Assessment of Data Fusion Systems Part 2: Sensor Network Architectures

Chung Huat Tan, Hai'an Chen, Gee Wah Ng
Information Exploitation Programme
DSO National Laboratories
20, Science Park Drive, Singapore 118230
{tchunghu, chaian, ngeewah}@dso.org.sg

Abstract – In the previous paper, we described an assessment methodology that provides us with a more well-rounded interpretation of data fusion (DF) system performance based on complexities of the ground truth and sensor reports. The methodology in that paper yields a more accurate performance indication of a data fusion system as compared to a methodology based solely on output performance. However, we still need to incorporate other significant input factors to further address the complexity of scenarios in order to fortify our assessment methodology. A key area that was not incorporated in our previous paper is communications among nodes within a sensor network. Communications are integral to the functioning of a sensor network DF system and can drastically affect the quality of its outputs, especially in harsh hostile environments. In this paper, an additional series of complexity metrics is incorporated with regards to the architectures and communication factors of data fusing sensor networks. These metrics are incorporated with the metrics in the previous paper to obtain an improved assessment index of the fusion system performance.

Keywords: performance evaluation, data fusion, network architecture, communications, tracking, assessment.

1 Introduction

This paper is an augmentation to our initial paper on "Assessment of Data Fusion Systems" [1], in which a number of complexity metrics were designed to measure the ground truth aspect of the input scenario. Several performance metrics were also defined to assess the fusion system solution. In this paper, we investigate the various communication factors in a sensor network that affect the complexity of the input scenario. This allows us to obtain a more accurate measure of the scenario's difficulty. The complexity metrics presented in this paper attempts to estimate the difficulty of the input scenario in terms of the networking and communication aspect. The performance metrics judge the quality of the global track picture produced by the DF system. Sections 4 and 5 discuss these metrics in greater detail. We conclude this paper in Sections 6 and 7 with the application of the evaluation tool on a few computer simulated test scenarios and an explanation of the results obtained.

2 Architecture of Sensor Network

Akin to ground truth complexities discussed in the previous paper, the complexities of sensor network architecture as well as network operating conditions of the input scenario can have a significant influence on the overall performance of a data fusion system. With the intention of achieving a more robust assessment index when evaluating a data fusion system, it is essential for us to take these complexities into consideration. In this paper, we investigate the networking and communication factors of sensor networks, focusing on two major classes (centralized and decentralized) of architecture and discover how these complexities affect the quality of outputs produced by a fusion system.

2.1 Centralized Network

A centralized sensor network with all messages flowing inward to some central processor is essentially a star configuration with links radiating from a single central node. It is the simplest form of network topology and requires a link to be dedicated between the central node and each sensor node. Communication usually takes place across a shared channel in a centralized network.

In a centralized sensor network, no decision making or data fusion takes place locally at each sensor node. All observational data are sent from the sensors to the central node for processing. This translates to high bandwidth usage and communication costs. Secondly, since communication is only possible from each sensor to the central node, any transmission barrier in between them would mean that the affected sensor's observations would never reach the central node. This can significantly affect the effectiveness and accuracy of the data fusion process. The centralized network architecture therefore lacks reliability and is inflexible to network changes.

2.2 Decentralized Network

A decentralized sensor network has no central node. Fusion occurs locally at each node. Communications in a decentralized network is strictly node-to-node and among adjacent nodes only.

Unlike in a centralized network, there are no fixed communication paths in a decentralized network. Consequently, the network is flexible and tolerant to

dynamic changes in the network, such as the addition or loss of sensing nodes. This architecture improves the connectivity and reliability of the network by balancing the workload among nodes, providing multiple connections between nodes and removing single points of failure.

3 Assessment Methodology

The basis of comparison for all new metrics introduced in this paper remains unchanged from [1]. A common standard for scoring each metric is employed. For every metric that is considered, a score between 0 and 1 is assigned for normalization purposes. As such, no individual factor is favoured over the others. Comprising of two indexes, the proposed measure of evaluation provides a clear indication of the DF system performance. A smaller index indicates better DF system performance.

$$\text{quantity assessment index} = \frac{\text{quantity performance metric}}{\text{quantity complexity metric}} \quad (1)$$

$$\text{quality assessment index} = \frac{\text{quality performance metric}}{\text{quality complexity metric}}$$

Quantity assessment index quantify the capability of the DF system by considering the number of communication nodes, central nodes and communication paths throughout the entire scenario run-time. Quality assessment index relates the accuracy and precision of the reconstructed tracks to the complexity of the network architecture as well as other communication factors. The components of the main metrics are summarized in Table 1.

Main metrics	**Sub metrics**
Quantity complexity metric	No. of nodes + No. of communication paths
Quality complexity metric	Error level + Delay level + Information Loss + Information Discontinuity
Quantity performance metric	No. of false alarms + No. of missing tracks
Quality performance metric	Correlation accuracy + Individual track quality

Table 1: Summary of metrics

Together, the quantity assessment index and quality assessment index constitute the overall assessment results of a DF system. They describe distinctly different aspects of the DF system performance. With a large (poor) quantity assessment index and a small quality assessment index, we can conclude that, the output track picture has missing tracks and probably contains erroneous tracks that do not exist in the input scenario. However, the reconstructed tracks that exist in the input scenario accurately mirror the actual target paths. On the other hand, a small quantity assessment index and large quality assessment index implies that the output track picture contains an accurate number of tracks which differs significantly from the actual target paths.

4 Complexity Assessment

A data fusion system evaluated based on only its output performance effectively misses out the other half of the picture. When assessing the performance of a data fusion system, it is important to take the complexity of the scenario into consideration. In our previous paper, we have taken the complexities of ground truth into consideration. In this paper, we are incorporating complexities of the network communication factors to strengthen our assessment methodology.

4.1 Quantity Complexity

4.1.1 Number of Communication Nodes

The number of communication nodes in a sensor network affects the performance of the data fusion system in more ways than one. In the previous paper, we have seen that a large number of platforms translate to an increased difficulty in the scenario since the DF system will have to distinguish targets from many friendly platforms. On the other hand, with more sensor nodes, a better coverage can be achieved by reducing the target-platform separations. In our current context, an increased number of communication nodes contribute to a higher level of complexity in the input scenario since communication nodes in the network would have to deal with a greater amount of incoming data, primarily target updates. The overall communication process also becomes more complicated.

4.1.2 Number of Communication Paths

This metric measures the number of communication paths in the sensor network. Similar to the number of nodes, the number of communication paths in a sensor network also increases the difficulty of the scenario since the complexity of routing and inter-node communications increases with the number of communication paths in the network. In a centralized network, the number of communication paths is equivalent to the number of platform nodes since there is one path per platform node to the central node.

In a decentralized network, the number of communication paths is dynamic. Therefore, the average number of communication paths throughout the entire scenario runtime is computed for this metric. Any two nodes coming together within a user-specified distance threshold, the “neighbour node distance threshold”, are considered as neighbouring nodes.

4.2 Quality Complexity

The levels of error, delay, information loss, and information discontinuity in a sensor network can characterize its network performance. These four factors are used collectively to determine the quality complexity of the input scenario with regards to network architecture and communication factors.

4.2.1 Error Level Metric

Interference in communications introduces errors to data transmitted over a sensor network. The error level here measures only undetected errors introduced to the data fusion process. In other words, erroneous reports that are detected and removed before they are even used in the

data fusion process are excluded. An undetected error used in the fusion process will lead to inaccuracies in the output of the fusion system. Information loss due to detected erroneous reports will be discussed in 4.2.3. These erroneous reports are deleted even before fusion. The error level metric (2) encompasses two sub metrics which measures the error level due to two main sources of interference: terrain features and jamming devices. The greater this metric is, the higher the complexity.

$$\text{error level metric} = (\text{terrain interference metric} + \text{jammer interference metric})(1 - P_d) \quad (2)$$

where Pd is the probability that an error is detected. Errors arising due to multi-user interference are assumed to be negligible since collision detections are taken care by most protocols used in sensor networks. On the other hand, contention delays due to attempts to transmit concurrently must be considered. This aspect will be discussed in section 4.2.2.1 where the delay level metric is introduced.

4.2.1.1 Terrain Features

Terrain and environmental characteristics are major sources of interference. For example, multi-path reflections and electromagnetic masking interferes with data transmission in urban terrain, introducing errors to the data received at the destination node. The drop in the power of a transmission as it travels through a complex terrain renders the signal more interference-prone. A simple and commonly used model for calculation of the received power at a distance d from the transmitter is as follows.

$$P_R = P_T \frac{K}{d^n} \quad (3)$$

where K is a constant, P_T is the transmission power and n is a constant depending on the kind of terrain between the two transceivers. For open-air transmission, n is approximately 2, while for heavier terrain, n is close to 4. Based on this model, we calculate the inter-node score for a node pair, (i,j) at a time instance t as follows.

$$\text{inter node score}_{i,j}(t) = \begin{cases} 0 & \text{if } r \le 2 \\ 1 & \text{if } r \ge 4 \\ \dfrac{\text{dist}_{i,j}(t)^r - \text{dist}_{i,j}(t)^2}{\text{dist}_{i,j}(t)^4 - \text{dist}_{i,j}(t)^2} & \text{if } 2 < r < 4 \end{cases} \quad (4)$$

where $\text{dist}_{i,j}(t)$ is the distance between node i and node j at time instance t and r is the terrain constant that characterizes the type of terrain in the scenario. When r is lesser or equals to 2, a node pair gets a score of 0. When r is greater or equals than 4, a score of 1 is given. The node pair terrain interference metric (5) for a node pair, (i,j) is then computed by taking the average of all inter node scores from all time instances over the entire runtime of the scenario.

$$\text{node pair terrain intf. metric}_{i,j} = \frac{\sum_{t \in \text{samples}} \text{inter node score}_{i,j}(t)}{n} \quad (5)$$

where n is the number of time instances. The final terrain interference metric (6) is calculated by summing up the node pair terrain interference metrics for all node pairs.

$$\forall i, j \in \text{nodes}, (i,j) = (j,i) \wedge i \neq j,$$
$$\text{terrain intf. metric} = \frac{\sum \text{node pair terrain intf. metric}_{i,j}}{N_p} \times N_k \quad (6)$$

where N_p is the number of node pairs and N_k is the number of platforms. N_k is used for normalization.

4.2.1.2 Jamming Device

The presence of one or more jamming devices in the environment where the sensor network operates can cause serious interference to data transmission in the region. Since such interference is intentional, they are likely to bring about intense disturbance to the normal operations of the network and therefore must be considered when measuring the complexity of the input scenario.

The interference caused by a jamming device to a node is assumed to vary inversely with the distance between them since the power of jamming signals degrades with distance. As with the previous metric, the scenario is again sampled at fixed time intervals. At each sampling instance, we calculate the distance between a node, i and each jamming device. The node jammer score for a node i and a jamming device k at time instance t is given below in (7).

$$\text{node jammer score}_{i,k}(t) = \begin{cases} 0 & \text{if } \text{dist}_{i,k}(t) \ge r \\ \left(1 - \dfrac{\text{dist}_{i,k}(t)}{r}\right) f_i & \text{if } \text{dist}_{i,k}(t) < r \end{cases} \quad (7)$$

where r is the maximum effective range of the jamming device and f_i is the transmission frequency of node i. At a time instance t, if the distance between a node i and a jammer k is greater or equal to r, a score of 0 is given to the node pair. If this distance is lesser than r, a score between 0 and 1 is computed based on the distance between them and the transmission frequency of node i. The node pair jammer interference metric (8) takes the average of all node jammer scores for all time instances throughout the entire duration of the scenario.

$$\text{node pair jammer intf. metric}_{i,k} = \frac{\sum_{t \in \text{samples}} \text{inter node score}_{i,k}(t)}{n} \quad (8)$$

where n is the number of time instances. The jammer interference metric (9) is then calculated by adding up all the node pair jammer interference metrics for all node-jammer pairs.

$$\forall (i,k), i \in \text{nodes}, k \in \text{jammers},$$
$$\text{jammer intf. metric} = \frac{\sum \text{node pair jammer intf. metric}_{i,k}}{N_p} \times N_d \quad (9)$$

where N_p is the total number of node-jammer pairs and N_d is the number of platforms in the scenario.

4.2.2 Delay Level Metric

The amount of delays in communicating information across sensor networks has a great effect on the performance of a data fusion system, especially in situations where real-time monitoring is critical. Data received with substantial delays simply become too outdated to be of any use. Delays in the arrival of data from critical sensors also result in a reduced precision in the real-time data fusion results. Therefore, it is necessary

to consider transmission delays in the network as one of the many determinants of a scenario's complexity.

The delay level metric aims to measure the amount of delays involved in data transmissions across the entire sensor network. As with all other metrics, it does not attempt to measure the exact amount of delay in terms of any unit of time. Instead, its objective is to generate a score (based on simple parameters of the sensor network) such that a higher score indicates a higher delay, and thus, a greater complexity of the scenario.

4.2.2.1 Contention Delay

Contention occurs when two or more nodes within a certain range attempt to transmit at the same time over a shared channel. Nodes that are close to other nodes are subjected to a higher level of contention delay. Besides the inter-node distance, the transmission frequency of each node is another important parameter for estimating the delay level due to contention. The transmission frequency refers to the probability that a node attempts to transmit at any one time. The average simultaneous-transmission-attempt frequency of 2 nodes is given by $f_{i,j}$.

$$\begin{aligned} \text{minimum overlap}_{i,j} &= \begin{cases} (f_i + f_j) - 1 & \text{if } (f_i + f_j) > 1 \\ 0 & \text{if } (f_i + f_j) \le 1 \end{cases} \\ \text{maximum overlap}_{i,j} &= \min(f_i, f_j) \\ f_{i,j} &= \frac{1}{2}\left[\text{minimum overlap}_{i,j} + \text{maximum overlap}_{i,j}\right] \end{aligned} \quad (10)$$

where $f_{i,}$ and f_j are the transmission frequencies of node i and node j respectively. If f_i is 0.5, the probability of node i attempting to transmit at any one time is 0.5. Minimum overlap represents the minimum amount of time for which node i and j attempt to transmit together. For example, when $f_{i,}$ is 0.5 and f_j is 0.6, the minimum overlap for these two nodes is 0.1. Conversely, the maximum overlap for two nodes represents the maximum amount of time for which the two nodes attempt to transmit concurrently. The smaller transmission frequency out of the two nodes is taken.

The average frequency of two nodes attempting to transmit simultaneously is computed by taking the average of their minimum and maximum overlap times. This represents the mid-point of the best and worst case scenario. An inter-node distance threshold, r, is also specified. This threshold represents the minimum distance between a pair of nodes such that their communication signals are too weak to be considered as interference, and hence does not cause contention delay.

Any inter-node distance that falls on or above this threshold is given a score of 0. The least possible inter-node distance of 0m is given a score of 1 which is the maximum score. The inter-node score between two nodes i and j at a given time t is given below in (11).

$$\text{inter node score}_{i,j}(t) = \begin{cases} 0 & \text{if } \text{dist}_{i,j}(t) \ge r \\ \left(1 - \frac{\text{dist}_{i,j}(t)}{r}\right) f_{i,j} & \text{if } \text{dist}_{i,j}(t) < r \end{cases} \quad (11)$$

where r is the inter-node distance threshold and $\text{dist}_{i,j}(t)$ is the distance between targets i and j at a given time t. The node-pair contention metric (12) can now be computed for a pair of nodes (i,j) by taking the average of the inter node scores obtained from each sampling instant. This metric quantifies the level of contention between a pair of nodes over the entire scenario run-time.

$$\text{node pair contention metric}_{i,j} = \frac{\sum_{t \in \text{ samples}} \text{inter node score}_{i,j}(t)}{n} \quad (12)$$

where n is the number of time instances. Finally, taking the average of all node-pair contention metrics and multiplying the result by the total number of nodes gives us the node contention metric in (13).

$$\begin{aligned} &\forall\, i, j \in \text{nodes}, (i, j) = (j, i) \wedge i \ne j, \\ &\text{node contention metric} = \frac{\sum \text{node pair contention metric}_{i,j}}{N_p} N_k \end{aligned} \quad (13)$$

where N_p and N_k are the total number of node pairs and nodes in the scenario respectively.

4.2.2.2 Propapagation Delay

Propagation delay refers to the amount of time it takes for a signal to be transmitted across the communication medium from the source node to the destination node. Since propagation delay can be assumed to vary proportionately with the distance of the communication path, the straight line distance between the two nodes is an appropriate parameter we can use in computing the score for this sub metric. Two distinct models are required for the formulation of this metric since the organization of communication paths in centralized networks is essentially different from that of decentralized networks.

4.2.2.2.1 Centralized Network

In a centralized network, all communication paths extend from sensor nodes to the central node. There is no communication path between sensor nodes. The inter node score for a node and a central node is given by (14).

$$\text{inter node score}_{i,k}(t) = \begin{cases} 0 & \text{if } \text{dist}_{i,k}(t) \ge r \\ \frac{\text{dist}_{i,k}(t)}{r} f_i & \text{if } \text{dist}_{i,k}(t) < r \end{cases} \quad (14)$$

where $\text{dist}_{i,k}(t)$ is the distance between a node i and the central node k. The transmission frequency of node i is represented by f_i and r is the maximum transmission range of a node. Similarly, the node pair propagation delay metric (15) is calculated by taking the average of the inter node scores obtained from each sampling instant.

$$\text{node pair prop. delay metric}_{i,k} = \frac{\sum_{t \in \text{ samples}} \text{inter node score}_{i,k}(t)}{n} \quad (15)$$

Finally, the propagation delay metric (16) is calculated by summing up the delay metrics as shown below.

$$\begin{aligned} &\forall\, i \in \text{nodes}, \\ &\text{propagation delay metric} = \sum \text{node pair prop. delay metric}_{i,k} \end{aligned} \quad (16)$$

4.2.2.2.2 Decentralized Network

In a decentralized network, there is no central node. Nodes can communicate with each of its neighbouring

nodes. Therefore, instead of considering the distance from a node i to the central node, we need to consider the distance from a node to each of its neighbouring nodes at any one time. In (17), we calculate a score for a node pair based on the distance between them.

$$\text{inter node score}_{i,j}(t) = \begin{cases} 0 & \text{if } \text{dist}_{i,j}(t) \geq r_d \\ \frac{\text{dist}_{i,j}(t)}{r} f_i & \text{if } \text{dist}_{i,j}(t) < r_d \end{cases} \quad (17)$$

where r_d is the neighbour node distance threshold and f_i is the transmission frequency of node i. The neighbour node distance threshold represents the maximum distance between two nodes to consider them as neighbouring nodes. If the distance between two nodes falls below this threshold, the node pair is given a score of 0. The node pair propagation delay metric (18) is calculated by taking the average of the inter node scores obtained from each time instances.

$$\text{node pair prop. delay metric}_{i,j} = \frac{\sum_{t \in \text{samples}} \text{inter node score}_{i,j}(t)}{n} \quad (18)$$

Finally, the propagation delay metric is computed as shown in (19).

$$\forall i, j \in \text{nodes}, (i,j) = (j,i) \wedge i \neq j,$$
$$\text{propagation delay metric} = \frac{\sum \text{node pair prop. delay metric}_{i,j}}{N_p} N_k \quad (19)$$

4.2.2.3 Traffic Volume

The traffic volume is one of the most important network factors for determining the difficulty of a scenario for it has significant implications on the delay level. It is therefore elemental in the formulation of our input complexity metrics. The quantity of data sent by all nodes on the sensors network determines the traffic volume. At time instance t, the node score for a node i is given by (20).

$$\text{node score}_i(t) = \frac{\text{data\_size}_i(t)}{r} \quad (20)$$

where r is the maximum sensor report size and $\text{data\_size}_i(t)$ is the data size of the sensor report sent by node i at time instance t. The node traffic volume metric (21) gives the average node score for a node over the entire runtime of the scenario.

$$\text{node traffic volume metric}_i = \frac{\sum_{t \in \text{samples}} \text{node score}_i(t)}{n} \quad (21)$$

The final traffic volume metric (22) sums up the node traffic volume metrics for all nodes.

$$\text{traffic volume metric} = \sum_{i \in \text{nodes}} \text{node traffic volume metric}_i \quad (22)$$

4.2.2.4 Buffers/Processors Delay

The typical sensor network contains a large number of sensors, usually limited in buffer space as well as computing power. As a result, delays in the transmission of data due to inadequacy of such resources are likely to occur. Any substantial delay incurred at the buffers or processors implies that the report, when eventually received, will be outdated. Consequently, the number of buffers and computing power available to communication nodes in a sensor network are important factors that determine the complexity of the scenario. With a small number of buffers or a slow processor, a node will inevitably cause delays in the flow of data across the network. This metric is computed using the number of buffers and processing power of each node in the sensor network.

$$\text{processingdelayscore} = \frac{\sum_{i \in \text{nodes}} (1 - \frac{nb_i}{\text{maxnb}}) + \sum_{i \in \text{nodes}} (1 - \frac{pp_i}{\text{maxpp}})}{2} \quad (23)$$

where nb_i is the number of buffers on node i and pp_i is the processing power of node i. The chip rate is a suitable measurement for processing power. maxnb and maxpp are constants, denoting the maximum number of buffers and the maximum processing power respectively.

4.2.3 Information Loss Metric

The third sub metric for the measurement of quality complexity is concerned about the loss of data when data is transmitted over the sensor network. Specifically, data loss here refers to data sent from a sensor node but never used in the data fusion process. We will consider three main situations when this is likely to occur.

4.2.3.1 Congestion

Congestion is a very realistic concern in sensor networks since such networks typically use radio communications over a shared communication channel. Congestion occurs when an increase in data transmissions results in a proportionately smaller increase, or even a reduction, in throughput. Congestion here, results from sensor nodes sending more data than the network can accommodate, thus causing the buffers on such devices to overflow. In wireless sensor networks, congestion causes overall channel quality to degrade and loss rates to rise. The congestion score (24) of a node is calculated using the amount of data sent over the communication link and the bandwidth of the link.

$$\text{congestion score}(t) = \begin{cases} 0 & \text{if data size}_i(t) \leq r \\ 1 - \frac{r}{\sum_{i \in \text{nodes}} (\text{data size}_i(t))} & \text{if data size}_i(t) > r \end{cases} \quad (24)$$

where r is the bandwidth of the communication channel and $\text{data size}_i(t)$ is the data size of the sensor report sent by node i. If the total data size of all sensor reports at a time instance does not exceed the bandwidth of the communication channel, there is little risk of congestion and therefore a score of 0 is specified. The final congestion metric is computed as shown in (25) below.

$$\text{congestion metric} = \frac{\sum_{t \in \text{samples}} \text{congestion score}(t)}{n} N_k \quad (25)$$

where n is the number of time instances and N_k is the number of nodes.

4.2.3.2 Detected Interference

This metric aims to measure the information loss level caused by the intentional deletion of erroneous data. It is calculated in the same way as the error level metric with two exceptions. Firstly, the probability of detecting an error is used instead of the probability of not detecting an error. Secondly, the probability that the error is not correctable is added.

$$\text{detected interference metric} = (\text{terrain interference metric} + \text{jammer interference metric})\, P_d(1 - P_c) \quad (26)$$

where P_d and P_c are the probabilities that an error is detected and correctable respectively.

4.2.3.3 Nodes out of range

To estimate the level of information loss due to the receiver node moving out of communication range, we calculate an inter node score for each node pair based on the distance between them. At a time instance t, for node i and j,

$$\text{inter node score}_{i,j}(t) = \begin{cases} 0 & \text{if } \text{dist}_{i,j}(t) \le r \\ \left(1 - \dfrac{r}{\text{dist}_{i,j}(t)}\right) & \text{if } \text{dist}_{i,j}(t) > r \end{cases} \quad (27)$$

where $\text{dist}_{i,j}$ is the distance between node i and j, and r is the maximum communication range of two nodes. A node pair with a distance lesser than r will be given a score of 0. The node pair score is then computed by taking the average of inter node scores over the run-time of the scenario.

$$\text{node pair score}_{i,j} = \frac{\sum_{t \in \text{time samples}} \text{inter node score}_{i,j}(t)}{n} \quad (28)$$

where n is the number of time samples. The out of range metric for node i is calculated by taking the average of node pair scores between i and all its neighbouring nodes. In a centralized network, the central node is the only neighbouring node to each sensor node. In a decentralized network, all node pairs are taken into consideration since each node can be a neighbour node of each other node.

$$\forall i \in \text{nodes}, j \in \text{nodes} \vee j = \text{central\_node}, (i,j) = (j,i) \wedge i \neq j,$$
$$\text{out of range metric} = \frac{\sum \text{node pair score}_{i,j}}{N_p} N_k \quad (29)$$

where N_p is the number of node pairs and N_k is the total number of nodes.

4.2.4 Information Discontinuity Metric

In a sensor network where hundreds and thousands of sensors are deployed, the connections and disconnections of sensors to and from the network occur frequently due to environmental obstructions, depleted power supply and other factors. The disconnections of communication nodes in a sensor network lead to discontinuous reports of targets being tracked. This increases the complexity of data association in the data fusion process. In this metric, we aims to measure the level of discontinuous data presented to the data fusion system due to disconnections of sensor nodes in the network. Any disconnection having a duration equals or greater than the "disconnection time threshold" will be given a maximum score of 1. The inter node score for node i and j at a time instance t is defined.

$$\text{dist}_{i,j}(t) \le r \Leftrightarrow \text{connected}_{i,j}(t) \quad (30)$$

$$\text{inter node score}_{i,j}(t) = \begin{cases} 0 & \text{if connected}_{i,j}(t) \\ f_i \dfrac{1}{s} & \text{if } \neg\text{connected}_{i,j}(t) \wedge \text{dc\_time}_{i,j}(t) \le s \end{cases}$$

where r is the neighbour node distance threshold as explained in 4.2.2.2.2, f_i is the transmission frequency of node i and s is the disconnection time threshold. $\text{dc\_time}_{i,j}(t)$ is the duration of a continuous disconnection occurring through time t. Suppose s is 5 seconds and a 6-second disconnection of node i and node j occurs from time $(t+1)^{th}$ second to $(t+6)^{th}$ second, the score given for each time instance from (t+1) to (t+5) is 1/s. Therefore a total score of 1 is given for the entire disconnection of 6 seconds. Over the entire duration of the scenario, the average inter-node score for a node pair is given by (31).

$$\text{node pair score}_{i,j} = \frac{\sum_{t \in \text{time samples}} \text{inter node score}_{i,j}(t)}{n} \quad (31)$$

where n is the number of time instances. The final information discontinuity metric is computed by taking the sum of all node pair scores.

$$\forall i \in \text{nodes}, j \in \text{nodes} \vee j = \text{central\_node}, (i,j) = (j,i) \wedge i \neq j,$$
$$\text{information discontinuity metric} = \frac{\sum \text{node pair score}_{i,j}}{N_p} N_k \quad (32)$$

where N_p is the number of node pairs and N_k is the total number of nodes.

5 Performance Assessment

In contrast to complexity assessment which determines the difficulty of the input scenario, performance assessment is concerned with the quality of the output track picture. The methodology for performance assessment follows that of the previous paper in which quantity performance and quality performance formed the two main parts of it. Quality performance describes the quality of the global track picture in terms of the number of reconstructed tracks without taking the integrity of the tracks into account. Accuracy of the reconstructed tracks is then measured by the quality performance metric.

As illustrated in the previous paper, the quantity performance metric is computed using the global track picture metric while the quality performance metric comprises of the correlation accuracy metric and the track quality metric.

6 Test Scenarios and Results

Having extended the set of complexity metrics to incorporate networking and communication factors, tests were carried out to assess the evaluation tool. These tests were carried out with the use of a scenario generator which models the movements of platforms, targets and jamming devices. All thresholds relating to the previous paper are set to their default values and kept constant for all test cases described below.

To test the effectiveness of the improved DF system evaluation tool, the networking and communication-related conditions which impact the performance of the

fusion system are identified. These conditions and their respective impacts on DF system performance are listed in Table 2. Scenarios testing each condition are then generated and assessed by the evaluation tool. Finally, the results are compared to those of the default scenario to ascertain if the conclusions match our hypotheses.

Conditions to vary for analysis	**Expected impact on data fusion performance**
User-defined Inputs	Decreased performance with stringent thresholds.
Number of Nodes	Decreased performance with increased amount of communication overheads.
Error and Delay Levels	Decreased performance with increased error and delay levels.
Information Loss and Discontinuity Levels	Decreased performance due to increased information loss and discontinuity levels.

Table 2: Conditions affecting DF system performance and the corresponding expected impacts.

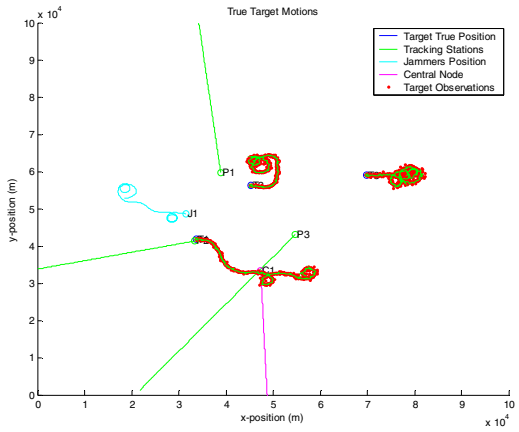

Figure 1: Scenario A (default) and B testing the effects of stricter thresholds.

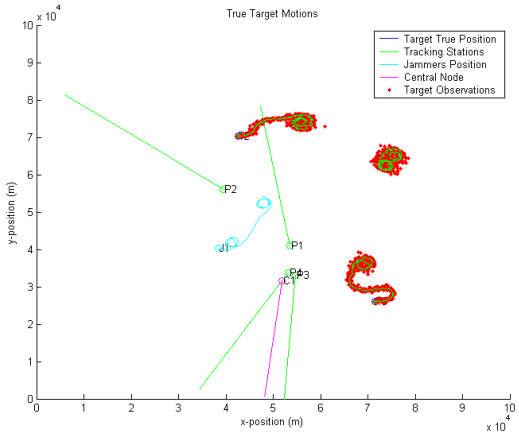

Figure 2: Scenario C (increased number of platforms)

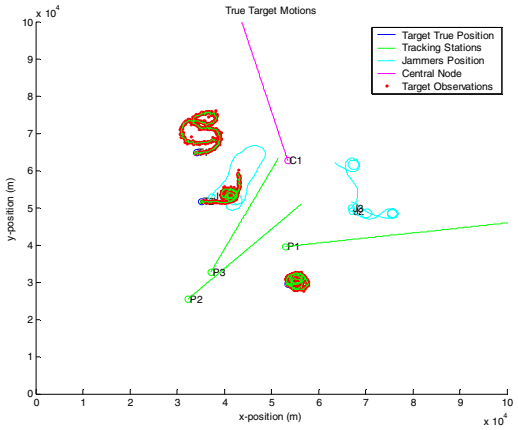

Figure 3: Scenario D (errors and delays introduced)

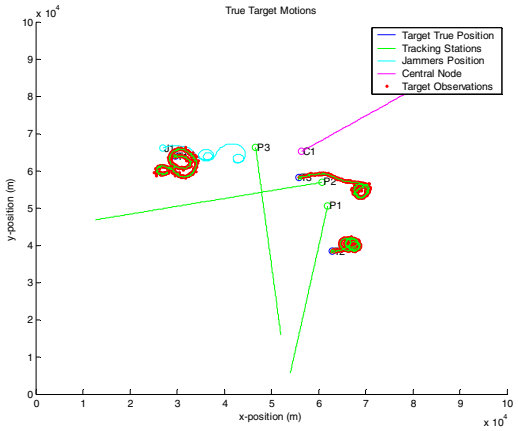

Figure 4: Scenario E (information loss and discontinuity introduced)

Figure 1 depicts the computer-generated scenario A with 3 platforms (P1, P2 and P3), 3 targets (T1, T2, and T3), 1 central node (C1) and 1 jamming device (J1). Scenario A serves as the default scenario and is the basis of comparison with other scenarios. To determine the impact of the conditions discussed in table 2, scenarios B, C, D and E were generated. They are depicted in Figures 1, 2, 3 and 4 respectively. Scenario A and scenario B are tested on the same input scenario with different thresholds used when computing the complexity metrics for the latter. Table 3 summarizes the various scenario settings and their corresponding evaluation results.

Scenario	A	B	C	D	E
No. of nodes	3	3	4	3	3
Average platform separation (m)	30000	30000	30000	30000	50000
Maximum jammer range (m)	10000	30000	10000	10000	10000
No. of jammers	1	1	1	3	1
Terrain type constant (2 – 4)	2	2	2	4	2
Contention distance threshold (m)	20000	30000	20000	20000	20000
Neighbour node distance threshold (m)	20000	40000	20000	20000	20000
Disconnection time threshold (s)	100	25	100	100	100
Max transmission range (m)	90000	90000	90000	90000	40000
Avg transmission frequency	0.3	0.3	0.3	0.7	0.3
Avg data size (KB)	300	300	300	300	600
Avg no of buffers	10	10	10	5	10
Avg chip rate	100	100	100	50	100

Centralized Network					
Quantity assessment index	0.1667	0.1667	0.1333	0.1667	0.1667
Quality assessment index	0.4069	0.3681	0.3984	0.1593	0.2030
Decentralized Network					
Quantity assessment index	0.2222	0.2000	0.1667	0.2000	0.1818
Quality assessment index	0.4482	0.3902	0.4276	0.1812	0.2230

Table 3: Table of scenario settings and evaluation results.

Scenario A is first evaluated using the settings as defined in Table 3. We obtained a quantity assessment index of 0.1538 and a quality assessment index of 0.4069 for the centralized network. 0.2222 and 0.4482 were obtained for the respective indexes of the decentralized network. To determine the impact of user-defined settings, Scenario B is evaluated using stricter thresholds. With a lesser tolerance for errors and other negative effects, a poorer global track picture is expected. Since the scenario generator produces the same global track picture, the quality assessment index of Scenario B would be smaller since the complexity of the scenario was increased. This is clearly evident from the quality assessment indexes of 0.3681 and 0.3902 obtained for the centralized and decentralized network respectively.

As shown in Figure 2, Scenario C has four platform nodes instead of three in all other scenarios. The increased number of platforms contributes to a higher level of traffic volume, propagation delay and other effects, leading to a higher complexity in the scenario. The quality assessment indexes of 0.3984 and 0.4276 compared with 0.4069 and 0.4482 confirm this hypothesis.

Scenario D was generated to gauge the effect of introducing errors and delay effects to the sensor network. This was achieved by setting a higher terrain complexity, increasing the number of jammers, reducing the number of buffers and processing speed of communication nodes and raising the transmission frequencies of these nodes. We obtained lower quality assessment indexes of 0.1593 and 0.1812 which correctly indicate a higher complexity in the input scenario.

Finally, scenario E draws attention to the effects of information loss and discontinuity on the performance of the data fusion system by increasing the average platform separation, decreasing the maximum transmission range and increasing the average data size of sensor reports. The assessment indexes calculated match our hypotheses and provide a good estimate of the performance for DF systems.

7 Conclusion and Future Work

From tests conducted above, we have demonstrated that the proposed extended method of evaluating DF systems enables us to achieve an improved measure of the effectiveness of a DF system in the light of the scenario complexity. This allows us to factor in networking and communication parameters of varying complexity as inputs to a particular fusion system. Besides being able to interpret the assessment metrics in relation to each other, particular deficiencies can also be identified to optimize system performance. Without considering the complexity of the scenarios, estimation of the true performance level for any given scenario would be difficult and assessment indexes of these scenarios could not be compared readily.

The assessment methodology described in this paper is a proposed approach to obtain a better estimate of the performance for a data fusion system with respect to the complexity of the sensor network as well as other communication factors. All sub metrics used for computing the quantity and quality complexity are weighted equally. Future work can make use of real sensor network data to determine the weight of each sub metric according to their impact on the data fusion performance or specific user/operational requirements.

8 References

[1] G. W. Ng, C. H. Tan, T. P Ng, and S. Y. Siow, *Assessment of Data Fusion Systems*, Proc. of the 9th International Conference of Information Fusion – Fusion 2006, 10-13 Jul 2006.

[2] H. Durrant-Whyte, R. Deaves, and P. Greenway, *Decentralised Multi-platform Data Fusion*, SPIE Conference on Digitization of the Battlespace III, vol. 3393, pp. 63-71, April 1998.

[3] D. Nicholson and R. Deaves, *Dencentralized Track Fusion in Dynamic Networks*, Signal and Data Processing of Small Targets 2000, pp. 452-459, 2000.

[4] J. L. Nemeroff, L. Garcia, D. Hampel, and S. Di Pierro, *Networked Sensor Communications for the Objective Force*, In R. Suresh and W. E. Roper, editors, Proc. SPIE Vol. 4741, pages 29--35, Aug. 2002.

[5] S. Utete and H. Durrant-Whyte, *Reliability in Decentralised Data Fusion Networks*, Proc. 1994 IEEE International Conf. on Multisensor Fusion and Integration for Intelligent Systems, pp. 215-221, Oct1994.

[6] E. Nettleton, H. Durrant-Whyte, and S. Sukkarieh, *A Robust Architecture for Decentralised Data Fusion*, In Proceedings of the International Conference on Advanced. Robotics (ICAR), 2003.

[7] H. Durrant-Whyte, M. Stevens and E. Nettleton, *Data Fusion in Decentralised Sensing Networks*, Proc. of the 4th International Conference on Information Fusion, Montreal, Canada, 2001, pp. 302-307.

[8] S. Rawat, *A Frame Work For Performance Evaluation Of Multi Target Tracking Systems*, Final Technical Report for AFOSR and AFFTC, Aug 2002.

[9] O.E. Drummond, *Methodologies For Performance Evaluation Of Multiple Target Multi Sensor Tracking*, Proc. SPIE, vol. 3908, pp. 355-369, 1999.

[10] M.O. Hofmann, and S.M. Jameson, *Complexity and Performance Assessment for Data Fusion Systems*, Proc. IRIS National Symposium on Sensor and DF, Mar 1998.