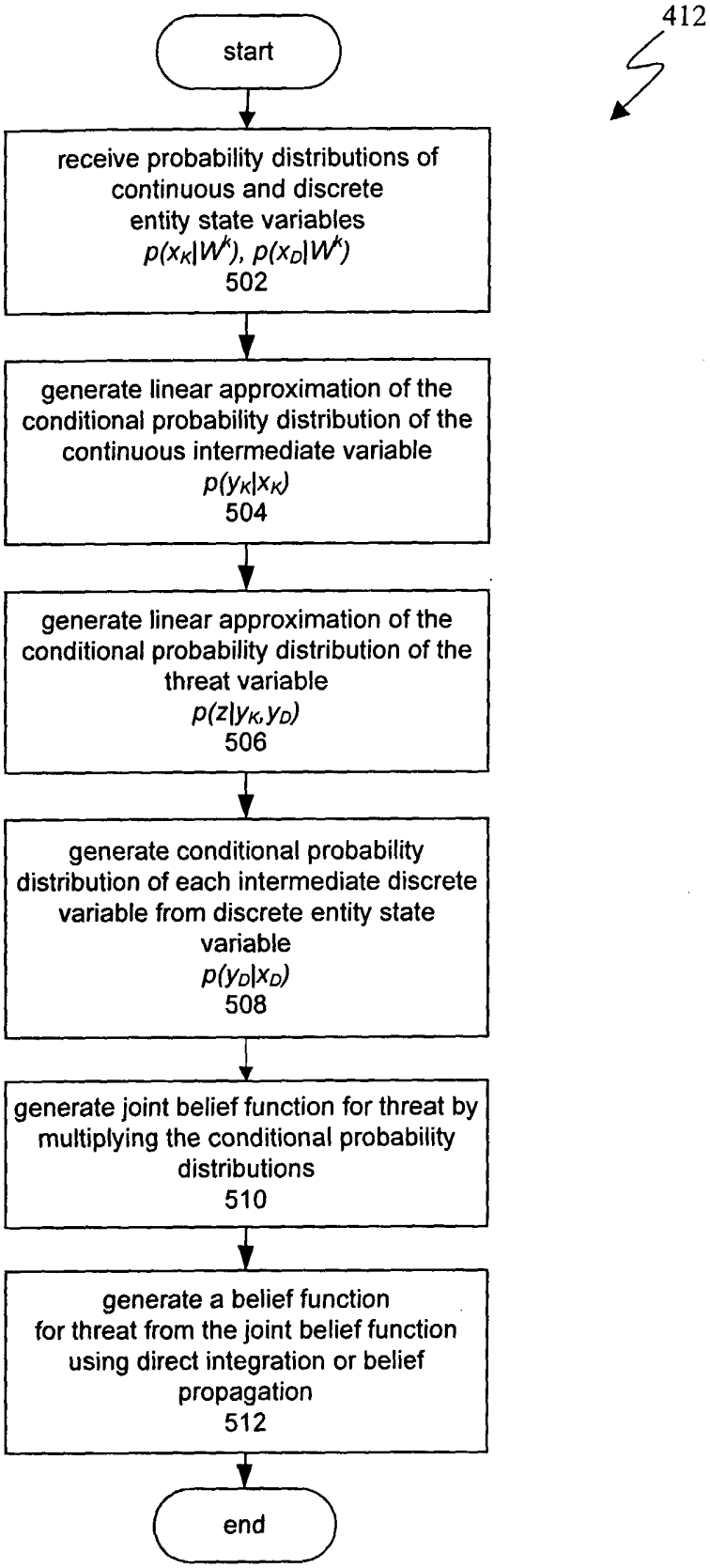

412
start
receive probability distributions of continuous and discrete entity state variables $p(x_K|W^k)$, $p(x_D|W^k)$ 502
generate linear approximation of the conditional probability distribution of the continuous intermediate variable $p(y_K|x_K)$ 504
generate linear approximation of the conditional probability distribution of the threat variable $p(z|y_K,y_D)$ 506
generate conditional probability distribution of each intermediate discrete variable from discrete entity state variable $p(y_D|x_D)$ 508
generate joint belief function for threat by multiplying the conditional probability distributions 510
generate a belief function for threat from the joint belief function using direct integration or belief propagation 512
end

Figure 5

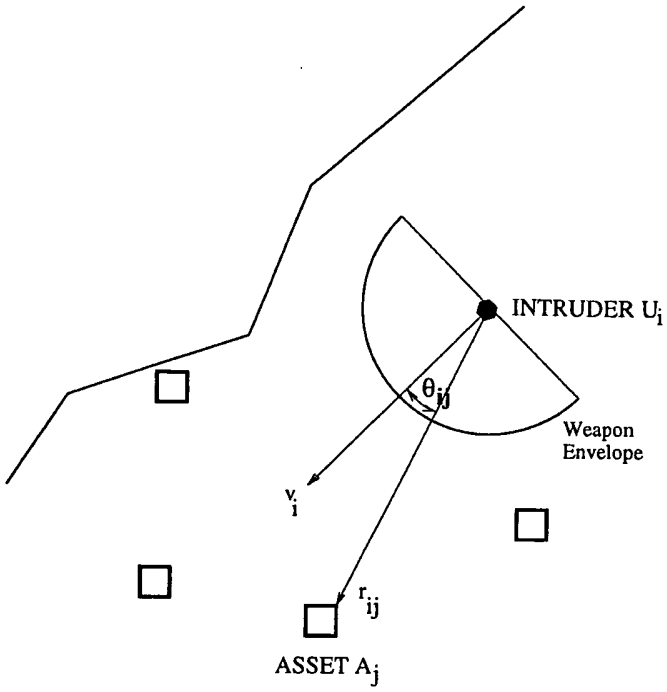


Figure 6

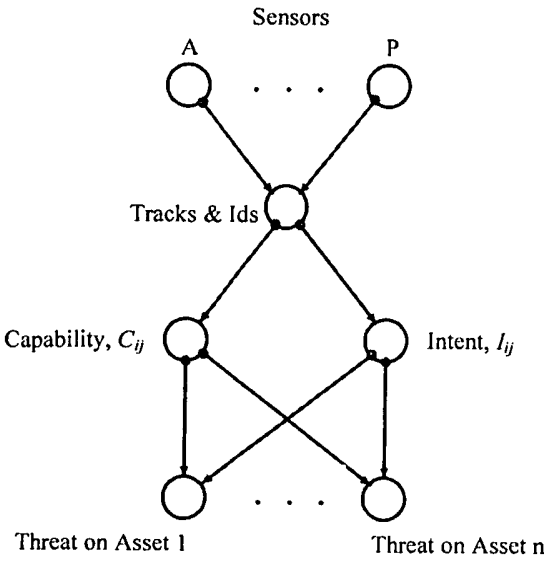


Figure 7

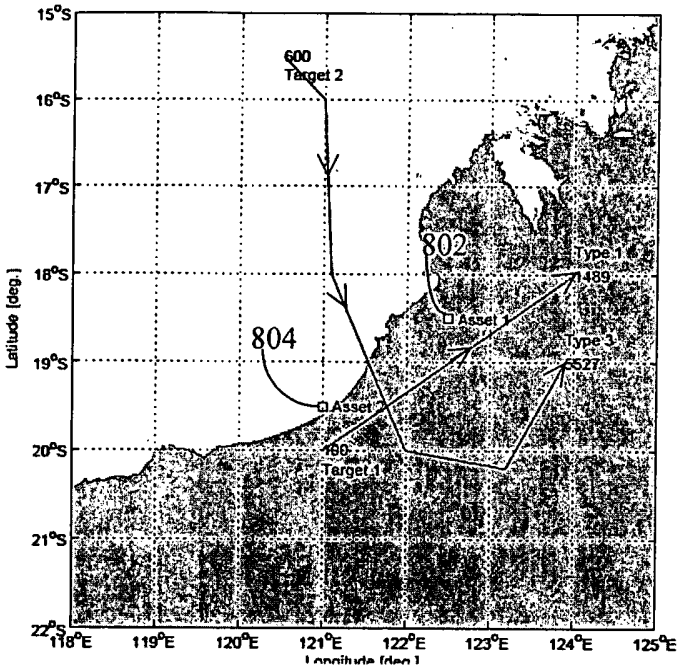


Figure 8

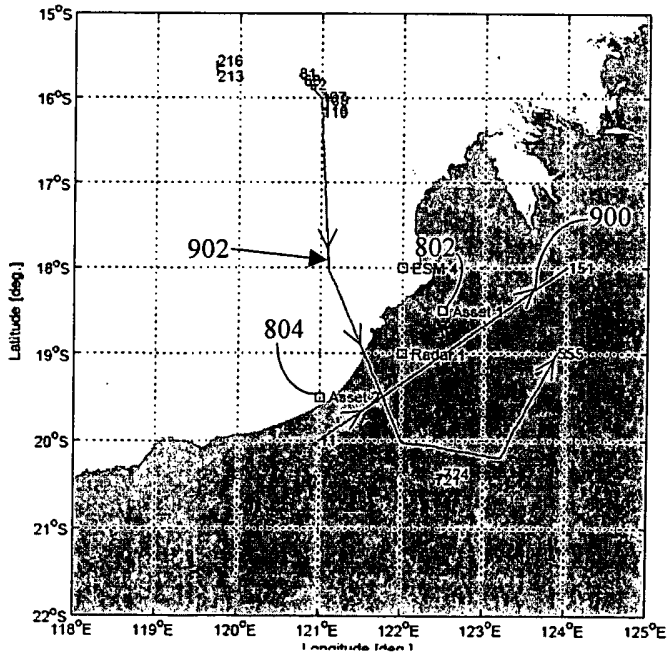


Figure 9

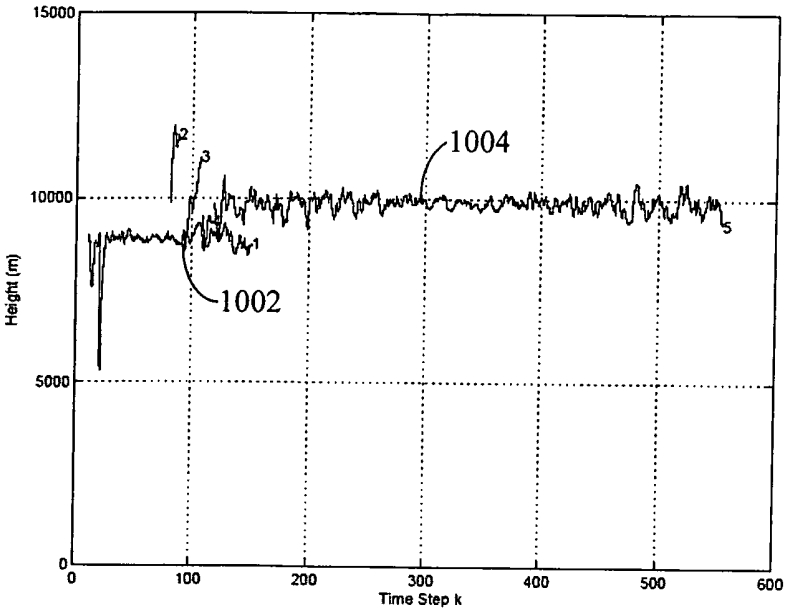


Figure 10

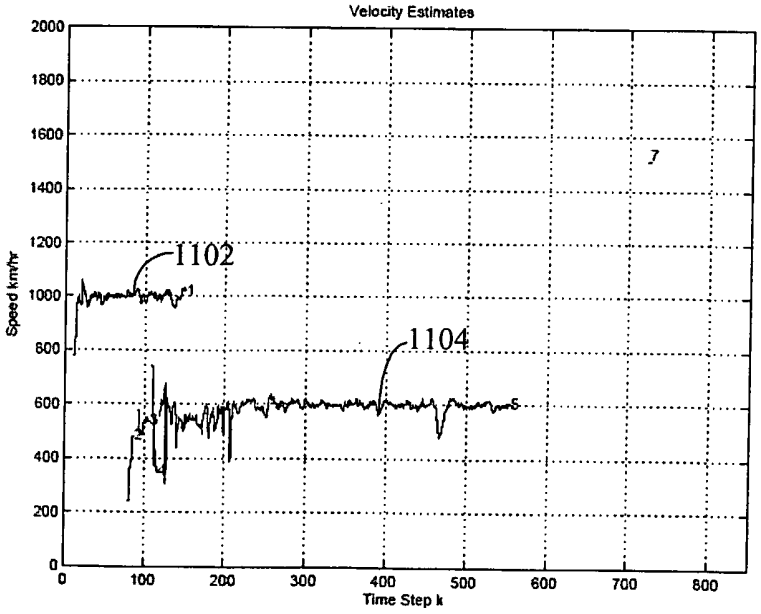


Figure 11

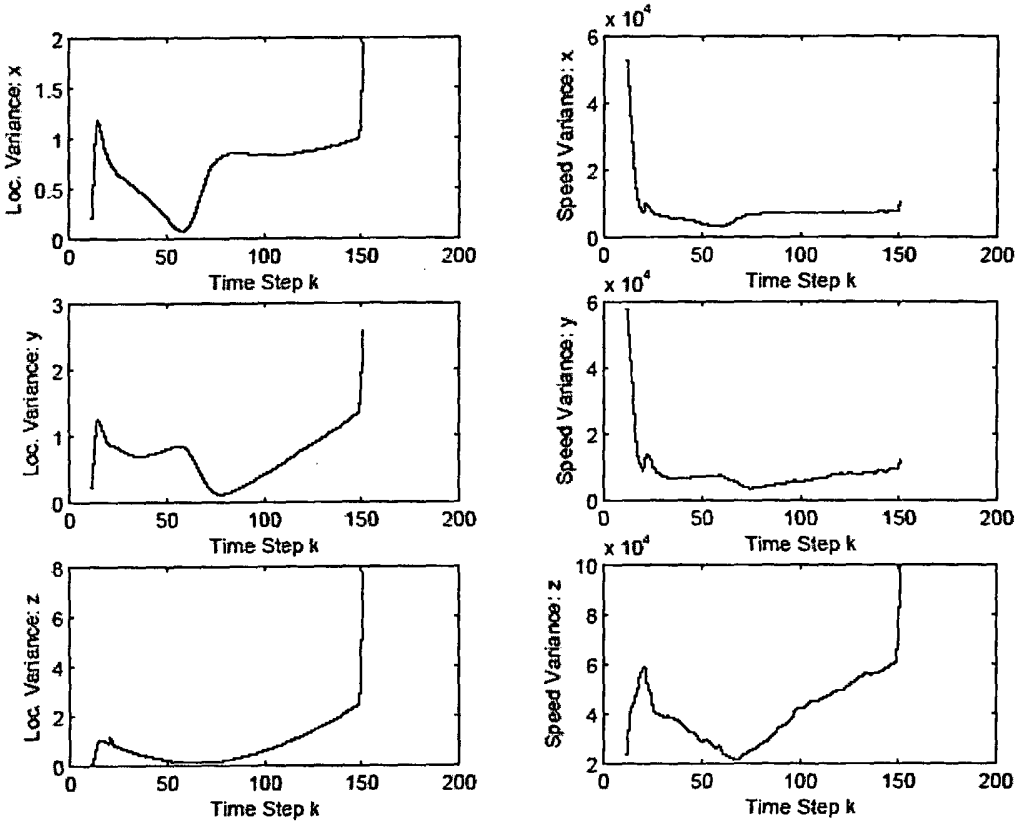

Loc. Variance: x
Time Step k
Speed Variance: x
x 10^4
Time Step k
Loc. Variance: y
Time Step k
Speed Variance: y
x 10^4
Time Step k
Loc. Variance: z
Time Step k
Speed Variance: z
x 10^4
Time Step k

Figure 12

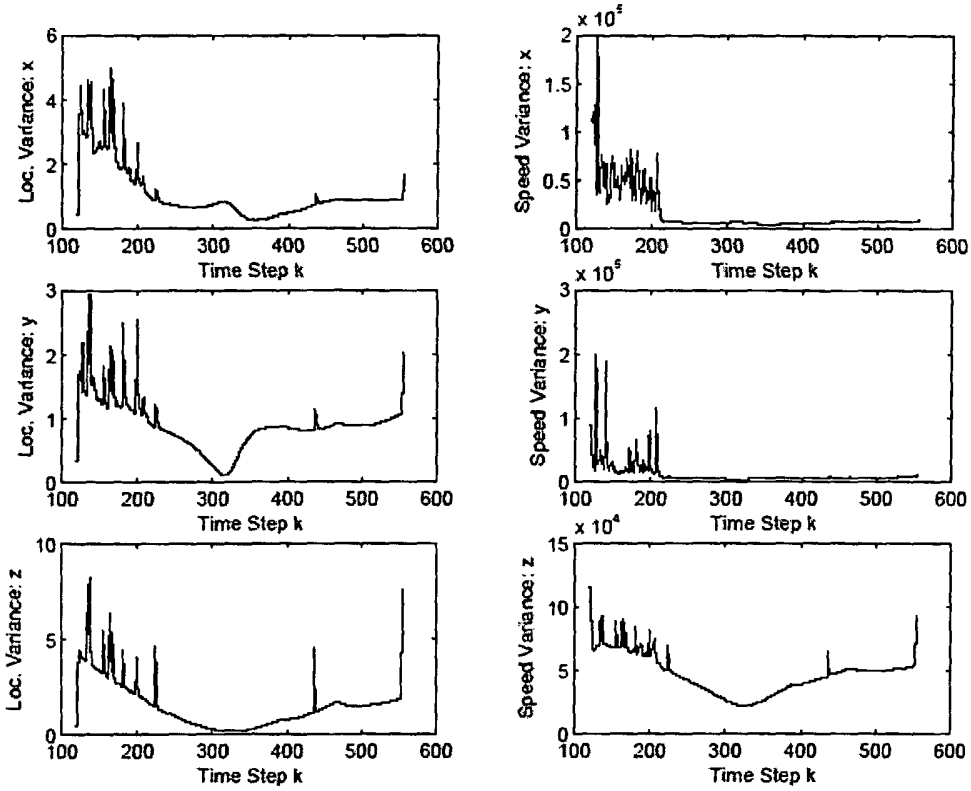

Loc. Variance: x
Time Step k
Speed Variance: x
x 10^5
Loc. Variance: y
Time Step k
Speed Variance: y
x 10^5
Loc. Variance: z
Time Step k
Speed Variance: z
x 10^4
Time Step k

Figure 13

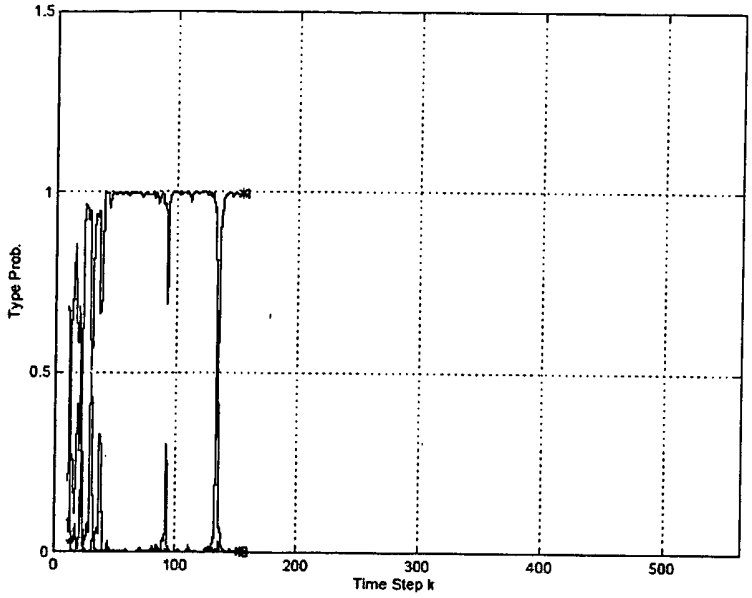


Figure 14

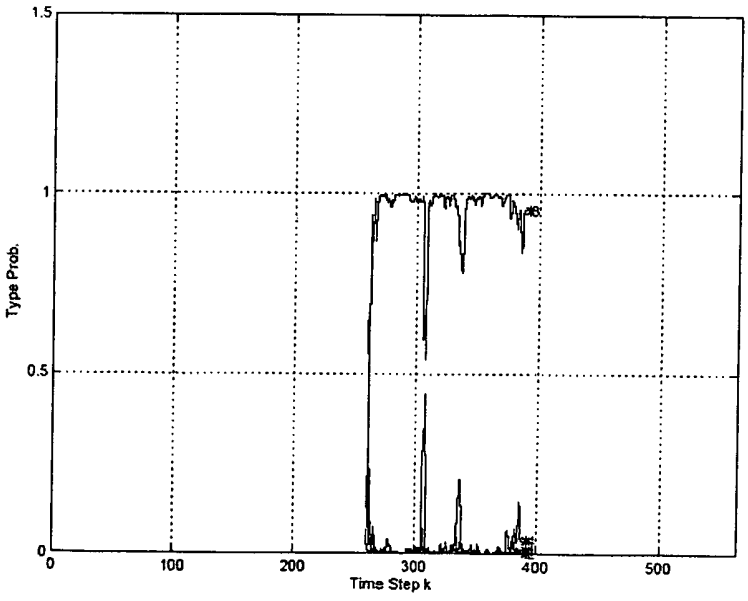


Figure 15

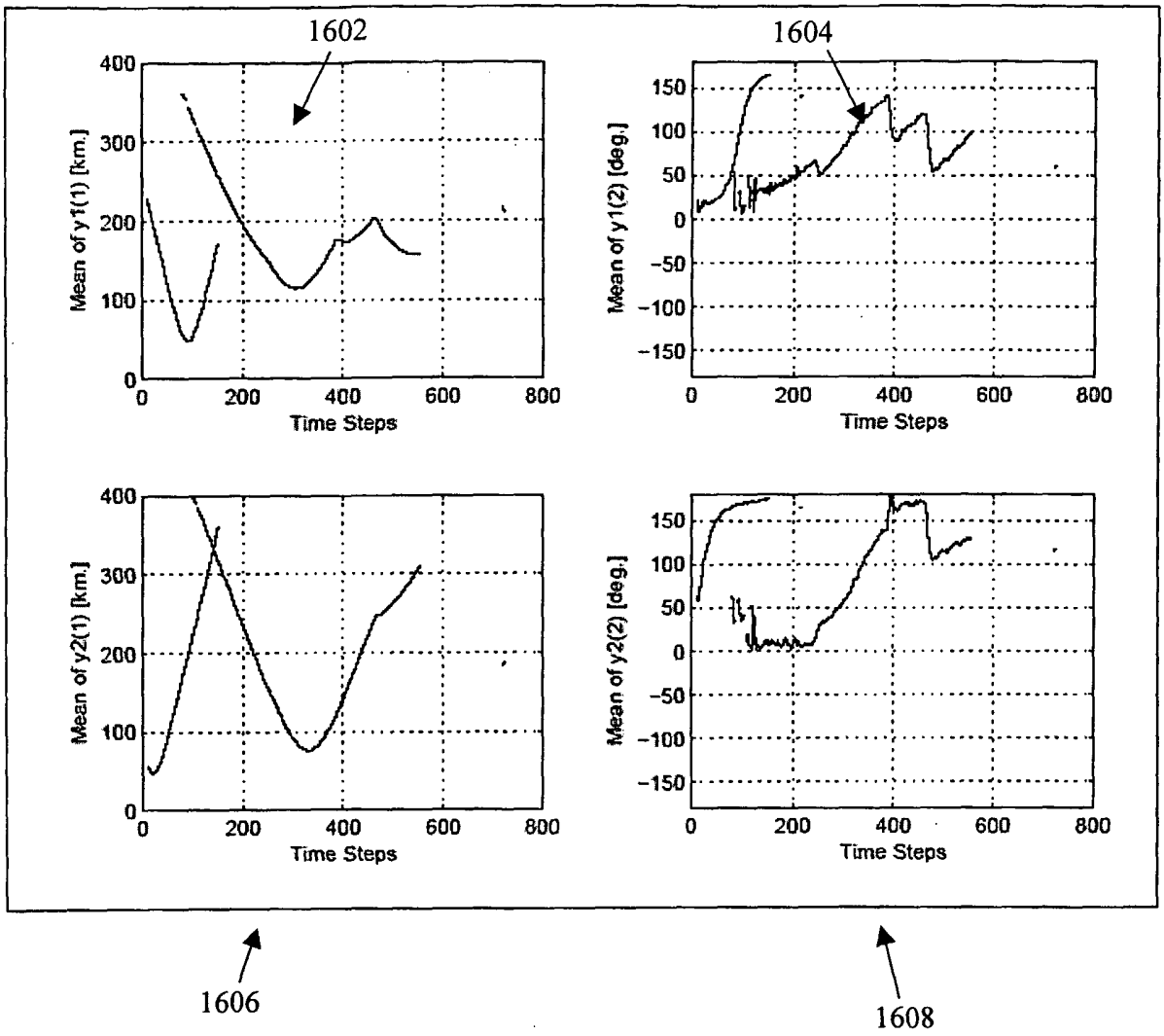

1602
1604
Mean of y1(1) [km.]
Mean of y1(2) [deg.]
Mean of y2(1) [km.]
Mean of y2(2) [deg.]
Time Steps
1606
1608

Figure 16

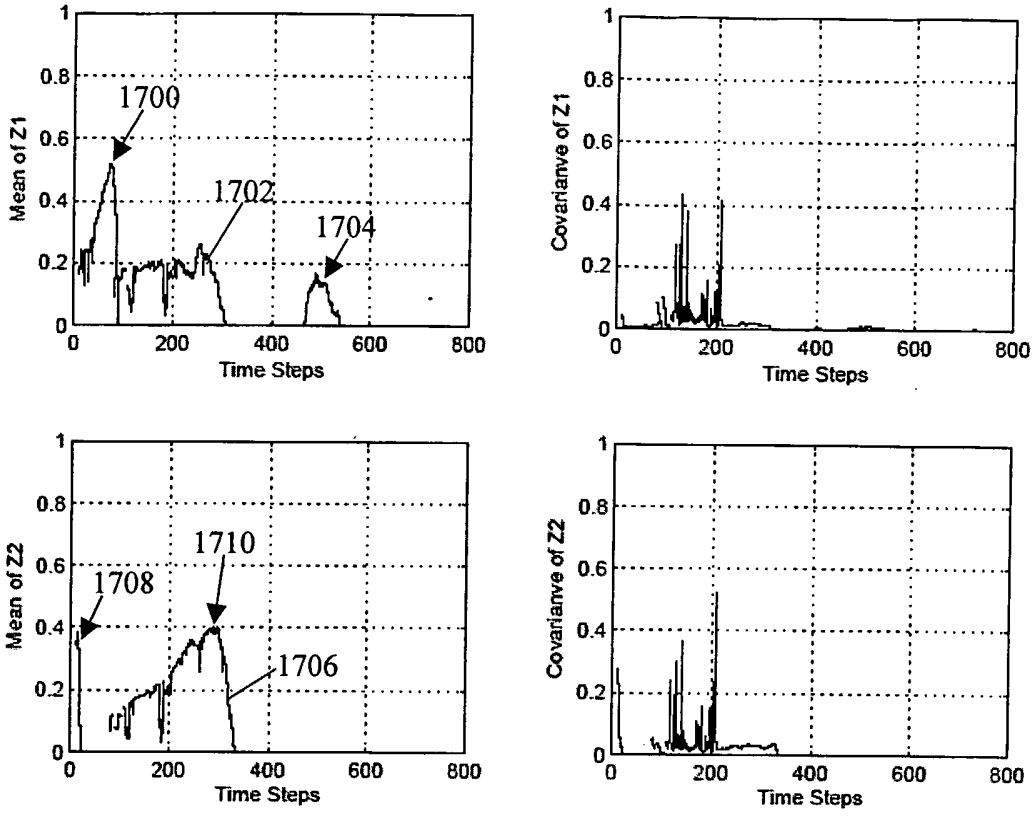

Mean of Z1
1700
1702
1704
Time Steps
Covarianve of Z1
Time Steps
Mean of Z2
1708
1710
1706
Time Steps
Covarianve of Z2
Time Steps

Figure 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2005/000857

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 17/00, G06N 5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DWPI, USPTO, PCT, IEEE, Google Scholar (belief, Dempster Shafer, bayesian network, conditional, posterior, joint, threat, military, defence, aircraft, target, intruder, linear, nonlinear, etc.)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	X. T. Nguyen, *Threat Assessment in Tactical Airborne Environments* Proc. 5th International Conference on Information Fusion, pp. 1300-7, July 2002	5-11, 22-37, 46-47
A	X. T. Nguyen, *Target Mission Estimation*, Proc. 3rd International Conference on Knowledge-Based Intelligent Information Engineering Systems, pp. 66-9, September 1999	1-47
A	D. M. Buede et al, *A Target Identification Comparison of Bayesian and Dempster-Shafer Multisensor Fusion*, IEEE Transactions on Systems, Man, and Cybernetics, 27(5), pp. 569-77, September 1997	1-47
A	B. R. Cobb et al, *On Transforming Belief Function Models to Probability Models* Working Paper No. 293, School of Business, University of Kansas, February 2004 http://hdl.handle.net/1808/156	1-47

☐ Further documents are listed in the continuation of Box C ☐ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 July 2005	26 JUL 2005
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**MATTHEW HOLLINGWORTH** Telephone No : (02) 6283 2024

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2005/000857

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a)

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See extra sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2005/000857

Supplemental Box
(To be used when the space in any of Boxes I to VIII is not sufficient)

Continuation of Box No: III

The international application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to from a single general inventive concept. In coming to this conclusion the International Searching Authority has found that there are two inventions:

1. Claims 1-4, 12-21 and 38-47. The generation of conditional probabilities of non-linear causal relationships is considered to be a first "special technical feature."
2. Claims 5-11, 22-37. The use of both intent and capability values is a second "special technical feature."

Since the abovementioned groups of claims do not share any technical features, a "technical relationship" between the inventions, as defined in PCT rule 13.2 does not exist. Accordingly, the international application does not relate to one invention or to a single inventive concept.

However, both inventions are easily covered by a single search, and an additional search fee is not warranted.