Quality-of-Information Aware Networking for Tactical Military Networks

A. Bar-Noy, G. Cirincione, R. Govindan, S. Krishnamurthy, T. F. LaPorta, P. Mohapatra, M. Neely, A. Yener

***Abstract*—In tactical military networks, decisions must often be made quickly based on information at hand. It is a challenge to provide decision makers with a notion of the quality of the information they have, or to provide a method by which decision makers can specify a required quality of information. It is a further challenge to honor requests for a required quality of information when selecting information sources, transporting information through a highly-dynamic network, and perhaps performing processing on that information. In this paper we motivate the need for a general, but formal, definition of quality-of-information so that this metric may be specified and potentially optimized by algorithms that operate a tactical network. Furthermore, we define a new notion, the operational information content capacity, to capture the amount and quality of information that a network can deliver.**

I. Introduction

The objective of a tactical military network is to facilitate information flow between its nodes in order to support distributed decision making in the best way possible. Recent counterinsurgency [9] (COIN) operations have highlighted the importance of tactical networks and placed increasing demands on their performance. COIN is an extremely complex form of warfare that places significant burden on the people and technologies that are employed during operations. It is an intelligence-driven endeavor and, unlike conventional warfare, relies on intelligence flows that are more bottom-up than top-down.

Conventional metrics to evaluate tactical networks consider communication quality, irrespective of the content of information, for example their throughput or the number of reliably communicated bits per unit resource. From a tactical perspective, however, these networks need to be ultimately judged by the effectiveness of network-centric decision-making they can facilitate. To this end, the nodes of the tactical network collectively produce and process information whose content matters a great deal. As such, it is imperative to revisit what networking means for tactical networks. Existing approaches generally assume that networks are designed to transfer bits without regard to the quality of the information or the context for its use. These approaches focus on derivative metrics that do not directly impact sense-making or decision making. In an information-agnostic manner, they focus on models and traffic engineering mechanisms that provide service quality by resource reservation control and developing routing and access control algorithms. It is becoming increasingly evident that communications networks are intricately linked to information and social networks and that treating them independently is insufficient for tactical settings.

Indeed, our vision is that networks must explicitly recognize, process, and optimize information, and this paper outlines a novel approach towards this vision: the adoption of Quality of Information (QoI)-aware networking that seeks to model the network as an information source and directly supports the information needs of the users. In addition, the information must be safe-guarded to retain its quality while it is transferred via the network.

QoI is a composite, multi-dimensional, metric that captures the trade-offs of several components to characterize the information ultimately delivered to the application. Applications may specify a *desired-QoI* in terms of values or value-ranges for several *attributes* of information such as the source of information, its freshness and precision, as well as the chain of information custody through the network. These factors determine the eventual value assigned to information in the decision-making process. The network then attempts to meet the *desired-QoI*, perhaps with some probabilistic guarantees, and deliver information with a certain QoI (called the *delivered-QoI*): depending on the type of application, if it cannot, it may reject the application request or deliver the information at a lower QoI. For a given network, a measure of the amount of information that can be delivered at a certain QoI satisfaction level is termed its *Operational Information Content Capacity* (OICC).

In this paper, we first motivate QoI and OICC by example in the next section. We then formally define QoI and present open research challenges in realizing a QoI-aware networking stack for tactical networks. We conclude with a couple of case studies that illustrate our ongoing research in this area.

II. Motivating Examples of QoI

Consider the case where a military unit is conducting counterinsurgency operations. Intelligence, surveillance, and reconnaissance (ISR) operations are used to collect information about the enemy, terrain, weather, local populace, and many other aspects that will affect operations. The commander will identify and prioritize uncertainties that must be resolved to accomplish the mission and create priority intelligence requirements that will be used to task ISR assets and soldiers. A key tenet of COIN doctrine is that control of intelligence assets is pushed to the lowest possible echelon. This significantly burdens networking, as the information to be collected and analyzed *far exceeds the ability of networks to deliver and process this intelligence*.

A specific example where the QoI impacts resources and decision making follows. A commander is faced with a series

978-1-61284-936-2/11/$26.00 ©2011 IEEE

of car-bombings in their area of operation and is employing a variety of collection assets to develop the intelligence necessary to mount effective operations to neutralize these threats. The scenario may unfold as follows: pattern analysis of wide area (low resolution) surveillance imagery that has been downloaded from aircraft returning from surveillance missions identifies routes to the car bombing sites from several suspicious buildings. A cordon is placed around the area where these buildings are located. Reports from interviews conducted by the patrol with locals and from informants identify an IED cell leader that has been seen in the area. Sensors are cross-cued to search and track based on information from sensors and reports. When the cell leader is detected arriving at the building a squad enters the building where they find vehicles rigged as car bombs and detain several insurgents. The squad questions the detainees and explores the building, which leads to other targets and car bomb staging areas.

Focusing on the simple case where the commander seeks to locate the cell leader, the QoI that is needed varies depending on the kind of decision that will be made and the risk inherent in that decision. For example retasking a sensor has less risk than sending troops into a dangerous area or calling in an airstrike. If the commander decides to detain and question the cell leader it may be done with less certain or lower quality of information than if the commander calls in an airstrike. Less credible sources or those that have weaker authentication may be acceptable to detain a suspect, although the commander may require corroboration from multiple sources. To call in an airstrike however, the commander may demand strong authentication of the sources with information that has high precision and delivered over secure communications links. These risk assessments are fluid and thus QoI requirements are dynamic which significantly complicates attempts to adjust the network to best meet these needs.

Consider three modalities of information that could be used to locate the cell leader: photo images, full motion video, and text messages from informants or from soldiers on patrol. It is easy to realize that all three such sources can provide the same information, albeit with different quality and with differing amounts of network resources required for delivery of the information. In this simple example, video requires more resources than images than do text messages. For any modality of information, however, there are several factors that determine QoI: the credibility of the information source, freshness/timeliness, correctness, precision/accuracy, and security. Some of these are intrinsic metrics of QoI: for example, precision, which relates to the resolution of the camera and frame rate of the video. The age (freshness), security, and correctness of the information are also intrinsic metrics as they are independent of the situation. Some metrics are contextual measures as they depend on the situation and the decision at hand. These include timeliness, which measures the availability of information relative to the time it is needed, and completeness which gauges the relevance of information for a particular use.

In this example, timeliness and completeness requirements are much more stringent if the commander wishes to call in an airstrike than if a squad is to be sent to detain and question the suspect. The required QoI of a piece of information may also depend on what other information is available. If a low resolution video is coupled with a simple report from an authenticated reliable source that the cell leader is present at a location, the composite QoI will be much higher than each individual piece of information.

III. QoI and OICC

QoI is a composite multi-dimensional metric that can be represented intuitively as:

$$QoI = f(I, D, P, S) \tag{1}$$

where I captures the attributes of the information source, D captures the characteristics of the network delivery, P represents the transformations of data by in-network processing, for example fusion or compression, and S accounts for the security properties present in the network.

QoI is a measure of the instantaneous quality of a piece of information. A photo delivered by the network has a certain freshness, resolution, etc. Similarly, a video stream has a rate, resolution, the field of vision, a loss rate, etc. The individual attributes define a vector which we call delivered-QoI. As network and source conditions change, subsequently delivered photos and videos may have different QoI. Finally, the ability to meet a desired-QoI may be stochastic, i.e., specified as a probability distribution.

As discussed above, certain attributes of QoI, such as video frame rate or photo resolution, are intrinsic to an information source. These attributes are independent of the situation for which the information will be used [1]. Other attributes of QoI, called contextual attributes, may depend on the situation for which the information is being used [1]. A good example is the timeliness of data. In some cases, an application requires data with very low latency as in the example above. In others, latency may not be as important, for example, for missions based on long-term planning.

Several attributes of QoI are listed in Figure 1, along with general definitions and characteristics of specific types of information sources that map to these attributes. These attributes are clearly specified in DoD documentation as the basis for evaluating information [10], [11], but prior work has not considered any systematic way of processing information based on QoI, and networking research has not accounted for information or its quality. Also, individual attributes of QoI, such as those listed in Figure 1, interact which each other, often depending on their intended use, to form a composite QoI.

The information source dictates a fundamental limit of the QoI of the raw information. For example, the resolution of a photo has a maximum value dictated by the camera. If the information from the source was instantaneously delivered to its consumer without any loss or processing, the QoI at the receiver will be the same as at the sender. More generally, however, the QoI at the receiver may be different than that at

	Metric	General Definition	Image	Video	Text
$QoI_{instrinsic}$	Correctness	Closeness to ground truth	Field of view, resolution		Truthfulness of report
	Freshness	Age	Capture time		
	Precision	Extent of detail	Resolution	Resolution Frame rate	Detail of description
	Security	Protection of information and source	Provenance, authentication, integrity, non-repudiation, confidentiality		
$QoI_{contextual}$	Accuracy	Specificity relative to need	Resolution, field of view	Resolution, frame rate, field of view	Ability of reporter
	Timeliness	Availability	Delivery latency		
	Completeness	Total relevance to ground truth	Field of view	Field of view, frame rate	Breadth of description
	Credibility	Extent believable	Trust in information		

Fig. 1. Intrinsic and Contextual QoI metrics

Video QoI Component	Data Delivery				Processing	
	Rate	Loss	Latency	Jitter	Com-pression	Fusion
Correctness		Reduces resolution			Reduces resolution	
Freshness			Increases age	May increase age due to buffering	May decrease age by reducing amount of data to be delivered	
Precision	Frame rate, resolution	Reduces resolution			Reduces resolution, frame rate	May increase detail
Accuracy					May reduce field of view, frame rate	May corrob-orate
Timeliness			Reduces timeliness	May reduce timeliness due to buffering	May decrease age by reducing data to be delivered	
Complete-ness		Reduces number of frames			May reduce field of view, frame rate	May increase info

Fig. 2. Factors affecting the QoI of video streams

the source because of the impact of the network, in-network processing and security properties. In this section we briefly discuss the impact of data delivery and in-network processing on QoI. In later sections, we explore other QoI attributes like provenance or credibility.

The data delivery characteristics of the network cannot improve the QoI, but can degrade it. Typical metrics of interest for data delivery are data loss, latency, rate, and jitter. While these are traditional quality of service metrics, each metric will have a different impact on QoI depending on the information source (intrinsic QoI) and the information use (contextual QoI).

In-network processing of information may either degrade or improve QoI. For example, lossy compression may reduce the resolution of an image, thus lowering its QoI. Conversely, software in a node that can perform feature extraction and identify individuals may increase the QoI delivered to a consumer.

Some of the relationships between network delivery and in-network processing, and the delivered-QoI are shown in Figure 2 for a video stream. For example, consider the impact of compression on the QoI of a video stream. If lossy, compression may reduce video resolution, frame rate and field of view, thus decreasing QoI because of the negative impact on precision, accuracy and completeness. On the other hand, because compression reduces the amount of information to be transferred over the network, it will reduce the age of the images in the video, and will improve the timeliness of the video. Likewise, losses in QoI caused by compression may be recovered or surpassed by fusing multiple information sources (and modalities) in the network. For example, the annotation of video with a textual description of an event from an independent source may provide additional details, improving precision, and corroborating what is in the video, thus improving accuracy.

Thus, there is a trade-off between the various metrics when determining the ultimate QoI of the video stream. It is also apparent that the selection and configuration of an information source has a large bearing on QoI. A camera, for instance, may adjust its zoom which will reduce is field of view. Depending on the context, the decreased field of view may not degrade completeness but may increase precision.

If an application has a minimum desired-QoI, in general that desired-QoI may be represented as a multidimensional surface that captures the trade-offs of different attributes of QoI.

Not all QoI attributes will be threshold-based. There may be values of attributes above which there is no gain in QoI. Contextual attributes may vary depending on the presence of other information.

IV. Challenges for QoI-aware Networking

There are several challenges in realizing our vision of characterizing networks on their achievable QoI, and ultimately their OICC. These include defining QoI functions, transforming QoI into OICC, and linking the communications and information networks. We summarize some of these challenges in this section.

Appropriate QoI functions for specific applications within the context of tactical missions must be defined. While several studies have defined attributes which impact QoI, some of which are summarized in Table 1, a model in which the tradeoffs of these attributes are quantified has been elusive. It is difficult to define these relationships for different applications, in context.

Furthermore, a transformation from QoI to achievable OICC must be undertaken. This transformation must take into account the time dimension, thus quantifying the amount and quality of information that can be transferred across a network in the presence of multiple information flows and end nodes. In essence, OICC is related to "how many correct decisions are enabled by information obtained by the network per unit time." Depending on how QoI is specified, there are several ways in which this formulation can transpire.

If QoI is represented as a surface of the minimal QoI requirements of a mission then we can define OICC as the number of information requirements that can be accommodated concurrently in a network so that the achievable QoI of all required information is above the minimum surface. Of course, specifying only a minimum QoI surface may not allow a true optimization of QoI. In many cases in addition to a minimum QoI, decision making will be improved by increasing QoI up to a point. To capture these situations, a measure of the derived decision making ability as a function of QoI must be developed.

The optimization of achievable QoI and OICC itself is challenging on two fronts. First, mathematical models must be developed followed by optimization over the variables of the model. Furthermore, functions to accurately represent QoI and OICC may not turn out to be non-convex, complicating the optimization task at best and often making global optimality guarantees impossible. In these cases, we may have to resort to approximation algorithms.

Second, realizing a mobile tactical network which provides optimal QoI will be challenging as it is difficult for nodes to obtain global knowledge of a network. Without global knowledge of network conditions, resource allocation within the network would be done based on locally available information. Any practical realization of such algorithms must be distributed, executing within network nodes that have knowledge of QoI requirements, network conditions, and context. While the network nodes may be able to accurately estimate and control their impact on intrinsic QoI attributes, to do the same for contextual QoI attributes will require intelligence within nodes to interpret information use. Furthermore, because QoI may also depend on what information has already been received by an information recipient, contextual QoI attributes will be especially problematic for network nodes to determine. Thus it is likely that QoI may only be ultimately determined at the information consumer.

Given the need for network nodes to understand contextual QoI requirements, and the strong dependency of QoI and OICC on the selection of information sources, information recipients will play a large role in achieving optimal OICC. The information recipients will influence source selection, set the contextual QoI attributes and provide QoI functions to network nodes.

To realize QoI-aware networking, methods must be developed to measure, estimate, or infer the QoI of information; and to pass information between nodes to learn QoI requirements and to understand how other nodes on a path in the network are impacting QoI. This information will be transported in meta-data attached to packets carrying data. Meta-data processing techniques are important because the size of this meta-data can become prohibitively large depending on the amount of attributes feeding QoI and the number of information sources and nodes involved in information transfer and processing. Thus, there will be a tradeoff between how precisely QoI information is passed between nodes and specified to the information consumers, and how much overhead QoI-aware networking will incur. Sensitivity analysis of which attributes have the largest impact on QoI is necessary so that these tradeoffs may be made efficiently.

Moreover, to fully realize our vision the techniques used in the communications network to recognize, process, and optimize information should be applied to information search, querying, and knowledge discovery operations in the information network. An important joint communications/information network challenge is understanding how QoI evolves as it is filtered, aggregated, and fused throughout the network.

V. Case Studies in QoI Tradeoffs

Although optimizing the QoI extracted from the network is a challenging topic, we have initial forays in two directions that illustrate how to make QoI tradeoffs, and the network costs associated with making these tradeoffs, in the context of two important attributes of the quality of information, *provenance* and *credibility*.

Provenance and QoI. An important attribute of QoI is *provenance*, the chain of custody and the transformations performed on a piece of data. Provenance can be used for forensics, to establish security properties, or to assess the credibility of information. However, gathering provenance information can impact the network throughput and its ability to delivery high QoI, a tradeoff that we briefly analyze in this case study.

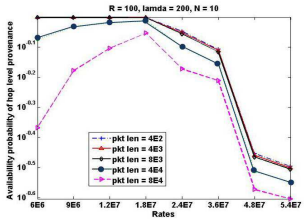

Fig. 3. Hop level provenance availability in a wireless network of 10 nodes.

To simplify matters, we consider what we call *operational provenance* or OP for short; OP refers to the procurement and maintenance of a history of transmissions that occur in the network. Provenance subsumes the desirable attribute of non-repudiation wherein a node cannot lie about performing a transmission in a network. In essence, a functional module that provides OP becomes a key part of a network forensic system. One might expect that providing OP impacts the data delivery functionalities of the network and thus influences the QoI in a complex way: this case study illustrates this tradeoff.

Let us consider a simple case wherein nodes are expected to digitally sign the packets they forward; this would verify that a node that claims to have performed a transmission did indeed do so. However, digital signatures incur both processing overhead and increase the size of the packets. The first factor limits the rates at which individual nodes can inject traffic into the network; the second factor limits the quantum of traffic that can be injected. If a PKI infrastructure is used for signing packets, nodes may have to have their keys certified by an authority; this would incur additional overhead that further affects the achievable rates.

Alternatively, consider the "overhearing packet transmissions by third-party" nodes as our verification process for collecting OP. In order to ensure that the packets being exchanged by a pair of nodes are *overheard* by other nodes for verification purposes, there may be a constraint imposed on the transmission rate. A lower transmission rate will decrease the likelihood that a packet is lost due to wireless channel induced effects; on the other hand it increases the packet air-time and is more likely to be subject to interference and collisions. One

can consider the following question for a given a packet length: What is the highest usable bit rate with (1) all hops using the same rate or (2) different hops using different rates – so as to fulfill a provenance requirement? In case (1), we can simply try each rate in descending order and find the maximum rate that satisfies the provenance requirement. Note that since the number of usable rates is finite, this operation can be done in a small finite time. Case (2) is more complicated. If we aim for using the highest rates possible, the problem can be posed as:

$$\begin{aligned} &\text{Minimize } \sum_{i=1}^{H} \frac{1}{r^{(i)}} \\ &\text{Subject to } \prod_{i=1}^{H} Pr_{hop\_OP}(r^{(i)}) \geq \beta, \\ &\quad r^{(i)} \in [r_0, ..., r_{M-1}], \forall i \in [1, H], \\ &\quad 0 < \beta \leq 1, \\ &\quad H \in \mathbb{N}. \end{aligned} \tag{2}$$

where, H is the number of hops on the considered path and is a positive integer. $r^{(i)}$ is the rate used on hop i. $Pr_{hop\_OP}\left(r^{(i)}\right)$ is the OP availability probability for hop i when rate $r^{(i)}$ is used; this probability represents the likelihood that one can effectively verify a transmission on the i^{th} hop of the path. β is the desired threshold on OP and is a real number between $[0, 1]$. The objective is to minimize the total transmission time along the path. This in turn results in the use of the highest rates on each link of the path. The constraint imposes that the path level provenance should be no less than β. $r^{(i)}$ can be any rate from among M available rates. Note here that computing $Pr_{hop\_OP}\left(r^{(i)}\right)$ is non-trivial; depending on the verification process, one may have to perform a set of complex analytical computations to derive this probability. If this probability was found, the above optimization problem can be solved by dynamic programming. Other network attributes such as packet size, network load and node density all influence the ability of nodes to overhear transmissions towards gathering OP. Accounting for these factors will make the problem multi-dimensional and more complex.

To illustrate these tradeoffs, we have chosen the above functions for providing OP (digital signing and overhearing) and have performed simulations using the OPNET 2.0 modeler. We consider a network of 10 nodes in one of our simulation runs and vary both the packet size and the data rates used for transmissions. We estimate the throughputs and the OP along various paths. The results are shown in Figure 3. We observe that at very low data rates, the OP on each hop is fairly low; this is because while such low rates help cope with wireless channel induced effects, they also increase the packet air-time thereby making overhearing more susceptible to interference related failures. As we increase the transmission rate, the likelihood of obtaining OP increases. However, at extremely high rates, channel induced failures dominate and the likelihood of obtaining OP drops. To our suprise we observed a similar trend in throughput. Upon careful examination, we determined that the very same factors affect the throughput in similar ways. Lower rates are not conducive to high throughputs due to interference and collision related effects; extremely high rates are again detrimental to throughput due to excessive channel induced losses.

Clearly, we are but scratching the surface. The impact of the choice of route has to be considered. More realistic and complex verification procedures are necessary. Finally, in our simulations we only consider performance in terms of throughput. The quality of information is more complex and may be affected by the type of media being transmitted (video versus text). Considering provenance (or security in general) with different types of information is to our best knowledge an open challenge.

Optimizing Credibility of Information. Another important factor that impacts QoI is credibility, defined as the objective believability of information [13]. Intuitively, credibility captures a notion we all use regularly in our daily lives: a piece of information from the New York Times is generally assessed to be more credible than hearsay from a stranger on the street. The credibility of information generated by a network depends upon many factors: the source of information, the circumstances under which information was gathered, and the provenance of the information.

In this case-study, we illustrate how to optimize a simplified form of credibility. Consider a field operation consisting of N participants, whom we call *reporters*. Each reporter is equipped with a wireless communications device and directly reports to a commander. Each reporter reports on an *event*; for example, sighting of an enemy combatant, or suspicious movements of insurgents. Events occur at a particular *location*, and multiple events may occur concurrently either at the same location or at different locations.

Reporters can transmit reports of an event using one of several formats: such as a video clip, an audio clip, or a text message describing what the report sees. Each report is a form of *evidence* for the existence of the event. In general, we assume that each reporter is capable of generating R different report formats, denoted by f_j, for $1 \leq j \leq R$. However, different formats have different costs to the network: for example, video or audio could consume significantly higher transmission resources than, say, text. We denote by e_j the cost of a report f_j.

Now, suppose that the commander has heard, through out of band channels or from a single reporter, of the existence of an event E at location L. To verify this report, the commander would like to request *corroborating* reports from other reporters in the vicinity of L. Which reporters should he get corroborating reports from? What formats should those reporters use?

To understand this, we need to define the *credibility* of a report. We can model the credibility using two common intuitions about credibility. The first intuition is based on the maxim "seeing is believing": a video report is more credible than a text report. We extend this maxim in our model to incorporate other formats, like audio: audio is generally less

credible than video (because, while it gives some context about an event, video contains more context), but more credible than text (for a similar reason).

Our second intuition is based on the often heard statement "I'll believe someone who was there", suggesting that proximity of the reporter to an event increases the credibility of the report. More precisely, a report A generated by a reporter at distance d_a from an event has a higher credibility than a report B generated by a reporter at a distance d_b, if $d_a < d_b$.

Formally, let S_i be the position of reporter i, L be the position of event E and $c_{i,j}(S_i, L)$ be the credibility of the report generated by reporter i when report format f_j is used. We define $c_{i,j}(S_i, L)$ as:

$$c_{i,j}(S_i, L) = \begin{cases} \gamma_j / d(S_i, L)^{\delta_j}, & \text{if } h_0 < d(S_i, L) \\ \gamma_j / h_0^{\delta_j}, & \text{if } d(S_i, L) \leq h_0 \end{cases} \quad (3)$$

with $1 \leq j \leq R$, $\gamma_1 \leq \gamma_2 \leq \cdots \leq \gamma_R$, and $\delta_1 > \delta_2 > \cdots > \delta_R$. Here, $d(.)$ is the Euclidean distance between points, h_0 is a certain minimum distance to avoid division by zero as well as to bound the maximum credibility to a certain level, γ_j is a constant of proportionality implying the maximum achievable credibility of report format f_j, and the credibility decays according to a power-law with exponent δ_j when format f_j is used.

Our credibility model incorporates the two intuitions described above: the dependence on proximity is captured by the power-law decay with distance, and the higher credibility of the video compared to text is captured by having a larger γ and a smaller exponent for video.

We can then formulate the following optimization problem, called MaxCred, which attempts to maximize information credibility, while keeping network cost to within a specified budget:

$$\begin{aligned} \text{Maximize :} \quad & \sum_{i=1}^{N} \sum_{j=1}^{R} x_{i,j} c_{i,j} \quad (4) \\ \text{Subject to:} \quad & \sum_{i=1}^{N} \sum_{j=1}^{R} x_{i,j} e_j \leq B \\ & x_{i,j} \in \{0, 1\}, \forall i \in \{1, ..., N\}, \forall j \in \{1, ..., R\} \\ & \sum_{j=1}^{R} x_{i,j} \leq 1, \forall i \in \{1, ..., N\} \end{aligned}$$

where $x_{i,j}$ is a binary variable that is 1 if reporter i uses format f_j, and 0 otherwise, and B is the desired cost budget (with credibility values being additive).

We briefly summarize our results in exploring this optimization [6]. This *one-shot* corroboration-pull problem can be cast a discrete optimization problem and we show that it reduces to a multiple-choice knapsack problem with weakly-polynomial optimal solutions. We develop strongly-polynomial, but inefficient, solutions for the case when the number of formats is fixed, and an optimal algorithm for the case of two formats. Finally, we derive an approximation algorithm for the general case that leverages the structure of our credibility model. On a realistic dataset of events obtained from Google news, this approximation algorithm is about 20% off the optimal, but its running time is 2-3 orders of magnitude faster than the optimal algorithm, which can make the difference between success and failure in COIN operations, and enables a tradeoff between the level of credibility and the timeliness of the information.

VI. Related Work and Conclusions

In this paper, we have introduced a vision for QoI-aware networking for tactical military settings, described some challenges in achieving this vision, and presented two concrete challenges that arise in ensuring QoI-aware tactical networks.

To date, QoI has been used to characterize data extracted using a sensor network [2], [3], and methods have been developed for admission control for multiple QoI tasks in sensor networks [7]. More generally, QoI has been used to assist in data retrieval [4] or to facilitate sharing stored data [8]. Unlike these approaches, ours incorporates information quality directly into the design of a tactical network, borrowing from military doctrine that specifies information quality criteria to be used during operations [10]. To our knowledge, prior work has not explicitly explored provenance tracking within a communications network, although limited forms of provenance tracking may be found in monitoring and forensics systems like [12]. Similarly, we are not aware of prior work on extracting credible information from within a communications network; credibility has mostly been explored in sociological research [5], [13].

References

[1] D.S. Alberts and R.E. Hayes. Understanding Command and Control. 2006.

[2] C. Bisdikian, L.M. Kaplan, M.B. Srivastava, D.J. Thornley, D. Verma, and R.I. Young. Building Principles for a Quality of Information Specification for Sensor Information. In *12th International Conference on Information Fusion*. IEEE, 2009.

[3] C. Bisdikian, D. Verma, L. Kaplan, M. Srivastava, and D. Thornley. Defining Quality of Information and Metadata for Sensor-originating information. In *4th USMA Network Science Workshop*. IEEE, 2009.

[4] M. Burgess, W. Gray, and N. Fiddian. Establishing a Taxonomy of Quality for Use in Information Filtering. *Advances in Databases*, pages 241–256, 2002.

[5] B. Hilligoss and S. Rieh. Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context. *Information Processing and Management*, 44, 2008.

[6] B. Liu, P. Terlecky, A. Bar-Noy, R. Govindan, and M. Neely. Optimizing Information Credibility in Social Swarming Applications. Technical report, http://arxiv.org/abs/1009.6006, 2010.

[7] C. H. Liu, C. Bisdikian, J. W. Branch, and K. K. Leung. QoI-Aware Wireless Sensor Network Management for Dynamic Multi-Task Operations. In *Proc. IEEE Secon*, 2010.

[8] P. Missier, S. Embury, M. Greenwood, A. Preece, and B. Jin. Quality Views: Capturing and Exploiting the User Perspective on Data Quality. In *Proceedings of the 32nd VLDB*, 2006.

[9] Department of Defense. Field Manual 3-24: Counterinsurgency. pages 1–152, 2006.

[10] Department of Defense. Joint Publication 6-0: Joint Communications System. 2006.

[11] Department of the Army. Department of Defense: Mission Command: Command and Control of Army Forces. 2003.

[12] K. N. Ramach, E. M. Belding-royer, and K. C. Almeroth. Damon: A distributed architecture for monitoring multi-hop mobile networks. In *IEEE SECON*, 2004.

[13] S.Y. Rieh and D.R. Danielson. Credibility: A Multidisciplinary Framework. *Annual review of information science and technology*, 41(1):307–364, 2007.