15th ICCRTS

"The Evolution of C2: Where Have We Been? Where Are We Going?"

Title of Paper: **Human Decision Making Performance in Degraded Network Video Conditions**

Topic(s):
Topic 2: Networks and Networking

Name of Author(s)

Kevin S. Chan
Natalie Ivanic
Elizabeth K. Bowman

Point of Contact: Kevin S. Chan

Name of Organization: US Army Research Laboratory

Complete Address:
RDRL-CI-NT
2800 Powder Mill Road
Adelphi, MD 20783

Telephone: 301-394-5640

E-mail Address: kevin.s.chan@arl.army.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Human Decision Making Performance in Degraded Network Video Conditions	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army Research Laboratory,RDRL-CI-NT,2800 Powder Mill Road,Adelphi,MD,20783**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Proceedings of the 15th International Command and Control Research and Technology Symposium (ICCRTS '10), Santa Monica, CA, June 22-24, 2010

14. ABSTRACT
Future capabilities of battle command systems and networked systems will increase Soldier situational awareness by providing access to information from various networked assets. We conducted a series of experiments at the United States Army Research Laboratory in Adelphi, MD and at C4ISR On-the-move (OTM) at Ft. Dix, NJ. Based on the quality of service of battle command systems, the Soldier will be able to complete his mission objectives with a varying degree of success. Our experiments study the ability of the Soldier to identify various details within a simulated unmanned vehicle sensor feed given a range of quality of service (QoS) (by varying specific network parameters). In addition to understanding these systems from a strictly technical perspective, we are also interested in the performance from a network science perspective. This involves the consideration of the communications, information, and social/cognitive networks and their influence on situational awareness in tactical environments. Specifically, we are interested in the relationship of the Soldier?s performance, decision-making ability, and trust in the network in these environments. We identify trends in these metrics as a function of video QoS, which if characterized properly can be used to predict Soldier performance based on the QoS. Further characterization of these relationships may assist in the design of future battle command systems with the optimization of individual and collective Soldier mission performance.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**21**	

Abstract

Future capabilities of battle command systems and networked systems will increase Soldier situational awareness by providing access to information from various networked assets. We conducted a series of experiments at the United States Army Research Laboratory in Adelphi, MD and at C4ISR On-the-move (OTM) at Ft. Dix, NJ. Based on the quality of service of battle command systems, the Soldier will be able to complete his mission objectives with a varying degree of success. Our experiments study the ability of the Soldier to identify various details within a simulated unmanned vehicle sensor feed given a range of quality of service (QoS) (by varying specific network parameters). In addition to understanding these systems from a strictly technical perspective, we are also interested in the performance from a network science perspective. This involves the consideration of the communications, information, and social/cognitive networks and their influence on situational awareness in tactical environments. Specifically, we are interested in the relationship of the Soldier's performance, decision-making ability, and trust in the network in these environments. We identify trends in these metrics as a function of video QoS, which if characterized properly can be used to predict Soldier performance based on the QoS. Further characterization of these relationships may assist in the design of future battle command systems with the optimization of individual and collective Soldier mission performance.

1. Introduction

Battle command systems and networked systems are a critical element of future netcentric architectures in assisting Soldiers to perform their missions. This future capability will allow Soldiers greater access to information from other networked assets including other Soldiers, providing increased situational awareness. Information will be presented to the Soldiers via battle command systems such as Force XXI Battle Command Brigade and Below (FBCB2) and Command Post of the Future (CPOF). We are interested in determining the effectiveness of these systems from several mission performance-related perspectives. The underlying structure of battle command systems is a communication network, which supports a social/cognitive network of Soldiers and their missions. The communications network provides essential Soldier-to-Soldier communications and Soldier-to-battle command systems communications. The instinctual communications network design goal would be to provide full-bandwidth and services to each Soldier at all times in all locations. However, this comes at a price in terms of energy usage and potential information overload to the Soldier. While it is possible to provide such services, we aim to find network design parameters to optimize the mission performance of the Soldiers. In these cases we find that these design parameters are in conflict. Our goal is to maximize Soldier mission performance while conserving energy usage within the network.

Our interpretation of Soldier mission performance is defined by the ability of the Soldier to use available communication network capabilities and accomplish specific mission objectives. In these scenarios, Soldier mission performance is affected by cognitive parameters such as stress levels, cognitive workload, team collaboration, trust in the group, and experience/training. Furthermore, many organizational factors contribute to mission performance such as the Soldier's physical location, the flow of information, in addition to the quality of service of the network. Our studies performed experiments to study the effect of network quality of service in a controlled environment, in which the influence of other factors affecting performance was designed to be minimized.

We conducted human-in-the-loop experiments in multiple settings. Multiple sets of experiments were conducted on civilian subjects at the United States Army Research Laboratory. A set of experiments was also conducted on military personnel as part of the Unified Battle Command Cognitive Impact Study (UBC-CIS) at C4ISR On-the-Move (OTM), held at Ft. Dix. The purpose of OTM is to analyze the performance of current and future tactical network architectures. OTM provides an environment where Soldiers are present to run experiments and provide feedback on their interaction with the networked platforms. An immediate goal of OTM is to assess the networked architectures and determine if the services are sufficient for the Soldier to perform their mission. In current and future tactical scenarios, netcentric operations will possess a great amount of integration of these networked services. Soldiers will interact with these services via a visual display (*i.e.* Rover 5, FBCB2) and their mission objective will be to draw situational awareness and mission pertinent information from these networked devices to fellow Soldiers and his commanders. This information will be sent to commanders or other decision-makers and used to make tactical and strategic decisions (ex. call for fire,

mobilization of troops, situation reports). If the information that is sent to the commander is incorrect, then this may cause a delay or a decrease mission performance with varying consequences. Based on the quality of the networked service, the Soldier will be able to complete his mission objectives with varying degree. The significance of this paper is founded on the expected prevalence of netcentric capabilities in tactical situations. Gaining and understanding of the interactions between humans and network platforms is crucial. Experiments are conducted to measure several Soldier performance metrics and to study the ability of the Soldier to identify various details within a simulated unmanned vehicle video stream given a range of video quality (by varying video bit-rate or error rate).

The result of these tests is a preliminary model that can be used to optimize individual or group mission performance metrics. We consider human trust in networks as a performance metric that can be characterized under varying network quality of service conditions. Other metrics of consideration are decision-making and subject recognition within simulated sensor video feeds. The broader scale outlook of this work involves the merging of the communications, information, and social networks and their influence on situational awareness in tactical environments. Specifically, we are interested in the relationship of the Soldier's performance, decision-making ability, and trust in the network. Further characterization of these relationships will assist in the design of future battle command systems.

2. Related Work

Studies have been conducted to assess similar performance metrics within a variety of situations. We now briefly review some of these works found in the areas of study including: trust in automation, trust in decision aids, situational awareness, and performance in network-centric environments. This paper has elements of each of these fields of study.

In terms of trust, we consider trust models from studies within trust in automation [Lee 2004, Muir 1987, Mayer 1995]. Several models of trust are proposed, identifying dimensions or factors that govern the evolution of trust in automated environments. When considering trust in automation studies, the task is to trust or not to trust the automation device. Specific to the problem that we are investigating, the task is to extract as much information from a decision aid as possible. We introduced a framework for human trust in networks [Chan 2009] that considers network reliability and availability as the main contributing factors of this variety of trust.

Cohen [Cohen 1997, 1998] discusses concepts of trust with respect to decision aids, any automated system designed to assist humans in performing certain tasks. They discuss the designed benefits of decision aids in attempting to manage the uncertainty of certain situations. The performance of the decision aids is measured by temporal scope, reliability and calibration; it is also mentioned that these factors are similar to interactions with other humans. Training of these devices is important in improving mission

performance as it reduces time to identify certain events as well as reduces perceived uncertainty of the information drawn from the decision aid in these scenarios.

Krueger [Krueger 2007] surveys several network centric papers concerning team performance and team situational awareness. Individual situational awareness is well studied [Endsley 2000, Parasuraman 2008], but it is suggested that team performance and situational awareness is a much more complex problem, and one that should be emphasized. Information overload, monitoring of team functions, the impact of stress are noted as areas of potential investigation.

In terms of these topics, we have considered human decision-making and human trust in networks with a series of experiments in simulated tactical environments. We are investigating the effect of the network quality of service on several performance metrics. In the next section, we describe our method of investigation. In Section 4, we detail our testing populations, and in Section 5, we provide some results of data obtained from these experiments. We conclude this paper in Section 6 with some preliminary observations.

3. Methods

The idea of Soldier performance when using networked services within tactical scenarios is a complex problem. The network quality of service can be modeled, but the interaction with humans is multi-dimensional and also varies with each Soldier. Our expectation is that performance metrics will follow the relative quality of service of the network. What is not clear is the behavior of these metrics (i.e. linear, threshold effect) with respect to network quality of service. We created a software application to test our hypothesis by presenting a series of related videos to a test subject and asked several questions based on the video. The participant is briefed on the mission scenario before any videos are viewed (See Appendix A). The participant is a Soldier who is asked to extract specific information from a simulated sensor feed and is responsible for sending the information they gather to their superior, one considered to be in a decision-making position with respect to the information being gathered.

For each video, the mission objective is to identify one of five questions: the quantity of vehicles, quantity of nationals, presence of a blue pickup truck belonging to a known terrorist, quantity of police vehicles, or the identification of any suspicious activity. These are described in further detail in Appendix A. In addition to gathering this information, the Soldier is asked two questions for each video. They are asked to provide their trust and confidence in the accuracy of the information that they are sending to their superior and to evaluate their opinion of the quality of the video clip provided based on their ability to extract information from it. A screen shot of the application is shown in Figure 0.

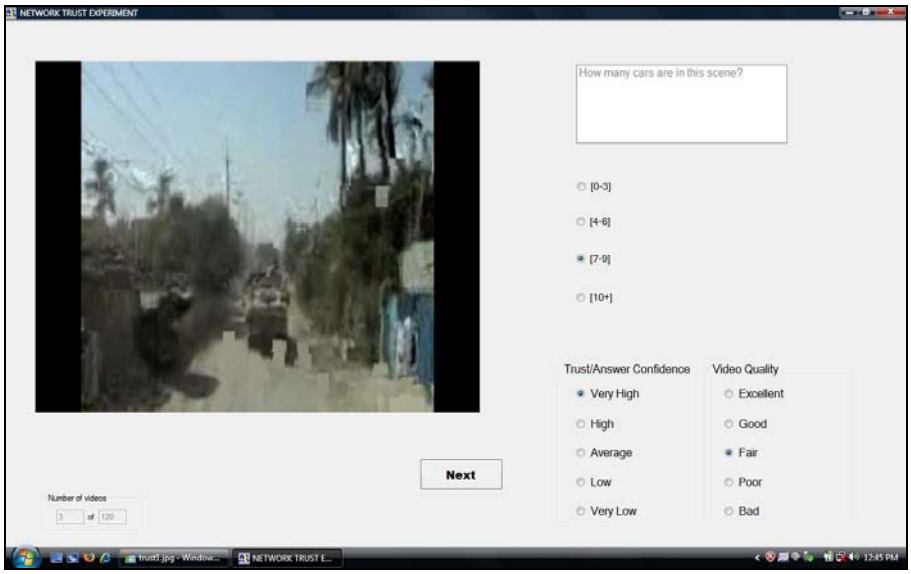

Figure 0. Trust Experiment Screenshot.

We gathered a set of 21 unique video clips from YouTube. We also used the Wireless Emulation Laboratory (WEL) to stream video across the network. Using the `netem` queuing discipline library, various parameters of the links in the network can be controlled such as packet loss, packet delay, packet integrity, and bandwidth. We streamed the video clips across a link in the Wireless Emulation Laboratory [Ivanic 2008] and generated two sets of videos to use for the applications. The first set contained videos with varying packet loss ratios, $\mathbf{E} = \{0\%, 5\%, 10\%, 15\%, 20\%, 25\%\}$, and the other was streamed with several available bandwidths, $\mathbf{B} = \{512, 768, 1024, 1280, 1536, 2048\}$ `bits per second`. The video was streamed at `1024` bps. With these videos with varying quality, we evaluated performance, trust/confidence, decision-making, and video quality perception. We briefly describe the metrics that we are interested in for this study.

3a. Video quality

We base our metric of video quality on the mean opinion score (MoS) [ITU 2007]. This is a subjective scale that varies from 1-5 to indicate an average rating that a video may receive. The range of MoS is typically between 1.5 and 4.5. The MoS is dependent on many factors such as the codec, display size, content, frame rate, and bit rate. While there is no universal standard for measuring MoS for video, this allows us to use the MoS to compare videos with different parameters. A great amount of work exists in video quality perception, where ITU standards can be found describing existing models and approaches [ITU 2002, ITU 2007].

MoS	Quality	Impairment
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly annoying
2	Poor	Annoying
1	Bad	Very annoying

Table 1. Mean opinion score with quality and impairment description [ITU 2007].

For our experiment, we use video that is certainly transcoded multiple times (from original source to .flv format), where the original codecs are not known. Additionally, when streaming the video to insert error, MPEG-TS is used to stream the video with packet loss. With the multiple transcoding steps, even with a presumed error-free source, the MoS would represent an error-free version of the transcoded video, potentially resulting in a lower MoS than the MoS of the original video. We consider the MoS to be a common subjective metric across all videos.

Further, we evaluated the MoS for videos while varying different network parameters. However, we use MoS as the common point of reference. For example, if we have a metric that is a function of MoS, then we can evaluate the metric as a function of any of the network parameters for which we have a mapping from the network parameter to MoS. In our study, we establish a mapping of various metrics as a function of MoS, and then investigate the relationships between these metrics and packet error rate and bandwidth.

3b. Trust/Confidence

We are particularly interested in trust relationships of the soldier to the battle command systems. This is related to the trust in automation or automated device and how they are used to improve performance. The difference in our experiment is that the participant has no alternative method to gather this information. The trust in automation studies allow the

user to choose between using the automation or to manually perform a process. In our experiment, the capability of battle command systems that we examine is the video/streaming. Based on the video quality, we are interested in the dynamics or levels of trust of the Soldier in terms of his responses sent to his superior. With diminishing video quality, we expect for the trust in what the Soldier sends to his superior to decrease. We are interested in observing if the dynamics is a linear or threshold effect.

It has been shown that trust in networks is a function of many factors such as context (mission scenario, mission objectives, collaboration, environment), individual tendencies (preference, training and experience), and time-varying elements (evolution of trust, hysteresis, climate of tactical activity) [Lee 2004, Mayer 1995, Chan 2009, Bowman 2009]. In this study, we have used a single mission scenario and are interested in the dynamics of trust while considering the extent of training and experience and in the context of having varying mission objectives.

Trust in networks is the merging of concepts within the communications and social/cognitive networking domains. We are interested in characterizing the Soldier network trust relationship to identify techniques or approaches to the design of networks to optimize the trust in the network. Trust in networks is a very complex relationship, and the work we present here is a subset of the trust research problem.

3c. Performance and Decision-making:

We are interested in how well the Soldiers are able to extract information from the videos as a function of the MoS, which includes the packet loss rate of the videos. We have measured the accuracy of their responses in the application we developed. We expect the performance of the responses to decrease with increased packet loss ratios.

Additionally, under the question asking to describe any suspicious activity, the response format was open-ended. Therefore, we measured the performance of the Soldier for this question to be the ability (or willingness) of the Soldier to identify anything suspicious. It was possible for the Soldiers not to provide an answer, whether it was due to not being able to see anything or choosing not to provide a response. We also expect this behavior to decrease with increased packet loss ratios. This may be correlated with the ability of a Soldier's decision-making ability.

4. Testing

Our testing of the Trust Experiment involved several separate populations.

1. **23 JUL 2009**: 9 members of the RDRL-CIN-T branch took a 15-minute version of the Trust experiment to evaluate metrics as a function of packet error rate. (dataset: ARL)

2. **3 AUG 2009**: 9 Soldiers (with ranks E5, E6, O4) took a 1-hour version of the Trust experiment to evaluate metrics as a function of packet error rate. This was

administered as part of the cognitive impact survey at the C4ISR On-the-move E09 experiments at Ft. Dix. (dataset: OTM)

3. **4 SEP 2009**: 10 members of RDRL-CIN-T, ARL/CISD took a 15-minute version of the Trust experiment. This test was solely used to construct the relationship between MoS and available bandwidth. (dataset: BR)

4. **20 SEP 2009**: 7 Army Reserve Soldiers took a 15-minute version of the Trust experiment to evaluate metrics as a function of packet error rate. (dataset: RES)

The tests to evaluate the metrics with packet error rates were comprised of sets of six videos. A predetermined random selection of videos was shown with decreasing packet loss rate, 25%, 20%, 15%, 10%, 5%, and 0%. For the entire set of six, one of the following questions was asked:

1. How many cars are in this scene?
2. How many police cars are in this scene?
3. There is a blue pickup in this scene.
4. How many people are in this scene?
5. Describe any suspicious activity.

For the 15-minute version, five sets of six videos were given with one set for each of the five questions for a total of 30 videos. The 1-hour version was four sets of the 15-minute version, with different sets of videos (120 videos in total). The goal of this test was to examine the trust/confidence, video MoS, and performance and decision making metrics as a function of the packet loss rate.

For the test to establish the relationship between MoS and available bandwidth, videos were show in increasing bandwidth, `512, 768, 1024, 1280, 1536, 2048 kbps`. The video was streamed at 1024 bps. This established the MoS as a function of the bandwidth of the video.

5. Results

This section is a presentation of the results from our experiments. Currently, this is the analysis using a limited number of data sets; therefore no statistical analysis was performed. We present these results to suggest trends towards relationships between the Soldiers mission performance, trust in the network, and video perception.

5.1 Composite Results

We can compare the results from the three testing populations. The results of the plots are shown in Figures 1, 2, 3, and 4. We have plotted OTM, ARL, RES and the average metric for each error rate for trust/confidence, mean opinion score, and performance. The results for OTM reflect the 10-hour and the ARL, RES reflect the results for the 15-minute test. The average metric results are the average of each of the population averages. This was used so that the results would not be biased to the OTM data. Each of

the plots reflects 10 or less data sets per point. Therefore, we see these results at suggestions for possible trends, but the lack of data precludes us from drawing any strong conclusions. Inconsistencies in the monotonic nature of the plots may be attributed to this lack of data. However, when more data is collected and these anomalies remain, we would consider further investigation.

We note that the trust and MoS for each of the tested populations are very similar. For the MoS, the scale 1-5 was converted to a scale 0.0-1.0 (1 corresponding to 0.2, 5 to 1.0, etc…) to enable a common comparison with the performance and trust. The trust and MoS decrease as error increases. However, from 20%-25% the trust and MoS increase slightly. This is a behavior seen in each of the populations. In terms of the performance metric, the populations seem to exhibit different results. It is expected that the performance as a function of the error rate would be monotonically decreasing. However the ARL and RES populations exhibit their worst performance at E=0%, increase to its greatest performance at E = 10% and decrease from there with increasing E. For OTM, the performance as a function of error decreases with error (there is a small discontinuity at 5%), but we see a general monotonic relationship with error rate.

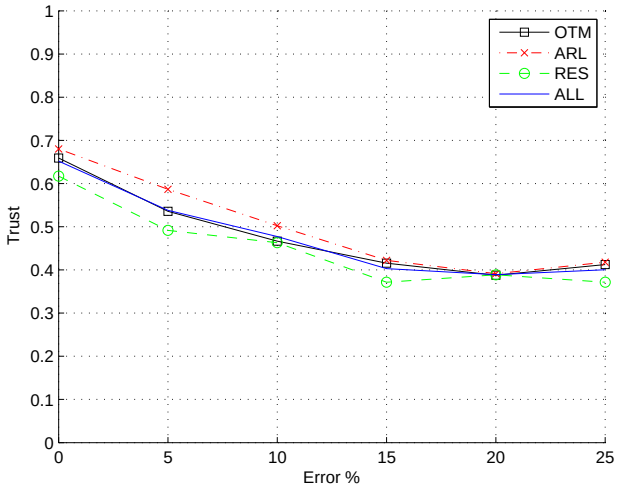

Figure 1. Trust/Confidence vs. Error rate for OTM, ARL, RES and Average.

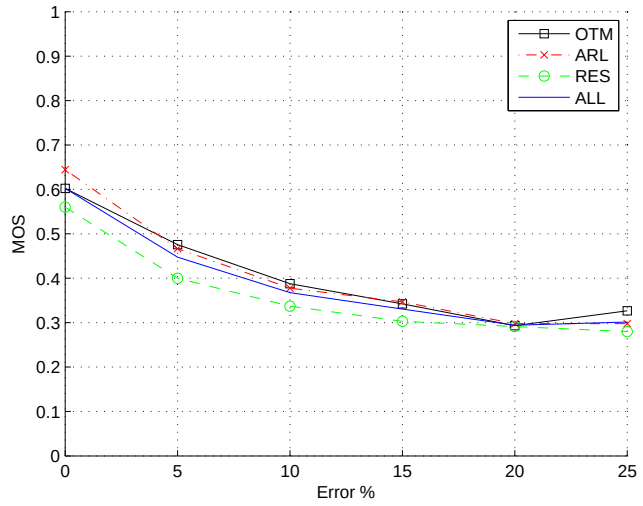

Figure 2. MoS vs. Error rate for OTM, ARL, RES and Average.

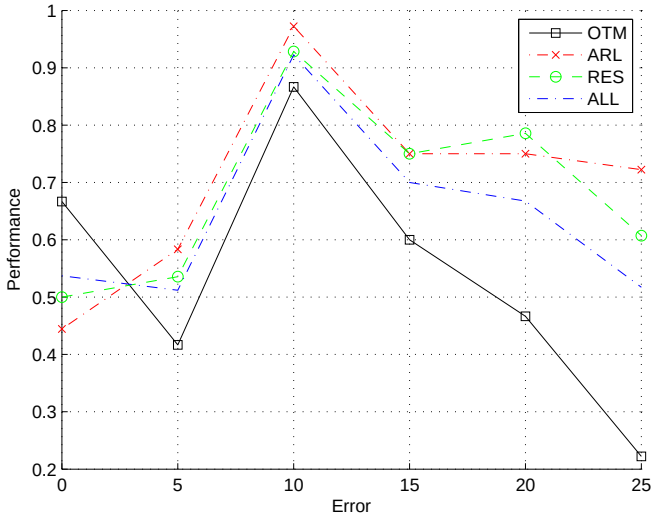

Figure 3. Performance vs. Error rate for OTM, ARL, RES and Average.

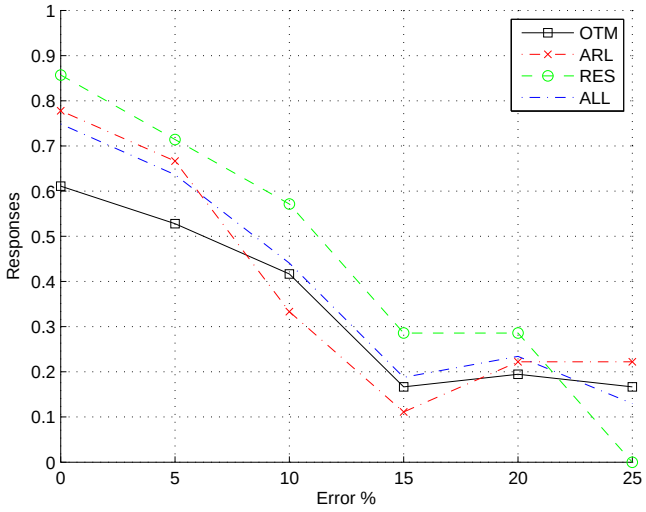

Figure 4. Response of Suspicious Activity vs. Error rate for OTM, ARL, RES and Average.

5.2 Metrics vs. MoS from OTM

Using only the OTM data set, we will further explore several emerging properties from these results. Figure 5 shows the results of the Soldier tests at OTM. Performance, trust/confidence and video MoS are plotted against **E**.

Here, it is seen that the mission performance exceeds the trust and MoS for lower values of **E**. At packet loss ration of 20%, the performance matches that of the trust. At 25% packet loss, the performance matches the MoS. Additionally, the response metric tracks the Trust and MoS metric until E=10%, where it decreases sharply. For MoS, the scale `1-5` was converted to a scale `0.0-1.0` (`1` corresponding to `0.2`, `5` to `1.0`, etc…) to enable a common comparison with the performance and trust. The trust and MoS decrease as error increases. However, from `20%-25%` the trust and MoS increase slightly (where it is assumed that this is due to lack of data). It is expected that the performance as a function of the error rate would be monotonically decreasing. For OTM, the performance as a function of error decreases with error (there is a small discontinuity at `5%`), but we see a general monotonic relationship with error rate. While, we accept that the data suggests trends of these metrics, we expect that these relationships to ultimately be monotonic as a function of **E**.

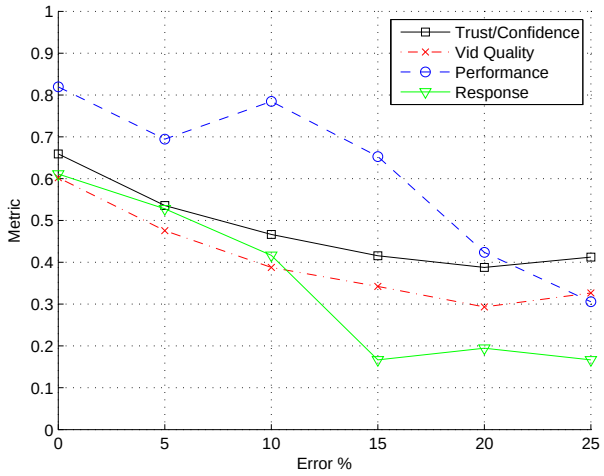

Figure 5. OTM Trust/Confidence, Video MoS, Performance and Response vs. Error rate.

5.3 Approximations of OTM Performance

The empirical results for the metrics contained convexities and non-monotonic properties that we attribute to the lack of data. For ease of data analysis, we approximated the Soldier performance metrics from the OTM data using linear regression techniques. The parameters of the functions were optimized to minimize the mean squared error of the approximation to the experimental data. The approximated functions are in Figure 6, and the equations and error are in Table 1.

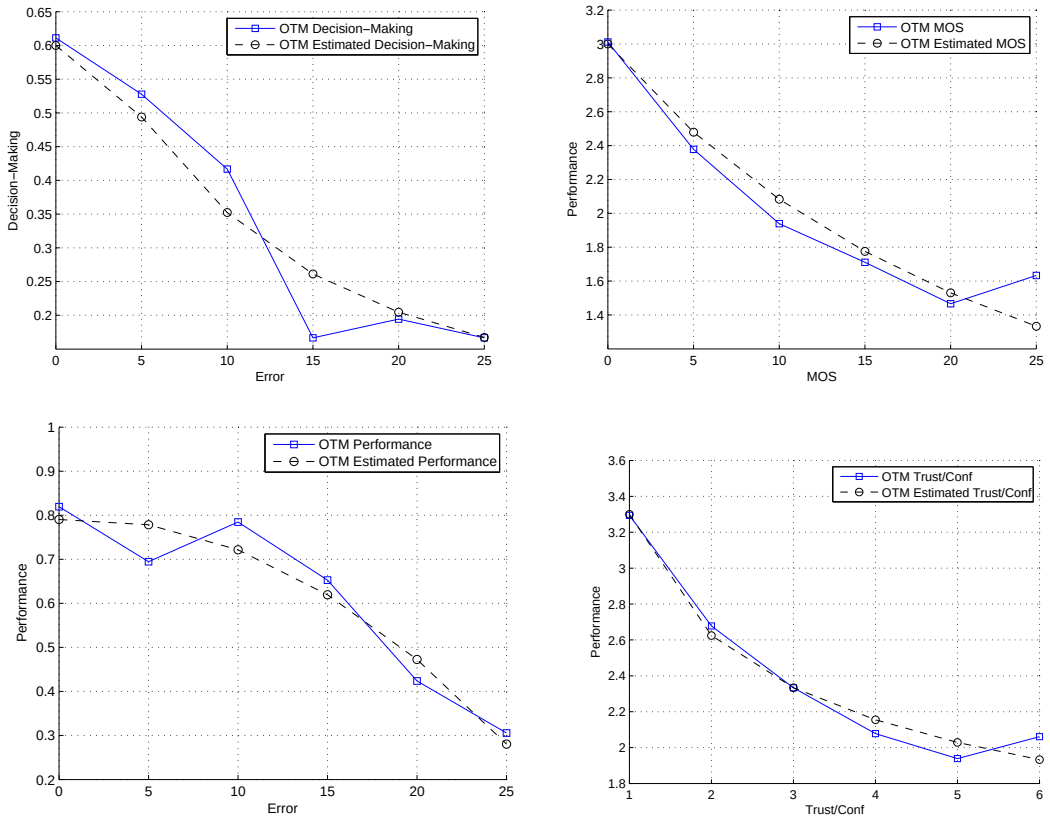

Figure 6. OTM Performance metrics and approximated functions.

Metric	Approximation (ζ = error)	Residual (MSE)
Performance	$0.0009\ \zeta^2 + 0.0021\ \zeta + .7904$	0.0720
Decision-making	$.6/(1+0.19\zeta^2)^{1/2}$	0.1202
MoS	$0.6/(1+0.02\ \zeta)^2$	0.0720
Trust/Confidence	$.66/(1+0.3\ \zeta)^{1/4}$	0.0366

Table 1. OTM Performance approximations and error.

Considering the relationship between error rate and MoS, we can look at the trend of the Soldier metrics as a function of MoS. This is shown in Figure 7. Figure 7 shows the Soldier performance metrics as a function of MoS. The inference that can be drawn from this plot is that for our particular tactical scenario, if the Soldier is provided with UAV stream of a specified MoS, the Soldier performance metrics can be predicted using these relationships. This also suggests that the trust in the information extracted from the video is linearly related to the MoS while the performance increases in a quadratic fashion towards a peak at 0.8. The decision-making ability displays a linear relationship with MoS. The difference between performance and decision-making is a result of the ability to detect the presence of a subject in the scene versus taking action on what is seen. These relationships are plotted using the approximated functions from Section 4.2.

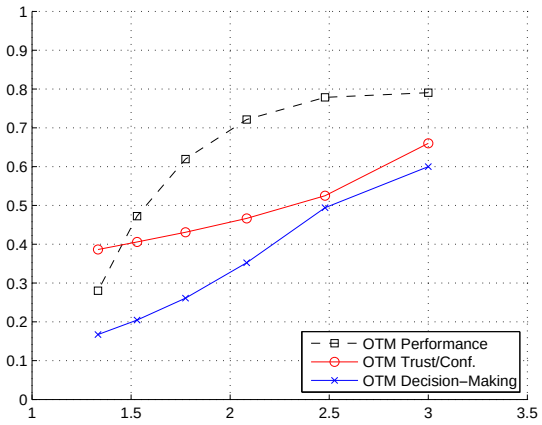

Figure 7. OTM Metrics vs. MoS

5.4 MoS vs. other Network parameters

We have looked at the results of the Soldier performance metrics against the packet error rate and MoS. In this section, we show how it is possible to establish predictions or relationships of the soldier performance against other network parameters. As part of UBC-CIS at C4ISROTM E09, they are interested in determining the minimum bit rate required with which to send UAV streams to send to Soldiers and still maintain acceptable mission performance. This can be shown to predict such performance given an available bandwidth for the video stream.

Using the BR data set, we took the assumption that since the MoS vs. error rate was concentrated about the overall mean for each of the populations, we could determine the relationship between the MoS and available bandwidth and use this relationship with the OTM dataset. The result of the BR dataset is found in Figure 8. A threshold in the MoS is shown around the BW that matches the bit rate at which the video was streamed. Deviations from being exactly at the streamed bit rate are the result of network overhead and other codec-related processes.

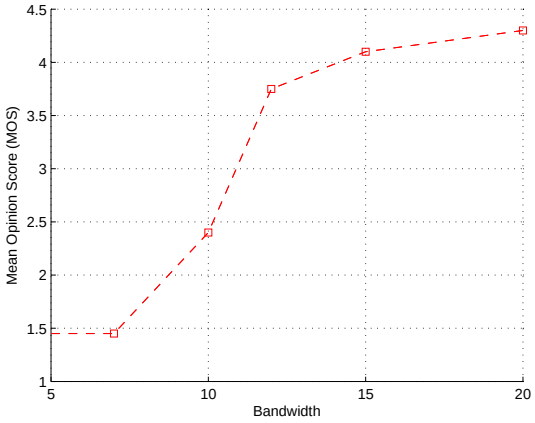

Figure 8. MoS vs. Available bandwidth

Now, this relationship can be used to substitute the x-axis in Figure 7 to compare the performance metrics against the available bandwidth. This is shown in Figure 9. We observe a threshold behavior in the performance metrics around 800kbps.

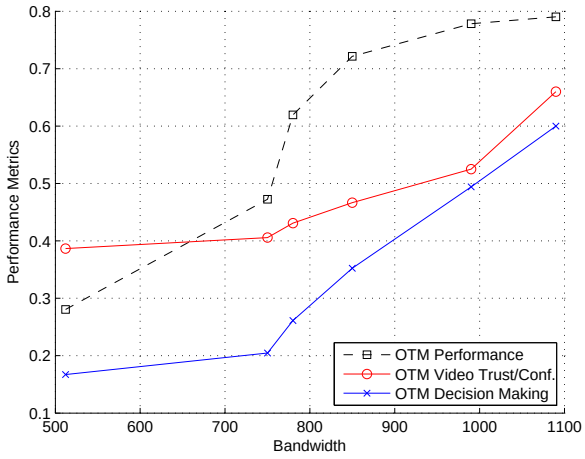

Figure 9. OTM Metrics vs. Available bandwidth

5.5 Observations

Based on the aggregate data (Figures 7, 9), we can establish several inferences from these results. Given the limited amount of data, we consider these to be preliminary assessments. Nonetheless, there are several interesting remarks that are worth noting. We look at the comparison of Soldier performance and Decision-making, Soldier performance and trust, and decision-making and trust.

Soldier Performance vs. Decision-Making: The Soldier-performance and decision-making metrics demonstrate an expected behavior. A diminished performance is expected in mission objectives requiring a greater amount of clarity in the video stream. This is a behavior that is expected, but the relationship between these two levels of information required is not known. Another interpretation of the two metrics is the idea that in the same tactical scenario, more information is required to complete mission objectives than the other, resulting in a diminished performance with respect to quality of service. If mission objectives can be classified into several categories of information required, then their performance could be characterized. Another factor that may affect performance in these cases is the perceived risk. There are mission objectives that have a different amount of risk associated with these information assessments. If there is more perceived risk, then more information will be needed or in these experiments a higher quality of video is required. Perceived risk may range in classifications from simply delaying completion time to putting Soldiers' lives at risk.

Soldier Performance and Trust: For the OTM data, the Soldier performance metric is greater than the trust/confidence metric. This mismatch in trust versus Soldier performance suggests a lack in trust in the simulated sensor feed. This task is more of a recognition of a particular event and not necessarily an assessment on particular detail (this is decision-making) within the video clip. At both ends of the MoS spectrum, it appears that the performance metric and trust are more closely matched than for intermediate levels of MoS. In terms of Lee [Lee 2004], this falls in the region of mistrust.

Decision-Making and Trust: In Figure 7, it is shown that the decision-making metric is lower than trust for lower MoS values, while they are relatively similar for higher MoS values. This suggests an "over trust" characteristic for the decision-making metric. This behavior also suggests that a mission objective with a specific required information or perceived risk can be found that is very closely matched to the trust metric. This is important in the optimization of networks with respect to Soldier performance metrics if the optimization objective is to align trust and performance.

6. Conclusions

We have presented results of a study to analyze Soldier performance metrics with an emphasis on trust in networks. Given a quality of service of the network, we have shown that the Soldier performance metrics behave with various dynamics. This works has shown steps leading towards the characterization of human cognition and perception of networked services in tactical scenarios.

This work is a collaborative effort between engineers and cognitive psychologists, which spans areas of both communication networks and human psychology. These are considered to be first steps towards finding metrics of human cognition that can be related to the design of communications networks. We have considered Soldier trust in networks, performance, and decision-making metrics in a simulated UAV video feed with varying quality of service.

We can draw some emerging results on the dynamics of Soldier trust and performance in a situation with varying network quality of service. From human subject testing, we have seen that the trust in networks or confidence in the information extracted from the network service is linear with respect to the quality of service. Also, experimental results show that Soldier performance decreases when a higher level of detail is required of the video.

Appendix A: MissionScenarioDescription.txt

MISSION SCENARIO

You are an intelligence analyst supporting a vehicle convoy where it is your duty to monitor a streaming video feed and detect specific threats to the convoy along the course of your route. You will be reporting this information to your superior.

There will be a series of videos (around 10 seconds in length) that you will be asked to analyze after each clip.

You have three tasks:

1. Complete the mission objective. For each video clip, you will be asked to perform one of the following objectives:

    * The route of the convoy is a new route, where IEDs are a strong possibility. Identify the presence of the location of possible IEDs along the route (out of place objects, suspicious vehicles, disturbed soil, etc).

    * Intelligence is attempting to obtain specific information on the demographics of the neighborhood the convoy is driving through. Identify the number of vehicles you are able to see.

    * Intelligence is attempting to obtain specific information on the demographics of the neighborhood the convoy is driving through. Identify the number of people you are able to see.

    * Local insurgents have also been impersonating law enforcement officials and their vehicles. Identify any observed law enforcement vehicles to your superior.

    * Intelligence reports that a wanted terrorist has been spotted along the route of the convoy. He has been spotted driving a blue pickup truck. Report the observation of any blue pickup trucks on the route.

2. Provide your trust and confidence in the accuracy of the information that you are sending to your superior.

3. Evaluate your opinion of the quality of the video clip provided based on your ability to extract information from it.

When you have read and understand your mission objectives, click the box below and Click 'Next' to begin the experiment.

Appendix B: ScenarioQandA.xml

```
<?xml version="1.0" encoding="utf-8"?>
<ScenarioQandA>
  <Question>
    <QuestionID>1</QuestionID>
    <QuestionStr>How many cars are in this scene?</QuestionStr>
    <QuestionType>MC</QuestionType>
    <AnswerSet>
      <AnswerStr>[0-3]</AnswerStr>
      <AnswerStr>[4-6]</AnswerStr>
      <AnswerStr>[7-9]</AnswerStr>
      <AnswerStr>[10+]</AnswerStr>
    </AnswerSet>
  </Question>
.
.
.
  <Question>
    <QuestionID>5</QuestionID>
    <QuestionStr>Describe any suspicious activity.</QuestionStr>
    <QuestionType>MW</QuestionType>
    <AnswerSet>
    </AnswerSet>
  </Question>
  <Scenario>
    <VideoID>AMBUSH_V15_E25</VideoID>
    <QuestionAnswer>
      <QuestionID>1</QuestionID>
      <AnswerStr>[0-3]</AnswerStr>
    </QuestionAnswer>
  </Scenario>
.
.
.
  <Scenario>
    <VideoID>AMBUSH_V15_E25</VideoID>
    <QuestionAnswer>
      <QuestionID>1</QuestionID>
      <AnswerStr>[0-3]</AnswerStr>
    </QuestionAnswer>
  </Scenario>
</ScenarioQandA>
```

Bibliography

[Bowman 2009] E. Bowman, “Human Trust in Networks,” 14th International Command and Control Research and Technology Symposium, Jun. 2009.

[Chan 2009] K. Chan, N. Ivanic, B. Rivera, E. Bowman, “A General Framework of Human Trust in Networks,” 14th International Command and Control Research and Technology Symposium, Jun. 2009.

[Cohen 1997] Cohen M.S., Thompson, B., and Freeman J., Cognitive aspects of automated target recognition interface design: An experimental analysis. Arlington, VA: Cognitive Technologies, Inc., 1997.

[Cohen 1998] Cohen, M. S., Parasuraman, R., & Freeman, J. T. (1998, July). Trust in decision aids: A model and its training implications. Proceedings of 1998 Command and Control Research and Technology Symposium, Monterey, CA, 1998.

[Endsley 2000] Endsley, M. and Garland D., Theoretical Underpinnings of Situation Awareness: A Critical Review. Situation Awareness and Analysis and Measurement. Mahwah, NJ: Lawrence Erlbaum Associates, 2000.

[ITU 2007] ITU-T Recommendation G.1070 (4/2007), online: http://www.itu.int/rec/T-REC-G.1070-200704-I/en

[ITU 2002] ITU-R BT.500-11, online: http://www.itu.int/md/R07-SG06-C-0150/en

[Ivanic 2008] Ivanic, N.; Rivera, B.; Gopaul, R.; Luu, B.; Gwyn, D.; Hardy, R.; Marcus, K.; Scott, L.; Tran, G.; Nguyen, B., “A scalable testbed for emulating wireless Mobile Ad-hoc Networks,” Military Communications Conference, 2008. MILCOM 2008.

[Krueger 2007] Krueger, Gerald P.; Banderet, Louis E. “Implications for Studying Team Cognition and Team Performance in Network-Centric Warfare Paradigms,” Aviation, Space, and Environmental Medicine, Volume 78, Supplement 1, pp. B58-B62(1), May 2007.

[Lee 2004] Lee, J. and See, K. Trust in Automation: Design for Appropriate Reliance. Human Factors, Vol 46, No. 1, pp. 50-80, Spring 2004.

[Mayer 1995] Mayer, R. C., Davis, J. H., & Schoorman, F. D., “An integrative model of organizational trust.” Academy of Management Review, 20, 709–734, 1995.

[Muir 1987] Muir, B., and Moray, N., “Operator’s trust in relation to system faults,” IEEE International Conference on Systems, Man, and Cybernetics, 258-263, Alexandria, VA, 1987.

[Parasuraman 2008] Parasuraman, R., Sheridan, T., Wickens, C., “Situation Awareness, Mental work load, and trust in automation: viable, empirically supported cognitive engineering constructs,” Journal of Cognitive Engineering and Decision making, vol. 2, no. 2, 2008.

[YouTube 2009] Ambush, online: http://www.youtube.com/watch?v=Rxx1Lo8fZwQ, http://www.youtube.com/watch?v=rVGyQvvg-9c