MODELING THE DECISION QUALITY IN SENSOR-TO-SHOOTER (STS) NETWORKS FOR UNATTENDED GROUND SENSOR CLUSTERS

(Research-in-Progress)

Patrick J. Driscoll
U.S. Military Academy, West Point, USA
pat-driscoll@usma.edu

Edward Pohl
U.S. Military Academy, West Point, USA
rwang@mit.edu

Abstract: One of the most promising concepts being considered for use by the Objective Force of the U.S. Army is an automated Sensor-to-Shooter (STS) network. An STS network is a closed-loop, internal feedback system that links various suites of sensors deployed throughout a 3D battle space to a network of weapons platforms (shooters) using optimized communications pathways. The system decision to fire or not is based exclusively on the information generated by this network. Hence, the quality of this decision process is directly dependent upon the quality of the information used to support it. In this paper, we introduce a novel sensitivity analysis framework capable of assessing the marginal contributions to uncertainty made by the various processes and devices of an STS network. This approach extends earlier work in modeling data and process quality for multi-input, multi-output information systems that principally focused on reducing error rates. While this study represents a work-in-progress, we are optimistic that the results can be directly used to identify an information quality critical path defined as an end-to-end pathway through the STS network composed of those devices and processes whose marginal rate perturbations most affect the quality of the final information product at the decision point. Moreover, a simple ranking of these marginal rates can identify and prioritize locations in the network where effective information quality enhancements should be performed to maintain a high quality final information product. This approach will also provide valuable insights as to whether or not continued efforts to improve sensor device precision beyond current levels is warranted.

Key Words: Decision Quality, Information Quality, TDQM, Information Product, Sensor network, Sensitivity analysis.

INTRODUCTION

Successfully transforming the U.S. Army into an Objective Force for the 21st Century requires new ways of thinking about the resources at the Army's disposal to create such a force: time, manpower and equipment. These assets must uniquely combine to not only afford future commanders a level of battlespace situational awareness far beyond that of adversaries, but to equip commanders with systems capable of near instantaneous reaction and response to enemy presence [1]. One of the most promising concepts consistent with this design philosophy is an automated Sensor-to-Shooter (STS) network. An STS network is a closed-loop, internal feedback system that links various suites of sensors deployed throughout a 3-dimensional battlespace to a network of weapons platforms (shooters) using optimized communications pathways.

A fully-automated STS network is one in which there is no required human interaction in order to achieve its principal functionality. These networks can be decomposed into three major segments: target acquisition, a fires commitment decision process, and a weapons engagement process. Targets are detected, classified and identified through the sensor end of the network. A decision support system then determines if threshold criteria for target identification has been met, and if so, makes the decision to commit the appropriate available weapons platform(s) to engage the target. Once handed this fire mission, the weapons platform would engage the target, the sensors would assess the damage, the decision support system would again compare target damage to threshold criteria, and re-engage as necessary.

Doing this successfully is both tricky business and admittedly several years away, especially when such systems are deployed in general support of operational forces. Direct support STS networks are currently in-use in Afghanistan, where special operations units of the Army use handheld laser target designators that are linked directly to U.S. Air Force fighter aircraft (shooter) rather than routing fire support requests through alternative communications routes that would be far less responsive. It is the aspect that the sensor, in this case a combination of soldier and lasing device, is pre-assigned directly to the weapons platform (shooter) prior to commencing the tactical operation that defines this arrangement as direct support. This pre-assignment of sensor to shooter avoids many of the challenges associated successful general support of operations using STS networks such as target handoff, cross-service weapons allocation, and commitment of fires within restrictive engagement time windows, among others.

This general support role for an STS network is the more difficult and vastly more important case. In this scenario, targets are not pre-designated and weapons systems are not pre-assigned to targets. These actions along with their associated decision processes unfold as the dynamics of the battlespace dictate. Thus, the general support case naturally subsumes direct support as a special case. It is the general support role that has a strong potential to dramatically reduce the cycle time for all engagements in a 3-dimensional battlespace.

Three distinct major processes characterize an STS network in this perspective: information input, processing and presentation to the fire/no fire decision point, weapons allocation and assignment once the fire decision has been made, and battle damage assessment and recommitment of fires following an initial engagement. Our focus herein is on the first process because it is this segment of the overall operational STS network that contains all of the information directly supporting the only decision point in an STS network. It appears to follow that one ought to be concerned with how “good” the information is at this point, and whether or not actions could be taken to improve the quality of this information, if such a need were present.

Information Quality

While there exists an abundance of effort focused on the technical aspects of sensor network design (see The International Society for Optical Engineering (www.spie.org), and IEEE Sensors Council (www.ewh.ieee.org/tc/sensors/) for example), there is a notable absence of effort to-date focused on examining issues associated with the quality of the information that is flowing on these networks. Harney [10] was the first to suggest that an information-based analysis applied to sensor functions might be of significant merit to both improving individual sensor design and providing insights into more viable alternative approaches. Since the fire/no fire decision in a fully automated STS network is based exclusively on this information, we concur with him.

The focus of his analyses at that time centered on information technology issues such as transmission rates and data assurance. This aspect of his effort aligned with that of Yu and Neter [21], Cushing [8], Bodnar [5], and Stratton [17] who all sought to efficiently automate error checking and validation in computer-based accounting systems. While all five of these studies employed a somewhat different concept of information quality than that of this study, Harney’s results in particular bears a certain appeal to several notions underlying our work. These are summarized in the context of the three propositions that follow.

First, he proposed the conjecture that the information gained from a single sensor in a sensor cluster has the same quality level as information obtained from another sensor. By this he meant that in terms of detection, classification and identification, all sensors had equivalent potential. Although it appears that the validity of this conjecture necessarily assumes a cluster is composed of the same type of sensor, we agree with the presumption that within sensor types there should not be a measurable difference in the quality level of information generated into a sensor network. Therefore, if one can capture some closed-form measure of the contribution of a single sensor to the decision quality associated with an STS network, it is simply a matter of scaling up this contribution to assess the overall impact of a sensor cluster of varying sizes.

Secondly, he proposed that the information obtained from multiple sensors, presumably of the same type, has the same quality level as that obtained from a single sensor in the network. The thought behind this conjecture was that if a single sensor was able to identify an enemy target with a high degree of accuracy and pass this information into the network, then having multiple sensors do the same reflects a redundancy in the information. The validity of this conjecture depends upon whether or not one considers both the technical sources of error and the error components introduced in the processes used to construct information products. Since he did not consider the costs associated with multiple sensor configurations, the notion of designing effectiveness with bang-for-buck considerations was not addressed. We do so here.

Lastly, Harney proposed that the information obtained from non-imaging sensors has the same quality level as that obtained from imaging sensors despite the attractiveness of imagery as a means of communicating information. We strongly support this conjecture, believing that a high quality information product assembled from a host of low-cost independent sensor types is equivalent to a high quality information product assembled from a single high cost sensor.

Accepting this final conjecture directly implies that by identifying such equivalences between the information products generated by different sensor types it is possible to quantify thresholds for continued investment efforts focused on improving the precision of sensors. Moreover, such investments should experience diminishing marginal returns to decision quality associated with increases in precision simply because there is a certain amount of uncertainty contained in a sensor network that cannot be engineered out of the system.

In this study, we propose a different set of three conjectures. First, the quality of the decision process is directly dependent upon the quality of the information used to support this decision process. Second, that information quality in this setting is a function of the uncertainty imposed by the various devices and processes that make up the STS network. And third, that understanding the marginal rates of contribution made by individual devices and information handling processes throughout this network will facilitate developing strategies that will enhance and maintain high quality information. In the sections that follow, we employ a simple information manufacturing framework based on that introduced by Ballou et al. [4] to conceptualize an STS network and develop our approach to quantifying this underlying uncertainty.

An Information Manufacturing Framework

In a general support role for the Objective Force units, an STS network is intended to automatically detect, classify, and identify targets in a dynamic battlespace that evolves in concert with current operations ([11], [9]). Sensors generate the lowest level of primitive data that begins this process flow. This data is then transformed, or *manufactured*, into various intermediate information products as it flows throughout the network, culminating in a final information product that is presented to the fire/no fire decision point. For example, an intermediate information product is formed when primitive sensor data is aggregated to accomplish a low level classification in a sensor cluster [12].

Viewing an STS network as an information manufacturing network is quite useful because it is generally recognized that the quality of information flowing in such networks erodes over time due to both internal and external affects when some set of information maintenance activities are not performed ([13], [2], [3]).

For most sensor networks in existence today, the need to perform maintenance actions has been driven by a concern that the hardware involved in these systems have a high quality *information technology* serving the backbone of the network. This concern resides principally in the domain of computer scientists and programmers. However, it does not follow that such actions necessarily insure high quality information, but merely guarantee that a high percentage of the information passing on this network propagates from point-to-point without interruption or excessive error generation. A new methodology appears to be needed that specifically focuses on information as an entity, and provides a means by which the quality of such information entities can be assesses and enhanced as necessary.

In concert with our conjecture that the quality of information presented to the decision point, hence the *decision quality* of an STS network, is directly dependent upon the level of uncertainty contained in the information supporting the decision, it follows that high quality information in this setting can be characterized as containing as little uncertainty as possible. As such, for any particular suite, or combination of suites, of sensors comprising the front end to the network, minimizing this amount of information uncertainty through deliberate design or post-deployment operational activities should be a major objective of any design initiative. This requires STS network designers to understand the levels of uncertainty present at critical locations in an STS network, the upper and lower bounds of this uncertainty, what these levels should be in relation to those present in existing equivalent battlefield decision processes, and the location and type of maintenance actions that should take place in an STS network to reduce the level of uncertainty and thereby maximize the decision quality. The necessary first step in this undertaking is to develop an appropriate framework within which these issues can be clearly illuminated and understood.

The major goal of this study is to develop both a framework and a methodology for assessing the decision quality at the fire/no fire decision point in STS general support networks. The approach we take to accomplishing this goal is to characterize the STS network as a stochastic *information manufacturing* network [20] in which the various processes and activities introduce elements of uncertainty that become embedded in the information products. The framework we propose explicitly represents these contributions to uncertainty and tracks their individual flow to the decision point.

This framework enables us to use a recursive method of backtracking to develop closed-form expressions for the marginal contribution to uncertainty by activities occurring at specific locations in the network, and thereby capture each critical location's role in contributing to the overall decision quality. At the same time, these marginal expressions describe a sensitivity that enables us to assess the impact of several optional activities including increased precision at any device in the network, or changes in fusion algorithms at information consolidation points, thereby being able to prescribe design guidelines with a 'bang-for-the-buck' motivation in mind. Moreover, such an approach can identify locations in the network where information maintenance operations should be performed in order to maintain a high decision quality at the critical locations noted. Additionally, we hope to be able to prescribe the goals of such maintenance activities as well and to capture the specific probability distributions associated with each critical location in the STS network, the fire/no fire decision point being one of these.

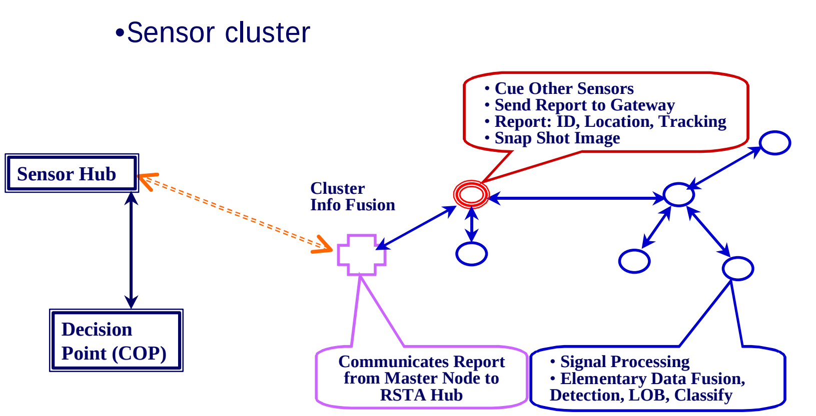

Figure 1. A generic UGS base unit cluster configuration.

UNATTENDED GROUND SENSORS

One family of sensors that can be used as the front end of an STS network is Unattended Ground micro-Sensors (UGS). These sensors are capable of delivering mission critical information in both Beyond Line of Sight (BLOS) and Non-line of Sight (NLOS) areas of the battlefield.

UGS come in various sizes and forms. Each individual sensor may contain one or more types of sensing capability (seismic, acoustic, magnetic, image, IR). UGS are small, relatively low cost to manufacture, operationally robust, and capable of performing information gathering missions on the battlefield for extended, although limited, periods of time. This operational time is driven both by the life of the on-device battery and the power requirements for various operations the sensor is asked to perform. Battery life is currently the principle factor constraining sensor communications as well.

Sensor *clusters*, comprised of three to five individual sensors (nodes) linked through efficient, low-range communications, are capable of being deployed by several means (e.g., air, artillery, and hand). Figure 1 illustrates a generic base unit cluster and the functions associated with the various system components.

Positioning several clusters within spatial proximity to each other and linking the communications pathways between these clusters together into an integrated sensor *network*, as shown in Figure 2, creates a *sensor field*. Networked sensor fields are capable of performing a host of missions (e.g., general surveillance, early warning, target acquisition, target tracking, battle damage assessment) against a wide range of targets.

UGS operate in all-weather conditions around the clock. However, terrain, weather, background noise, and time of day all affect their precision. The level of precision ultimately has an impact on the resulting accuracy of the *information* produced by an UGS sensor cluster. The performance of an UGS

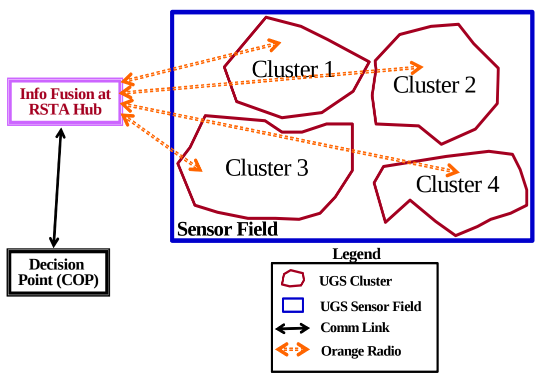

Figure 2. UGS field depiction.

sensor cluster is affected by environmental factors such as these, as well as device factors such as number, type, orientation, and reliability, among others.

UGS have the potential to not simply augment current operational capabilities, but to actually replace elements and processes in the Objective Force whose battlespace functions can be more effectively performed by UGS. In this manner, sensor technologies can change the way the Army does business, potentially change its operational art, and certainly change the way that Army forces are configured for battle. For example, some scout functions in support of target acquisition might be performed at higher precision, lower risk, and longer duration by UGS, thereby affording certain economies once appropriate tradeoff equivalences between these elements are identified.

The ultimate purpose of constructing STS networks is to facilitate rapid remote target detection, location, tracking, engagement and battle damage assessment in regions of the battlespace well beyond those that have been directly exploitable by ground force commanders. Identifying and engaging enemy forces and their resources well before they can do the same to friendly forces provides unit commanders with more complete battlespace knowledge, thereby directly enhancing both their *decision cycle*, by shortening it beyond the enemy's ability to insert disruptive measures into it, and the *decision quality* by reducing elements of uncertainty associated with accurately assessing an evolving enemy situation.

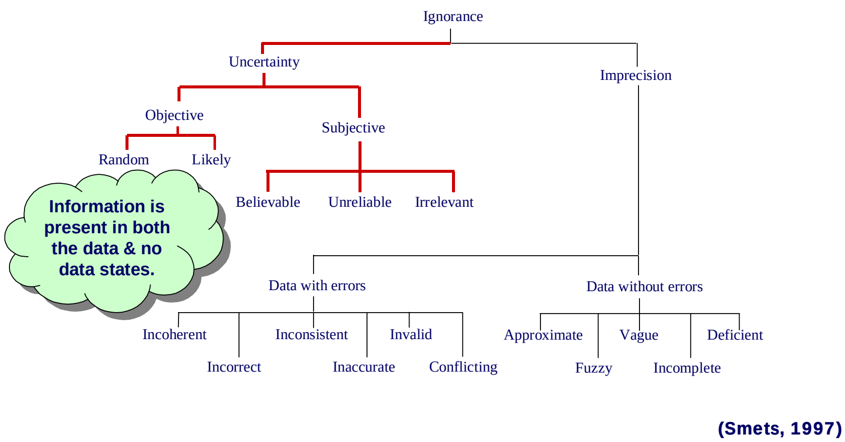

Figure 3. Smets' taxonomy of uncertainty.

A TAXONOMY OF UNCERTAINTY

The basis for accepting a partially automated or fully automated STS network goes to an issue beyond the technical specifications of the devices comprising the network: the degree of trust one has that an STS network will perform to expectation. This concept of trust is a dimension of subjective uncertainty resident in the user [6]. When an STS system fails to meet or exceed these expectations, and here we are conceptualizing field commanders as the group of users, this user group poses a serious impediment to development and fielding of an STS system. Even if such trust exists but is tenuous at best, these users will cease relying on STS functions at the first occurrence of a serious mishap. However, because sensor networks form the very foundation for achieving the high state of situational awareness envisioned for the Objective Force, turning them off will not be an option.

It appears to us that this subjective notion of trust is also related to the level of uncertainty contained in the information provided by the STS network. What is not known at this time is the level of uncertainty in the decision processes that commanders currently employ. We contend that such knowledge is crucial if one is to benchmark the improvement afforded by STS networks. To understand this link between uncertainty and trust, it is useful to understand how such uncertainty enters the network information and what one might do to mitigate these levels.

Several taxonomies concerning uncertainty have been proposed and accepted within the information research community ([6], [16]; [7]; [15]). While all provide a comprehensive representation and decomposition of uncertainty into its various components, it is Smets' taxonomy shown in Figure 3 that provides the best organization for understanding uncertainty in the context of this study for several reasons.

Unlike various other taxonomies, Smets' taxonomy makes a clear distinction between two concepts that are frequently and mistakenly mixed together: imprecision, where the central focus is on the resolution of the information, and uncertainty, where the central focus is related to the degree of imperfection present in the information.

STS network issues associated with imprecision remain an area that attracts the attention of computer scientists, sensor design engineers, network modelers. Sources of imprecision in an STS network include, but are not limited to, faulty sensors, input and/or data/information manipulation errors, inappropriate choices of representation (*e.g.*, forcing an attribute with a disjunctive value to be single-valued), and measurement noise.

The level of precision has an affect on the accuracy of information as well. This affect has its limitations, however, and past that limit, the resident uncertainty in the information itself fills the remaining gap between perfect and imperfect information.

Uncertainty can either be characterized as an objective property of the observer, or a subjective property of the observer [14]. If the uncertainty is objective, it is either random information that is subject to change whose stochastic process is known or suspected, or it is likely information that is represented by a frequency distribution based on past performance. One example of an objective uncertainty present in an STS network is the detection probabilities associated with individual sensor types.

In contrast, the degree of subjective uncertainty is based largely in the perceptions held by an observer which, for an STS network is the user. When uncertainty is subjective, it can relate to information that is believable but not entirely trustworthy, to information that is unreliable, or to information that is irrelevant. It is this uncertainty that the user faces and must either resolve or come to accept as appropriate. The nature of battle dictates that the latter should be part of the understanding this study attempts to communicate. Both objective and subjective uncertainty should be taken into consideration because both make contributions to the uncertainty of the final information product presented to the decision point of the STS network.

Subjective uncertainty arises when a user of an STS network must construct an opinion about a fact of truth of which he does not know for certain, such as enemy target information. To what extent does automating the decision process and increasing the precision of the reporting medium affect the accuracy of final information product is important to resolve.

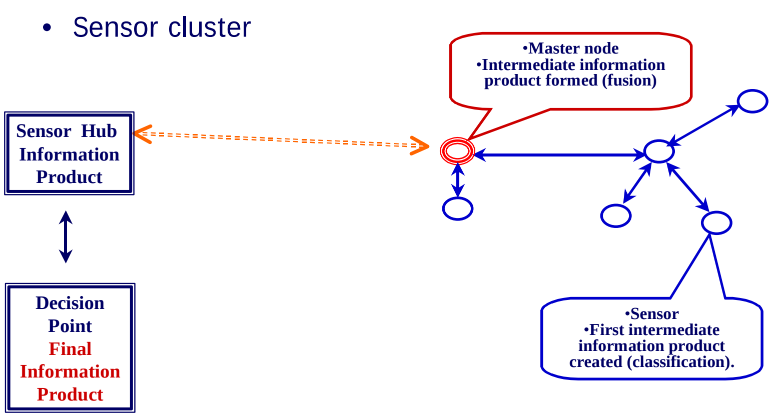

Figure 4. A generic representation of an UGS cluster as an Information Manufacturing Network.

UGS Information Manufacturing Network

Figure 5 shows the generic framework for conceptualizing an UGS network as an information manufacturing system. It also shows the most basic flow of information from point-of-origin to the fire/no fire decision point. Each individual sensor functions as a generator of *primitive data* through its process of detection. This primitive data is the most basic construct of information in both content and logical organization. When a sensor attempts low level classification by comparing sensed data vectors to classification processes, the result of this effort forms the first *intermediate information product* of the STS network.

The identification process used at the master node forms a second intermediate information product. This location is also the first point in the network at which information fusion is performed when this master node aggregates the collective classification it receives from individual sensors, applies an identification process, and constructs and transmits a single cluster report into the network that represents the conclusive opinion of the cluster.

Finally, the sensor hub further processes the intermediate information products it receives, shaping them into a form that ultimately becomes a part of the common operating picture (COP) that the decision maker sees at the decision point of the network.

Each of these processes: detection, classification, shaping, identification, voting, and re-shaping imposes some amount of uncertainty different from that caused by information technology issues such as transmission and bandwidth overflow, for example. The methodology introduced in what follows provides an explicit representation of this uncertainty that enables one to both assess the marginal contribution of each process and component of an STS network and to subsequently prioritize on locations where information maintenance must occur if the decision quality of an STS network is to remain high.

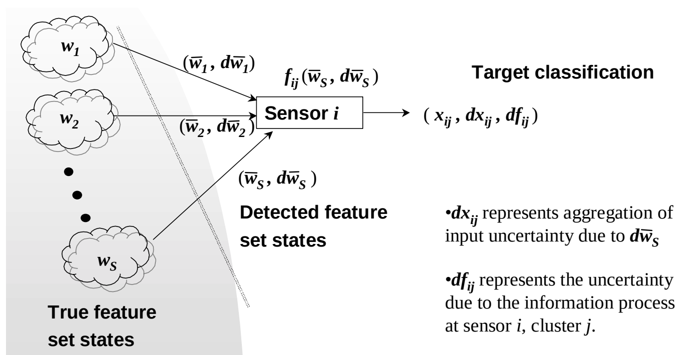

Figure 6. Initial propagation of uncertainty in an STS network.

MODELING THE PROPAGATION OF UNCERTAINTY

Potential targets on the battlefield are classified into types based on specific sets of physical features having the power to discriminate between them. Feature sets enable, for example, a sensor network to distinguish between a school bus and a troop transport. The greater number of features detected by a sensor, the stronger, and presumably the more accurate the classification that is possible. This logic supports the assertion that more information improves accuracy by reducing uncertainty. A point to be made in this regard is illustrated in Figure 6: it is the detected feature set information that is flowing on the STS network, not the true feature set. The difference between these two sets defines the first objective uncertainty propagated into the network.

Assuming that some device component is actively seeking to detect some physical feature of a potential target, we can let w_i represent a member of the true feature set *i*, *i* = 1,…, I, and $\overline{w}_i$ a member of the detected feature set. The contribution to uncertainty made by the detection process focused on each feature set is given by the differential $d\overline{w}_i$. Each sensor aggregates its input from the detection processes it houses and attempts a low level classification of the target. Let $f_{i\,j}\left(\overline{w}_i, d\overline{w}_i\right)$ represent this classification function.

Each individual sensor *i*, cluster *j* makes classification $x_{i\,j}$ and passes into the network an information product represented by the vector $\left(x_{i\,j}, dx_{i\,j}, df_{i\,j}\right)$, where $x_{i\,j}$ is the reported classification information from sensor *i*, cluster *j*; $dx_{i\,j}$ is the uncertainty associated with the classification result, and $df_{i\,j}$ is the uncertainty associated with the process of classification. We tacitly assume in this framework that if a sensor detects a potential target, the sensor will perform a classification and pass the result into the network. This is simply for convenience. The framework is capable of representing both the case where a lower threshold for acceptability is not met by the data so no classification can be attempted, or the sensor switches modes to acquire additional data prior to classification.

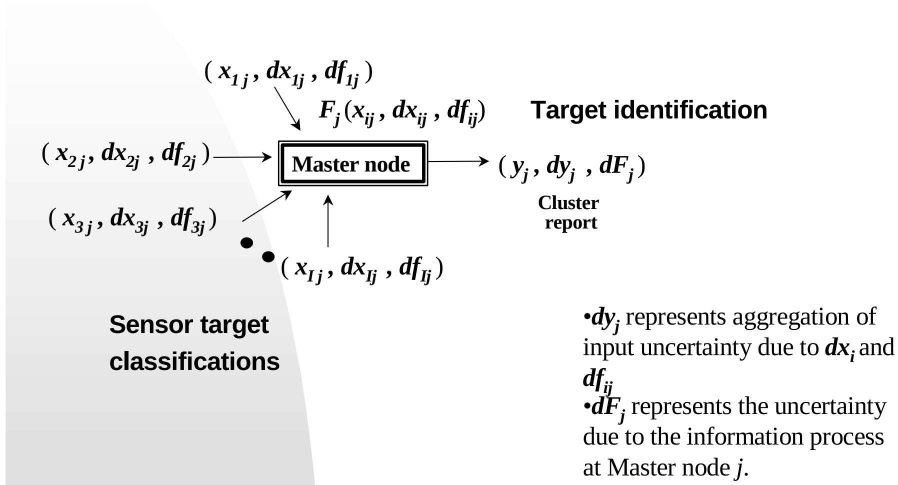

Figure 7. Uncertainty associated with the master node of a sensor cluster.

Master Node Uncertainty

Each sensor passes its classification information $\left(x_{ij}, dx_{ij}, df_{ij}\right)$ through optimized sensor cluster communications pathways using preset routing tables resident in each individual sensor. The elected master node of the cluster then aggregates the individual sensor classification information and applies a decision criterion that ultimately results in target identification. This decision criterion can be, for example, a voting process dependent upon a simple majority, or a *k*-out-of-*n* voting process. The result of this identification process gets structured into a cluster report that is subsequently passed into the network as a second intermediate information product $\left(y_j, dy_j, dF_j\right)$ to a hub location. Here, y_j represents the cluster identification reported from cluster *j*, dy_j is the uncertainty associated with identification y_j, and dF_j is the uncertainty associated with the identification process itself.

One salient difference between our framework and how an analysis of an STS network using an information technology focus would view such a network is that the "no-information" state for a sensor cluster is explicitly represented within this framework. There is an information product being passed into the network when x_{ij}, and hence y_j, is null. When either, or both of these quantities are null, the sensor cluster is actively asserting that it does not detect targets in its operational area. There is uncertainty associated with this classification and identification as well.

Decision Point Uncertainty

Finally, at some point in the network beyond or at the hub, the individual cluster reports $\left(y_j, dy_j, dF_j\right)$, *j* = 1, 2, …*n*, are consolidated and re-formatted either for presentation on a common operating picture (COP) or for comparison to preset decision thresholds. These decision thresholds take into account both the battlefield operational environment (enemy and friendly states) and prescribed rules of engagement.

The information fusion process $D\left(y_J, dy_J, dF_J\right)$ produces a final information product $\left(z, dz, dD\right)$ to the decision process. It is this final information product that forms the basis for the

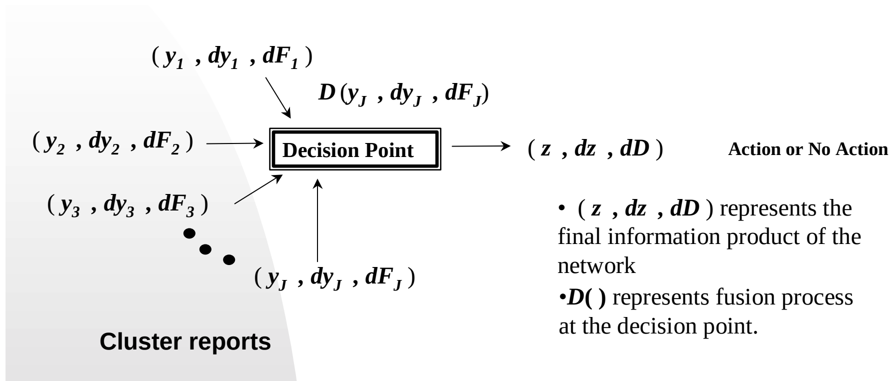

Figure 8. Uncertainty present at the decision point of an STS network.

fire/no-fire decision made by the STS network. The quality of this decision is directly dependent upon the quality of this final information product, which in turn, is directly dependent upon the amount of uncertainty present via the two components *dz* and *dD.*

The quantity *dz* represents the accumulated uncertainty propagated throughout the network from the sensors and processes preceding it. The quantity *dD* represents an additional amount of uncertainty present in this final information product due to the fusion process itself. Reducing either or both of these components should be a major design goal of STS designers since both of these quantities affect the accuracy of the final information product and hence the quality of the decision made at this point in the network.

UGS-based Single Cluster

As an illustrative example of why the type of analysis proposed in this study is relevant and important to the Objective Force design, consider the naïve single sensor target detection scenario presented in Figure 9. What is apparent to the decision point is the objective evidence provided by the information product *z*. In terms of information technology, all systems are operable and functioning with no apparent anomalies present in any of the communication pathways. Hence, the information forming the basis for the fire/no fire decision appears accurate to the decision maker.

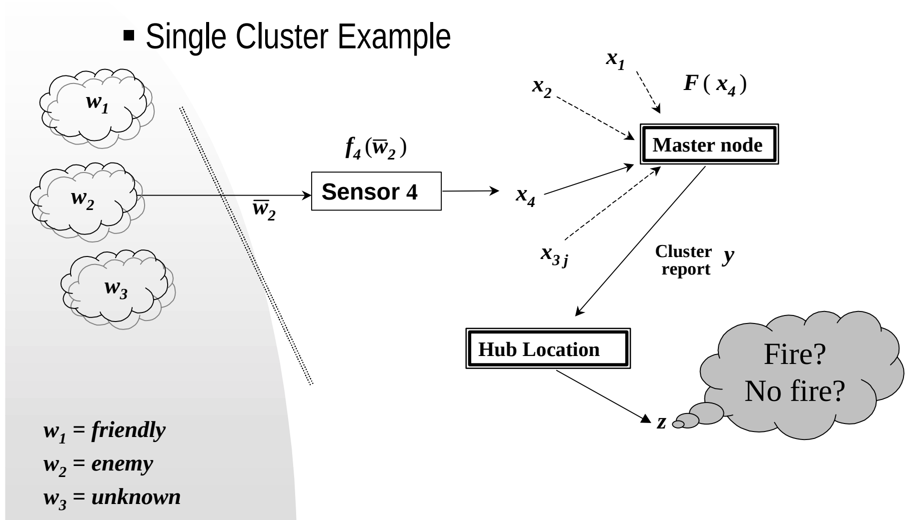

Figure 9. The propagation of uncertainty using a single UGS cluster.

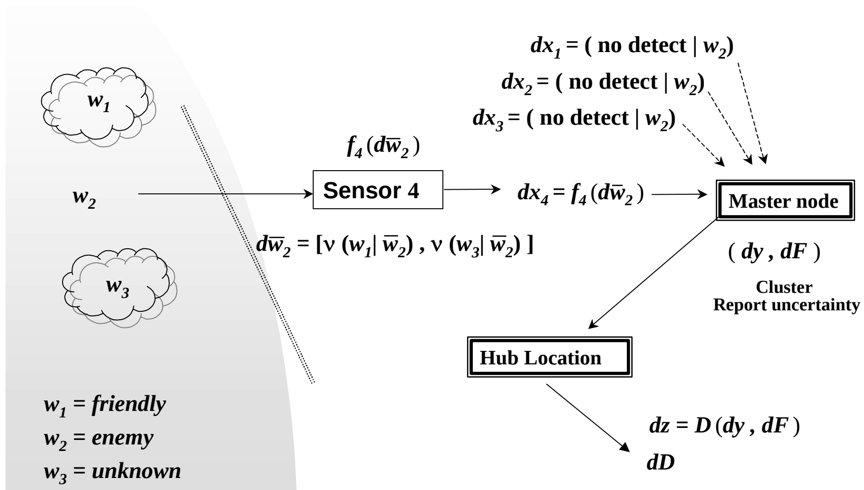

Figure 10. Uncertainty propagation due to a single sensor detection in an UGS-based STS network.

Figure 10, which represents this exact same scenario in terms of the uncertainty framework presented in this study, portrays a different perspective. When sensor 4 of the 4-sensor cluster detects an element of the enemy feature set $\overline{w}_2$ (enemy), this detection carries with it both the error associated with the likelihood that the true state of the target is w_1 (friendly) given that sensor 4 detects feature set $\overline{w}_2$ and the likelihood that the true state of the target is w_3 (unknown) given that sensor 4 detects feature set $\overline{w}_2$. This uncertainty is propagated into the STS network by the classification process *f*(*). This level of this uncertainty is further compounded by the no-detection information components provided by the other three sensors.

Finally, the cluster reporting process *F*(*) and the COP information fusion process *D*(*) each contribute to some yet unknown total amount of uncertainty present in the final information product. Using this framework, one can realize that the quality of the final information product depends upon the relative amount of uncertainty contained in *dz* and *dD*.

Measures of Sensitivity

The framework proposed enables one to quantify the contribution made to (z, dz, dD) by every device and process in the STS network. Being able to specify a closed-form expression for how changes in the level of uncertainty introduced by, say, a cluster identification report y_j affect the amount of uncertainty present in the final information product *dz* allows sensor designers to focus on device improvements that will reduce this contribution, and doctrine and force designers to identify and create resource allocations and actions that ensure the amount of uncertainty introduced during operations is minimized as well. Ultimately, such an analysis enables designers to establish priorities of effort to reduce these individual contributions based on their marginal sensitivities. This latter category is referred to as *information maintenance* ([18], [19]) operations.

Knowing the individual marginal contributions to uncertainty enables one to prescribe a prioritization scheme to existing pathways of the information flow network in an analogous fashion to that employed in a PERT chart. Ballou and Pazer [2] recognized the potential applicability of using PERT methods to handle judgmental data source items but did not address the connection with information pathways proposed here. Further, assuming that such an information quality critical path is possible to identify for any STS network, the highest priority of maintenance and protection would be assigned to this path under the rationale that the quality of the fire/no fire decision would not degrade by the loss of network elements not supporting this critical path.

A recursive method due to Ballou and Pazer [2] is currently being used to backtrack through an UGS-based STS network to obtain these closed form sensitivity expressions. Figure 11 illustrates four examples of marginal rate expressions concerning uncertainty contributions for various elements of an UGS-based STS network. These expressions yield formulas for calculating marginal contributions by using the exact distributions (when available) associated with each of quantities noted. For example, the uncertainty associated with device feature set detection would incorporate the probability distributions associated with a specific sensor device. We recognize that when such distributions are discrete, and hence non-differentiable, the discrete analog known as divided differences would be used in place of the differential expressions shown.

$\frac{dz}{dF_j}$ **To the Master node cluster *j* reporting process**

$\frac{dz}{d(df_{ij})}$ **To the uncertainty associated with the low-level classification process at sensor *i*, cluster *j***

$\frac{dz}{d(d\,\overline{w}_S)}$ **To the uncertainty associated with the detection precision**

$\frac{dz}{d(d\,x_{ij})}$ **To input uncertainty of sensor *i* to Master node *j***

•Sensitivity measures can be expressed for any point in the network.

Figure 11. Several marginal contributions to uncertainty in an STS network.

CONCLUSIONS

In this study, we introduce a framework for assessing the decision quality of an UGS-based STS network based on the level of uncertainty contained in the information products used to support this decision. Ultimately, we contend that each device and information process throughout the network contributes in some fashion to this level of uncertainty, and that these contributions can be quantified by identifying the marginal rates of contribution associated with each device and process.

The magnitude at which these marginal rates respond to perturbations caused by improvements in precision or deliberate information maintenance actions leads directly to valuable design guidelines as to efficient levels of precision that should be sought for these devices, and whether further improvements in precision are warranted. Moreover, a simple ranking of these marginal rates can identify and prioritize locations in the network where effective quality enhancements should be performed to insure the fire/no fire decision point in an STS network is supported with a high quality information product. This approach extends earlier work in modeling data and process quality in multi-input, multi-output information systems that principally focused on reducing error rates.

While this study represents a work-in-progress, we are optimistic that the results of this sensitivity analysis can be directly used to identify an *information quality critical path* defined by an end-to-end pathway through the STS network composed of those devices and processes whose perturbations in level of contribution to uncertainty most affect the quality of the final information product at the decision point. Information maintenance activities designed to enhance the quality of this final information product will then be focused on this IQ critical path. Moreover, since these STS networks will be used in conflict scenarios involving all armed services of the United States, protecting this critical path from disruption or destruction will necessarily become a high priority as well.

REFERENCES

[1] Alberts, D.S., Garstka, J.J., Stein, F.P. *Network Centric Warfare: Developing and Leveraging Information Superiority*, Department of Defense C4ISR Cooperative Research Program, Washington, D.C., 1999.
[2] Ballou, D.P., Pazer, H.L. . "Modeling data and process quality in multi-input, multi-output information systems," *Management Science*, 31 (2), 1985, pp. 150-162.
[3] Ballou, D.P., Pazer, H.L. "Designing information systems to optimize the accuracy-timeliness tradeoff," *Information Systems Research*, 6 (1), 1995, pp.51-72.
[4] Ballou, D.P., Wang, R.Y., Pazer, H.L., Tayi, G.K. "Modeling information manufacturing systems to determine information product quality," *Management Science*, 44 (4), 1998, pp. 462-484.
[5] Bodnar, G. "Reliability modeling of internal control systems," *Accounting Review*. 50 (4), 1975, pp. 747-757.
[6] Bonnissone, P.P., Tong, R.M. "Editorial: reasoning with uncertainty in expert systems," *International Journal of Man-Machine Studies*, 22, 1985, pp. 241 – 250.
[7] Bosc, P., Prade, H. "An introduction to the fuzzy set and possibility theory-based treatment of flexible queries and uncertain or imprecise databases. In A. Motro and P. Smets, editors, *Uncertainty in Information Systems: From Needs to Solutions*, Kluwer, Boston, MA, 1997, pp. 285 – 324.
[8] Cushing, B.E. "A mathematical approach to the analysis and design of internal control systems," *Accounting Review*, 49 (1), 1974, pp. 24-41.
[9] *FORCEnet and the 21st Century Warrior*. Chief of Naval Operations Strategic Studies Group XVIII, Naval War College, Newport, Rhode Island, November 2001.
[10] Harney, R.C. "Information-based approach to performance estimation and requirements allocation in multisensor fusion for target recognition," *Journal of Optical Engineering*, 36 (3), 1997, pp. 789-798.
[11] Kwinn, M.J., Davis, M.J., McGinnis, M.L. "A framework for the analysis of the future combat system conceptual design alternatives," Technical Report DSE-TR-01-05, Operations Research Center (ORCEN), U.S. Military Academy, West Point, New York, 2001.
[12] Lamm, L.M., Driscoll, P.J., Lamm, G. "Networked unattended ground sensor fields: tradeoff study and configuration rules methodology," Technical Report DSE-TR-02-10, Operations Research Center (ORCEN), U.S. Military Academy, West Point, New York, 2002.
[13] Morey, R.C. "Estimating and improving the quality of information in the MIS," *Communications of the ACM*, 25 (5), 1982, pp. 337 - 342.
[14] Parsons, S. *Quantitative Methods for Reasoning Under Uncertainty*, MIT Press, Cambridge, MA, 2001.
[15] Smets, P. "Imperfect information: imprecision and uncertainty." In A. Motro and P. Smets, editors, *Uncertainty in Information systems: From Needs to Solutions*, Kluwer, Boston, MA, 1997, pp. 225 – 254.
[16] Smithson, M. *Ignorance and Uncertainty: Emerging Paradigms*. Springer-Verlag, New York, NY, 1989.
[17] Stratton, W.O. "Accounting systems: the reliability approach to internal control evaluation," *Decision Science*, 12, 1981, pp. 51-67.
[18] Wang, R.Y., Storey, V., Firth, C.P. "A framework for analysis of data quality research," *IEEE Transactions on Knowledge and Data Engineering*, 7 (4), 1995, pp. 623-640.
[19] Wang, R.Y., Strong, D. "Beyond accuracy: what data quality means to data consumers," *Journal of Management Information Systems*, 12 (4), 1996, pp. 5-34.
[20] Wang, R.Y., Lee, Y.W., Pipino, L.L., Strong, D.M. "Manage your information as a product," *Sloan Management Review*, 39 (4), 1998, pp. 95-105.
[21] Yu, S., Neter, J. "A stochastic model of the internal control system," *Journal of Accounting Research*, 1 (3), 1973, pp. 273-295.