14th ICCRTS

"C2 and Agility"

Title of Paper: **Human Trust in Networks**

Topic(s)

Topic 1: C2 Concepts, Theory, and Policy

Elizabeth K. Bowman

Point of Contact: Elizabeth K. Bowman

Name of Organization: ARL-SLAD

Complete Address
B. 390-A
Aberdeen Proving Ground, MD 21005

Telephone: 410-278-5924

E-mail Address: ebowman@arl.army.mil

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Human Trust in Networks	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) **Army Research Laboratory,ARL-SLAD,B. 390-A,Aberdeen Proving Ground,MD,21005**	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
In Proceedings of the 14th International Command and Control Research and Technology Symposium (ICCRTS) was held Jun 15-17, 2009, in Washington, DC

14. ABSTRACT
see report

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**33**	

Human Trust in Networks

Abstract

The topic of human trust in a warfighting network is one that has many implications for the future of network enabled operations in military Command and Control (C2). In this paper we review the concept of trust and discuss relevance for networked operations. We also document results from an exploratory study of human trust in the technical components of a tactical network. A prototype mobile ad hoc network (MANET) was used to simulate an Intelligence, Surveillance, and Reconnaissance (ISR) field exercise with 39 Soldiers. A prototype survey was developed to examine the components of trust in the technical aspects of this network, and was administered daily. A principal components analysis with a Varimax rotated solution was conducted to investigate the major components of the survey questions. Four factors were extracted with significant loadings. This examination was a valuable first step in understanding how human trust of a tactical network can be measured and how we can use this information to improve networked performance. We identify areas of future research that can expand our understanding of how humans and networks interact to form trusting relationships. We review relevant papers from the 2008 13th ICCRTS that provide valuable assistance in determining a path forward.

Introduction

Networked communications are becoming ubiquitous on the battlefield; Soldiers are becoming reliant on the rapid availability of information that network connections provide to every echelon of command. Networked battle command systems are not new to the higher, less mobile, levels of C2; it is the devolution of the network to the tactical echelon that makes the Network Centric Warfare (NCW) implementation problematic (Taylor, 2005). The tactical commands will depend on mobile ad hoc networks (MANET) that have different physical and performance characteristics than local area networks (LAN) used by stable higher commands. Some of the problems associated with communications moderated by MANETs include disruptions and bandwidth constraints. Information warfare attacks will also play a role in network delays and outages, but it is the physical constraints that are having the most impact in recent campaigns. In his analysis of the Operation Iraqi Freedom (OIF) 2003 Thunder Run (where lead elements of the 2nd Brigade, 3d Infantry Division attacked Baghdad from the southern outskirts, through the city and west to the airport, Conner (2005, p. 15) noted that carrying the “robust intelligence capability [through a common operating picture] forward to the tactical level would prove almost completely lacking” (p.18). He characterized the existence of a ‘digital divide’ between operational and tactical commands, and suggested that the reasons for this divide were the great distances covered by tactical units and the vast amount of data attempting to be shared. Conner notes several examples in the early phase of OIF where “the promise of technology providing

near perfect situational awareness had failed the tactical commander" (p. 20). MANET services and capabilities are certain to improve as technologies are developed to overcome existing constraints, but the lesson of performance degradations drove our interest in understanding how Soldiers might develop and maintain trust in a tactical network. This interest includes both the human-human and the human-technology interactions that occur in networks. However, in the case of the former, we are considering the case where the human-human interaction is conducted through applications (voice, text) supported by a network.

This interest was driven by our research in network science and our realization that cross-discipline efforts are needed to advance knowledge. Figure 1 shows a simple cross-sectional view of a network divided into the physical, communication networks, information, and social/cognitive layers (Swami & Bowman, 2008). In this diagram, each layer contains descriptions of supporting technology or human behavior existing in that layer. The arrow connecting the layers suggests that each layer cannot exist in isolation but depends upon other layers for inputs or actions. For example, a sensor existing in the physical layer would detect an object in the environment and send an image that would be routed through the communication network to an operating system supported by the information layer; this image would be viewed and acted upon by an operator who would act upon this information in the social/cognitive domain.

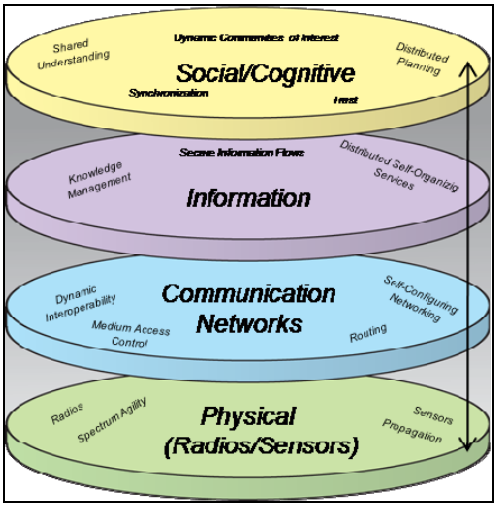


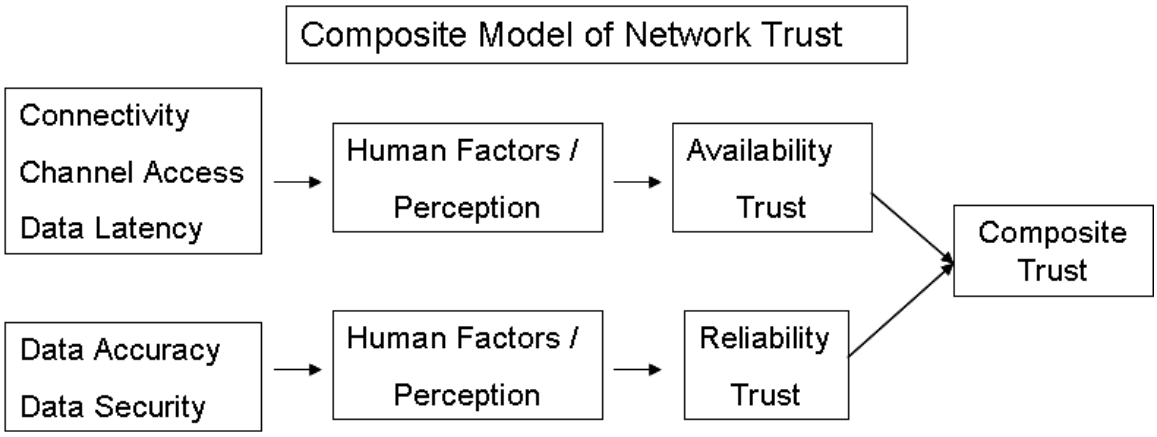
Figure 1 Physical, Communication Networks, Information, and Social/Cognitive Levels of a Network

Trust is a multidimensional concept that has a developmental component (Corritore, Kracher & Wiedenbeck, 2003; Mayer, Davis & Schoorman, 1995; Riegelsberger, Sasse & McCarthy, 2005). Trust is an integral factor in social groups; it facilitates cooperative team behavior and exchange of resources and serves to reduce uncertainty (Lee & See, 2004). Trust has also been widely discussed in the automation literature and is understood to be a predictor of system use,

appropriate reliance on automation, and strategies for system use (Atoyan, Duquet & Robert, 2006; Jian, Bisantz & Drury, 2000; Corritore, Kracher & Wiedenbeck, 2003; Parasuraman, Sheridan & Wickens, 2000). This literature identifies several dimensions of trust. Corritore et al. (2003) propose a model that identifies the existence of external factors that impact the perception of an actor's perspective of the credibility, ease of use, and risk associated with the object of trust. Riegelsberger et al. (2005) suggest that the introduction of new technologies leads to novel forms of interactions between users and technologies that require trust. The need for users to develop trust in the interaction with new technology poses a prime concern for system developers, the authors argue. This literature consistently suggests that trustworthiness is not a stable attribute but is determined by the situation in which the trust actor and the object of trust exist.

The conceptualization of the tactical network into the physical, communication, information, and social/cognitive domains provided us with a perspective with which to approach the concept of trust in networks from the point of view of the human user. This user may be expected to have several targets for trust. Certainly, the user would have to trust the individuals and team members with whom he communicates indirectly through the communication medium (radio, battlefield operating system), given that these team members are distributed in space, making face to face interactions unlikely. Underlying that human-human level of trust would be human-technology trust. An example of this would be the human actor's belief that information (text, audio, sensor images) sent over the transport layer and received in the application domain was valid, timely and complete.

In this experiment, we attempted to focus on the development of trust on the part of human actors as they interacted with applications and services provided by a network architecture. We were not examining how the humans developed trust in others, or the automation tools *per se*, but were attempting to identify how humans developed trust in the network architecture that made possible communication and visualization services (such as blue force tracker). The object of that trust was information obtained through a mobile ad hoc network. *A priori*, we conceptualized human trust in this network as the composite relationship of the network's availability and reliability to the user over time (Chang, 2008). Factors contributing to network availability may include connectivity, the number of servers, hops required, security/access control, channel access, routing protocols, network traffic, data latency, and node density. Factors affecting reliability may include data accuracy (synchronization of servers, current data), and data security (data integrity, authentication, validation). It is intuitive that human trust in a network would degrade as network failures increase. However, the function of these degradations is not known. Trust could degrade gracefully or there could be a threshold effect where trust remains stable until a destabilizing incident occurs. Figure 2 shows the process of composite trust.



Source: Kevin Chan, 20 March 2008 personal communication.

Recently, we conducted an initial investigation of the relationship between network performance and human trust of applications provided by that network. Our results provide insight into this large challenge and, more importantly, identify specific research questions for future exploration. The Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR) On The Move (OTM) July 2008 Cognitive Impact Study provided an opportunity to explore the concept of human trust in relation to a prototype MANET (Bowman and Thomas, 2009). The experimental MANET architecture supported two platoons operating as dissimilar units with shared unmanned air and ground vehicles and sensors. The network supported an enhanced Force XXI Battle Command Brigade and Below (FBCB2) common operating picture that was available to Soldiers in vehicles and on dismounted displays. Soldiers could communicate in several ways over the MANET; by voice via radio, and by text or instant messaging via FBCB2. Additionally, blue force vehicles and dismounted position reports were visible on FBCB2 to allow users to monitor visual cues about positions of own forces. Spot reports of opposing forces were also visible on this display.

We administered a survey of trust in network at the conclusion of daily trial runs. The two platoons were identified as the Spin Out (SO) and the Future Combat System (FCS) Platoons. The first was organized to represent a legacy or current force unit equipped with advanced technologies (as add-on equipment) and the second was organized to represent a platoon with integrated advanced technologies that might be used by future forces.

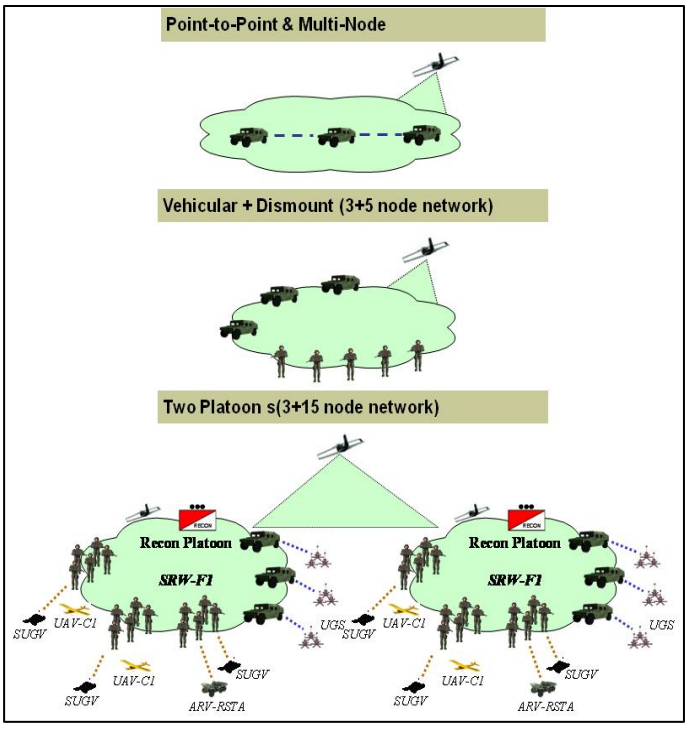
Procedures

Exercise Tasks and Goals

This field exercise was organized to test a developmental MANET architecture that integrated sensor technologies with a battle command display provided to 39 mounted and dismounted Soldiers. These Soldiers were organized into two reconnaissance platoons and a Company Headquarters element. Each

platoon was equipped with mounted and dismounted communications, battle command devices, and a number of dismounted ISR sensor collection devices. Additionally, each platoon benefitted from higher echelon ISR tools to include Unmanned Ground Sensors and several Unmanned and Manned Aerial Sensor platforms. These Soldiers operated against a live but scripted Opposition Force (OPFOR). The two platoons used a different communications architecture meant to replicate a current force and future force network configuration. The platoons were able to communicate with each other by a satellite link that connected the two platoon networks.

The two platoons operated in separate test sites as though they were independent, but supporting, organizations. They were separated by approximately 1.5 miles. On each trial run, the platoons traveled to their respective test site and dismounted to perform ISR activities. They were charged with completing Priority Intelligence Requirements (PIR) of OPFOR activities. Two Soldiers (the Platoon Sergeant and the Radio Operator) remained with the vehicles to monitor the enhanced FBCB2 display and manage PIR text messages and spot reports between the dismounted Platoon Leader and the Company Commander. The dismounted Soldiers were expected to observe the OPFOR and report known activity. Dismounted Soldiers used unmanned ground and air vehicles to aid these observations. They were to report OPFOR activity through voice (radio) or text communications and could also send messages on annotated images from the unmanned vehicles through a remote video terminal.



The supporting network architecture is shown in Figure 2. There were several levels of network connectivity. A point-to-point and multi-node network was used to connect the vehicles and was supported by an aerial relay node. Each of these vehicles also acted as a gateway for the dismounted Soldiers associated with that vehicle (e.g., a squad). If the dismounts got out of a specific range of the vehicle, their connection to the network would be broken, but they could re-establish this connection if one Soldier returned to the network vehicle range. This provides an example of how important it is for network users to understand the physical properties of the network. The lower image shows the entire connection for each platoon with its unmanned assets and the connecting aerial relay node.

Figure 2 Network Configurations

Survey Instrument

We adapted a survey of trust in automation developed by Jian, Bisantz, and Drury (2000) and tailored 15 questions to describe elements of factors we hypothesized would impact human trust in networks. Again, our focus was on the trust that Soldiers placed in the network architecture itself or the services that were provided by that architecture. We believed that those services (such as the blue force tracker visualization of FBCB2) would be impacted by network performance. Examples would be latency of blue icons resulting in stale images of blue force locations or delayed message transmissions. These questions were scored on a 7-point scale (1 = strongly disagree and 7 = strongly agree). This survey was administered at the conclusion of each day's mission, and is shown in Table 1. We were interested in several aspects of the network. The first seven questions address services supported by the network (voice, FBCB2) from the perspective of the user as an active user of the network. In question 6, we asked if others requested retransmission of messages because the original sender might not be aware if messages were successfully received. Questions 8-14 address general perspectives on the network as an entity. The last question that queried familiarity with the network was included because we thought users who were familiar with the network components and network performance might tend to be more trusting of the network.

Trust in Network Questions.
1. I was able to access services on my display
2. I am confident that I received all the communications meant for me.
3. I was able to send communications.
4. I could communicate with others in my platoon.
5. I was able to open sensor images on my display with no delays.
6. People asked me to resend images or messages.
7. The network's services supported the mission.
8. The network services were reliable.
9. I am confident in the services provided by the network.
10. The network is secure.
11. The network had integrity.
12. The network is dependable.
13. The network is reliable.
14. I can trust the network.
15. I am familiar with the network.

Table 1 Trust in Network Survey Questions.

Experiment Limitations

Two caveats are needed prior to describing the analysis. During the execution of the exercise, two issues arose with the technologies and the network. While these were useful for purposes of documenting technical performance of MANETs in field conditions with mobile nodes and variable bandwidth requirements, they impacted our investigation of trust in the network between two similar platoon organizations. The first concerns the differences in technologies assigned to the platoons; the second concerns information warfare attacks. The platoons used different prototype technologies for intra-squad dismounted communications (Bowman and Thomas, 2009, in press). These different communication and technology structures were

designed to replicate a current force ([SO platoon) and future force (FCS platoon) organizational structure. In the former, technologies were provided to Soldiers; in the latter the technologies were integrated into the network. For example, each platoon was provided an unmanned ground vehicle (UGV) that was tele-operated. The operator could view streaming video and create a still-image to share with others as needed. In the case of the SO platoon, this image could not be shared 'in the network' but would only be visible to other Soldiers watching over the shoulder of the operator. In the case of the FCS platoon, the UGV operator could take the image and send it to others electronically through the FBCB2 system because the UGV platform was integrated into the FCS network.

Consistent with the current/future force distinction between the platoons, each was equipped with different organic radio communications. The FCS Platoon was equipped with next generation digital Soldier Radio Waveform (SRW) radio system, while the SO platoon was equipped with an improved version of the currently fielded Enhanced Position Locating Reporting System (EPLRS). The improved version of EPLRS used in this exercise supported both voice and video communications which the currently fielded version does not.

While the SO platoon did not have the integrated capabilities provided to the FCS platoon, their simpler technology structure had the unintended effect of less platform breakdowns and less network disruptions. For instance, in the example described above of the UAV operator sending an image through the network, this required substantial bandwidth capabilities. Additionally, some of the prototype technologies used by the FCS platoon did not perform as hoped. Again, this was understandable and useful for system developers, but this led to an unexpected difference between platoons. Fortunately, redundant voice communications provided to both platoons allowed the FCS platoon to maintain operations when futuristic technologies malfunctioned.

The second caveat concerns the use of information warfare (IW), or Computer Network Operations (CNO) attacks that were planned for both platoons. The goal of this experiment was to determine how Soldiers were able to detect and respond to IW attacks. To simulate a vehicle that had been captured by enemy forces, the CNO analysts were provided an instrumented HMMWV that was affiliated with the FCS platoon. This was an arbitrary decision; they could have just as easily been assigned to the other platoon. The intention of the CNO analysts was to attack each platoon equally.

Unfortunately, network latency (delay) in traffic passing between the SO (EPLRS) network to the FCS (SRW) network was so high that many attacks targeting the SO platoon took too long to be effective in the dynamic live environment. Thus, the CNO attackers chose to focus primarily on the FCS platoon. For example, a single ping from the CNO team to the SO network sometimes took as long as 17 seconds for a return response. Generally responses less than 2 seconds are needed to allow for successful network intrusion operations to occur. When delays were longer than 2 seconds, the CNO team was forced to focus on fewer nodes thus reducing the

effectiveness of the attacks. [1] Thus, the FCS Platoon became the focus of the CNO analysts' IW attacks, with the SO platoon being unaffected.

We further acknowledge the tenuous sample size used in this analysis and do not attempt to make generalizations of these findings.

Results

Prior to analyzing the survey results, we explored the reliability coefficient and factor structure of the survey tool. We first computed a Cronbach's alpha reliability test of the survey. The reliability coefficient was .859 with all 15 items included in the analysis, suggesting an acceptable level of reliability. Examination of the inter-item correlations showed generally high correlations, suggesting that the survey measured a single uni-dimensional latent construct (Stevens, 1996).

Following the reliability analysis, we conducted a Principal Components Analysis (PCA). PCA is one "variable reduction scheme" (Stevens, 1996, p. 362) that allows one to determine the number of underlying constructs that are represented by a number of items in a scale. Factor analysis is a similar empirical approach; both PCA and factor analysis use linear combinations of original factors to derive a pattern of correlations (Stevens). Stevens suggests that PCA is psychometrically sound; it is simpler in a mathematical sense, and yields similar results to factor analysis (p.363). The approach used in this paper is an exploratory analysis where we are attempting to determine the number of underlying factors, decide whether or not the factors are correlated, and aspiring to name the factors based on the components. To conduct this analysis, we used the Statistical Package for the Social Sciences (SPSS, version 15). The PCA partitions the total variance (which is the sum of all variances for the 15 variables) into the linear combination that accounts for the most variance; this is the first principal component. The analysis continues until all variance is accounted for in the components, which are uncorrelated with each other. Once the components are identified, they are interpreted by examining the factor loadings that represent the component-variable correlations. Table 2 shows the factor

[1] The challenge of attacking the SO platoon for the CNO team was discovered during the trial runs when the network traffic was the highest. The CNO team operated from a vehicle equipped with SRW communications. This enabled them to be part of the SRW environment and facilitated their ability to attack the FCS platoon. To reach the SO platoon, the CNO team had to traverse the SRW network, go through a satellite communication (SATCOM) link, through a digital to analog translation software service, and then a second SATCOM link. Each of the SATCOM links had quality of service settings for message delivery and message queues. The majority of the messages that traversed the SATCOM link were "guaranteed" delivery messages. Messages like spot reports, image requests, etc. were all guaranteed to be delivered. The importance of guaranteed message delivery is; as guaranteed delivery messages were sent by both platoons they waited in the message queue to be delivered. This delayed the delivery of the CNO attacks because the queue operated as a first in first out system.

loadings for each of the original 15 variables. The red boxes show the highest correlations that determine the factor loadings. The components were named by examining the component loadings. For example, the factor 'communications' was so named because it is comprised of the questions: "Confident I received all communications meant for me", "Able to send communications", and "I could communicate with others when needed." In Table 2, the underlined correlations were disregarded because they represented weaker correlations of the factor to the component.

These four components explain a total of 77.12% of the variance in trust in the network. Individually, the components account for the following variance: component 1 (*dependability*): 39.6%, component 2 (*reliability*): 18.05%, component 3 (*communications*): 10.95%, and component 4 (*access*): 8.51%. In summary, the components account for much of the available variance in the construct of trust in the network. Future analysis will attempt to identify missing elements of the construct.

Using the results of the PCA, we combined data elements to create four summary items from the original 15 questions. That is, we combined items 10 through 15 to create the summary factor "*dependability*", we combined questions 6 through 9 to create the summary factor "*reliability*", we combined items 2 through 4 to create the summary factor "*communications*" and we combined items 1 and 5 to create the summary factor "*access*". The summary factors also are identified by the red boxes in Table 2. We recomputed data variables using these summary factors from the surveys that were administered on the first and last days of the experiment. We compared these factors between the two platoons and between the days of survey administration. We were interested in these comparisons to determine if the technologies used by each platoon impacted their trust in network scores and to determine if time impacted these scores. We conducted repeated measures Analysis of Variance (ANOVA) to explore these differences for this measure of trust in networks.

The survey was administered on four days. The first and last days are presented in this analysis due to problems with missing data on the intervening days. 29 responses were received on the first trial; 27 on the last. 39 Soldiers were asked to complete the surveys. The problem of missing data was due, in large part, to the distributed nature of the exercise. The Soldiers were organized in dismounted squads and at vehicle rally points that were separated by 200 meters. We attempted to position one data collector with one group of Soldiers to administer surveys. The dismounted squads were very mobile, and it was difficult to maintain this ratio of data collectors to squads (in some cases, the squads divided and moved apart). To ensure data validity, we decided that if the data collectors could not administer the survey within 15 minutes of the end of the experiment the survey was not administered.

Table 2 Rotated Component Matrix of Survey Questions

		Component			
		1	2	3	4
		Depend	Reliable	Comms	Access
1.	Ability to access services on display	.085	.312	.089	.786
2.	Confident I received all comms meant for me	.074	.240	.844	-.004
3.	Able to send comms	-.012	.571	.643	.036
4.	I could communicate with others when needed	.320	.184	.587	.210
5.	Able to open images w/ no delay	-.107	-.005	.045	.857
6.	Others asked me to resend images or messages	-.151	.604	-.561	.138
7.	The network supported the mission	.124	.865	.250	.074
8.	The network's systems were reliable	.253	.837	.172	.161
9.	I was confident in the services provided by the network	.237	.843	.223	.186
10.	The network was secure	.910	-.055	.076	-.170
11.	The network has integrity	.889	.014	-.018	-.146
12.	The network was dependable	.877	.107	.254	.105
13.	The network was reliable	.790	.284	.318	.268
14.	I could trust the network	.765	.397	.141	.069
15.	I am familiar with the network	.585	.245	-.151	.468

Note. Extraction Method: Principal Component Analysis.

Repeated measures analysis of variance was used to explore differences in platoon network trust ratings between the first and last days. We used the four composite items explained above in the analysis. The data showed a significant difference between overall ratings for the first (day 1) and last (day 2) day, (*Wilk's* λ F (4,16) = 4.98, p =.008). The source of this difference was located between the platoons in the rating of the factor *dependability*. This factor included the questions of security, integrity, dependability, reliability, trust, and familiarity. The platoons differed significantly on their ratings of this factor (*Wilk's* λ F (1,19) = 7.58, p =.013). The average mean scores for both days for the SO and FCS platoons were 3.88 and 2.49. The trend lines in Figure 1 show that ratings declined for both platoons during the experiment. For the SO platoon the mean score declined from 4.20 to 3.56. The respective mean scores for the FCS platoon were 2.76 and 2.21. The comparatively lower scores for the FCS platoon reflect the CNO attacks and the poor communication device performance mentioned above. These scores also demonstrate that neither platoon had high ratings of the network's dependability; this reflects the prototype nature of the MANET. The declining scores are also a function of the problems associated with maintaining the MANET over time in various field conditions (open and forested areas).

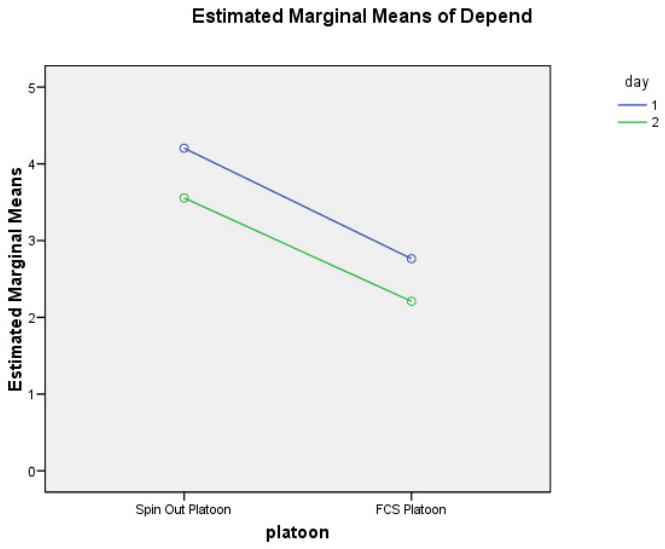


Figure 3 Comparison of SO and FCS Platoon Ratings of Network Dependability

Future Research

These results led us to ask questions that may be addressed by future research. We reviewed the papers submitted to the 13th International Command and Control Research Technology Symposium (ICCRTS), sponsored by the Command and Control Research Program (CCRP) to

determine if leading researchers in this C2 community of interest could offer relevant and interesting perspectives on our areas of interest. Interested readers can access these papers at the CCRP website: http://www.dodccrp.org/.

These three questions address the conceptualization of the network by the users, the impact of collaboration on the formation of trust in networks, and the process by which trust develops in a network.

Question 1: How do users of a network conceptualize this network?

In this exploratory study, we were interested in exploring in more detail how users conceptualize the "network". In our experience, Soldiers tended to view the network as the overall enabler of information sharing, but did not necessarily understand the architectural configurations. One helpful description of the network component parts was provided by Desouza, Roy, and Lin (2008), in which the authors examined information flows from the technical, social, and socio-technical dimensions. The authors identify useful social network measures that impact information transfer in the physical domain. For example, they suggest that the quality of information transfer in the network is a function of actors, channels, context, and information. Each of these is described in the following way. Actors are defined to be sources and recipients of information, and are subject to influence, trustworthiness, authority, positions and roles in the transfer process. Channels and context relate to the entire network and are defined by distance and density of the network nodal structure. Information can be distorted or delayed (Desouza, et al., 2008, p. 12). This research is useful for our research in human trust in networks in that it provides a bridge for possible performance metrics that relate physical performance metrics to relevant social measures.

Another effort that reports an attempt to bridge the physical and cognitive/social networks is the Uruguay et al. (2008) report on the Brazilian tool, C2OLISEU (from the acronym, in Portuguese, for Concepts for Operational Applications and Systems Engineering). These authors specify concepts within each of the network centric domains that can serve to assist researchers in conceptualizing each domain. For example, Uruguay et al. suggest the social domain is defined by 'role' and 'relationship' concepts; the cognitive domain is defined by 'belief' and 'goal' concepts. The information domain would include, among other concepts, 'operational nodes', 'data', and 'links'. The physical domain concepts include 'objects' and 'energy'. The authors provide examples of linkages across domains, for example, they note that "a *role* "is a set of constraints a given entity must accept in order to become a member of an organization…These constraints can be expressed as *goals*, which the organization expects the *node* to achieve (p. 9). These concepts suggest possible measures for investigating trust in networks among the technical, social, and socio-technical domains.

Question 2: How is trust impacted at the tactical level by collaboration?

Hudgens & Bordetsky (2008) report on an investigation of feedback loops with reciprocal resource commitments to provide greater trust and commitment in crisis response groups. The use of the crisis response context is particularly relevant because these groups have shared, complimentary, and competing goals and constraints, much like tactical organizations on the battlefield. The authors suggest that networks form in a crisis situation through resource

commitment and collaborative communication and that these serve as signals of trustworthiness to organizations engaged in the response. They hypothesize that "reciprocal resource commitments and collaborative communication can serve as a feedback loop creating greater levels of trust and relationship commitment, and thus influencing the structure of the crisis response network." (p. 12). The authors note that trust and commitment develop over time, and posit that the network structure will strengthen and change as the duration of the response matures. No studies were reported in this report, yet the concept of feedback loops is useful for evaluating human trust in networks. The ongoing research by Hudgens and Bordetsky (and, indeed, related research conducted by Dr. Bordetsky et al. in the Center for Network Innovation and Experimentation at the Naval Postgraduate School) will be of interest in our future analysis of this concept.

Kruse, Helquist & Adkins (2008) suggest collaborative tools that can synthesize the efforts of a large group of participants. Such large groups are a feature of networked operations with access to distributed team members. These tools, of the class of group support systems, have the potential to increase the effectiveness of a team by allowing previously passive members the opportunity to incrementally contribute to the collaborative process. The authors report on an open-source collaborative architecture that could potentially increase collaboration in the divergence, convergence and evaluation stages of teamwork. This work is of interest to us because it allows us to consider the case where team collaboration is inclusive, rather than exclusive, in a networked setting. However, we note that expanding the size of a networked team may cause problems of trust that could potentially reduce the original benefits of the collaboration tool.

Warne (2008) reported on a comprehensive qualitative exploration of the human 'networker' in the context of network centric operations. Her data suggest that personal face to face relationships are the foundation for trustful collaboration that cannot be reproduced by "technological interconnections". She suggests that technology is merely the base on which to build collaborative systems, and the focus should be on the networker, not the network. This research is useful in our exploration of trust in networks because it provides us with an avenue of approach; that is, to understand how trust is mediated by technology interfaces and connections.

Salamacha and Teates (2008) suggest a collaboration framework that specifies the social and the mission domains. In the social domain, team maturity and homogeneity are identified. In the mission domain, the authors suggest that the level of team interaction required for senesmaking and decision making is important. Also of interest are the disadvantaged users who have limited bandwidth or intermittent connectivity; collaboration tools will need to take into account these networked nodes. For our research, we might consider the differing levels of trust in networks reported by mature and homogeneous teams compared to heterogeneous, *ad hoc* teams.

Question 3: How does human trust in networks develop?

Ekman and Uhr (2008) provide an excellent review of interpersonal trust that develops in social relationships and trust that develops through a transfer process (whereby an actor ascribes trust to an entity based on associated trusting relationships). The authors note that this type of trust is frequently

associated with homogenous groups that will not always exist in military and crisis response situations. They introduce the term of 'endeavor networks' that refers to a group of teams formed for a specific response purpose. They note the feature of operational trust (Blatt, 2004), which is defined as the level of trust required by team members in order to accomplish a task; this trust is required, not just desired (pp. 5-6). Ekman and Uhr propose four themes. They suggest that: 1) endeavor specific social networks, whose members are new to each other, are likely to build interpersonal trust through transfer; that 2) such transfer may relate to how network members (trustors) perceive the legitimacy of the organization to which the trustee is associated, 3) that an organization seen as legitimate (by the trustors) in a specific endeavor may provide its representative (trustee) with a starting capital of trust; and 4) such a starting capital of trust is fragile to cultural enactment when interpretative frames conflict. Interpretive framing is defined by the authors as the mental mechanisms in social interactions that aid understanding of words and actions. Ekman and Uhr present four use cases where they explore this theme. In network centric operations, where ad hoc groups collaborate across national and organizational cultures, the concept of interpretive frames seems very useful in exploring the development of trust in this ubiquitous network.

Conclusion

This examination was a valuable first step in understanding how human trust of the technical components of a network can be measured and conceptualized. The survey tool we used should be condensed and improved to more parsimoniously represent the factors of the construct *trust in networks*. Additionally, we should examine the factor structure to identify components that could represent the missing 22.88% of variance. In support of future analysis, we will consider more frequent administration of a survey throughout a mission. This is based on the expectation that MANET behavior will be variable and could lead to fluctuations in trust by the human operators of systems dependent on the technical aspects of the network. Also, a better baseline of trust should be established prior to introducing information attacks. However, this initial examination provides a valuable start to a complex research effort.

Our review of relevant papers from the 13th ICCRTS provides a structure for future analysis of this concept of trust in networks. We reviewed seven research papers that assisted us in identifying factors that might be relevant to our area of interest. Our continued research in this area, combined with literature reviews of ICCRTS papers of recent presentation, promise useful results that can illuminate the issue of how humans develop trust in a network and how we can manage this trust with technology.

References

Blatt, N. (2004). Operational Trust: A new look at the Human Requirement in Network Centric Warfare. 9th International Command and Control Research and Technology Symposium, San Diego, 15-17 June, 2004

Bowman, E. K. & Thomas, J. A. (2009), in press. Cognitive Impact Study. 14th ICCRTS, Washington, D.C. Washington: CCRP.

Chan, K. (2008). Composite Model of Trust. Personal communication.

Conner, W. D. (2005). Understanding First in the Contemporary Operational Environment. Ft. Leavenworth, KS: School of Advanced Military Studies, US Army Command and General Staff College.

Corritore, C. L., Kracher, B. & Wiedenbeck, S. (2003). On-line trust: Concepts, eveolving themes, a model. *International Journal of Human-Computer Studies*, 58, 737-758.

Desouza, K. C., Roy, S. & Lin, Y. (2008). Performance Measures for Edge Organizations: A Preliminary Report. 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.

Hudgens, B. J. & Bordetsky, A. (2008). Feedback Models for Collaboration and Trust in Crisis Response Networks. 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.

Jian, J. Y., Bisantz, A. M., and Drury, C. G., 2000, "Foundations for an empirically determined scale of trust in automated systems," International Journal of Cognitive Ergonomics, 1(4), 53-71.

Kruse, J., Helquist, J. & Adkins, M. (2008). Large-Scale Collaboration for Ill-Structured Problems. 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.

Lee, J. D. & See, K. A. (2004). Trust in automation: designing for appropriate reliance. *Human Factors*, vol. 46, pp 50-80.

Muir, B. (1994). Trust in Automation: Part I. Theoretical Issues in the Study of Trust and Human Intervention in Automation Systems, Ergonomics, 37(1 I), 1905-1922.

Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. IEEE Tran. Syst. Man. Cybern. A. Syst. Hum., vol 30, pp 286-297.

Riegelsberger, J., Sasse, M. A. & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies*, vol 62 pp 381-422.

Salamacha, C. O. & Teates, H. B. (2008). A Framework for Effective, Interoperable Collaboration. 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.

Stevens, J. (1996). Applied Multivariate Statistics for the Social Sciences. Mahwah, NJ: Lawrence Erlbaum Associates.

Swami, A. and Bowman, E. (2008). Network Science Strategic Technology Objective. Adelphi, MD: Army Research Laboratory.

Taylor, C. D. (2005). The transformation of reconnaissance: Who will fight for information on the future battlefield? Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College.

Uruguay, A. L. P., Guerreiro da Costa, P. C., Nilton de Oliveira Lessa, N, & Ruybal dos Santos, C. L. (2008). C2OLISEU – A meta-model for research and development of complex network centric operations. 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.

Warne, L. (2008). The Human Terrain of NCO. 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.

Human Trust in Networks

Dr. Liz Bowman

ARL-SLAD

14th ICCRTS June 2009

Trust and Tactical Networks

- The devolution of the network to the ***tactical*** echelon makes the implementation of mobile networking problematic (Taylor, 2005).
- Conner (2005) notes presence of a 'digital divide' between operational and tactical commands, a result of great distances and the vast amount of data attempting to be shared.
- Trust:
  - Facilitates cooperative team behavior, exchange of resources and serves to reduce uncertainty (Lee & See, 2004).
  - Predictor of system use, appropriate reliance on automation, and strategies for system use (Atoyan, Duquet & Robert, 2006; Jian, Bisantz & Drury, 2000; Corritore, Kracher & Wiedenbeck, 2003; Parasuraman, Sheridan & Wickens, 2000).
  - Is not a stable attribute but is determined by the situation in which the trust actor and the object of trust exist (Corritore et al. (2003).
  - The introduction of new technologies leads to novel forms of interactions between users and technologies that require trust (Riegelsberger et al. (2005) .

How do users conceptualize the ‘Network’?

- Quality of information transfer in the network is a function of actors, channels, context, and information (Desouza, Roy, and Lin, 2008).
- Social domain: ‘role’ and ‘relationship’; Cognitive domain: ‘belief’ and ‘goal’ ; Information domain: ‘operational nodes’, ‘data’, and ‘links’; Physical domain: ‘objects’ and ‘energy’ (Uruguay et al.,2008).

How is trust impacted at the tactical level by collaboration?

- Feedback loops with reciprocal resource commitments seem to provide greater trust and commitment in crisis response teams (Hudgens & Bordetsky,2008).
- Collaborative tools that can synthesize the efforts of a large group can increase trust in the divergence, convergence and evaluation stages of teamwork (Kruse, Helquist & Adkins, 2008).
- Personal face to face relationships are the foundation for trustful collaboration that cannot be reproduced by "technological interconnections"(Warne, 2008).
- Collaboration must account for the disadvantaged users who have limited bandwidth or intermittent connectivity; collaboration tools will need to take into account these networked nodes (Salamacha and Teates,2008)

How does human trust in networks develop?

- Operational trust (Blatt, 2004): the level of trust required by team members in order to accomplish a task
- Ad hoc groups build interpersonal trust through transfer; transfer relates to perception of organizational legitimacy, this provides starting capital of trust, but this trust is fragile if members have different perspectives (Ekman and Uhr, 2008)

Exploratory Study Goals

- Obtain an empirical and analytical understanding of human trust in a tactical network
  - How do humans perceive “the network”?
  - What are the network performance characteristics that are most relevant to human performance
- Explore how MANET performance impacts tactical decision making
  - Information flow?
  - Situational Awareness?
- Investigate the human impact on network performance
  - Friendly: over/under use of applications? Overloading?
  - Enemy: Denial/Delay of service, insertion of false information
- Long term goal: Correlate physical network metrics to human performance metrics such as trust, situational awareness, etc.

Examples of Network Metrics

Primary Metrics

Connectivity

Offered Load (measured)

Packet Completion Rate

Packet Latency

Packet Jitter

Variables

Traffic Profiles

- Parametric loading
- QoS prioritization with background traffic

Mobility

- Static – simple LOS & heavy foliation
- Mobile – racetrack through open & foliated

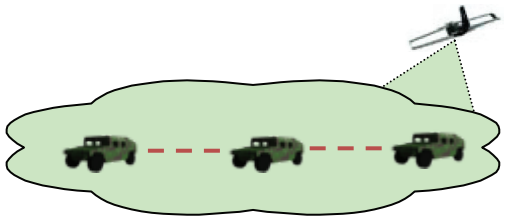
Packet Size

Window Size

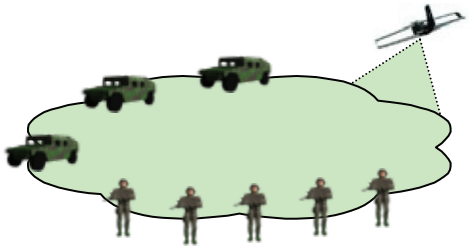
Data Dissemination

- Multicast Group Config
- Unicast

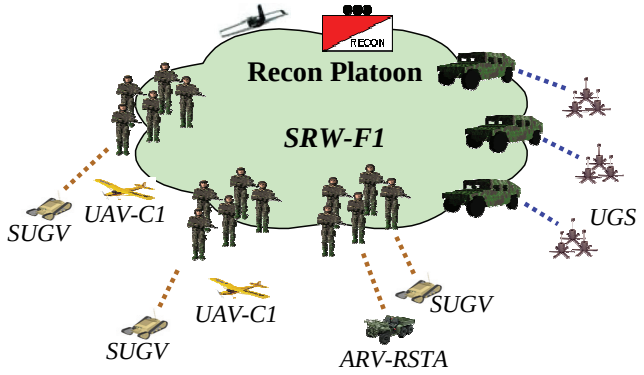
Point-to-Point & Multi-Node

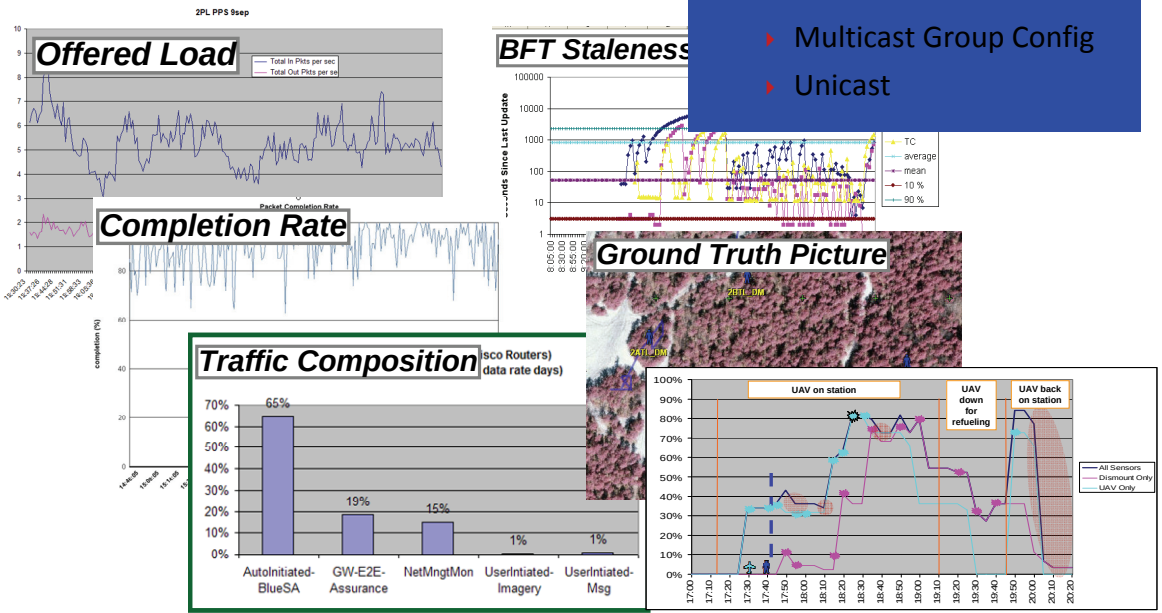


Vehicular + Dismount (3+5 node network)



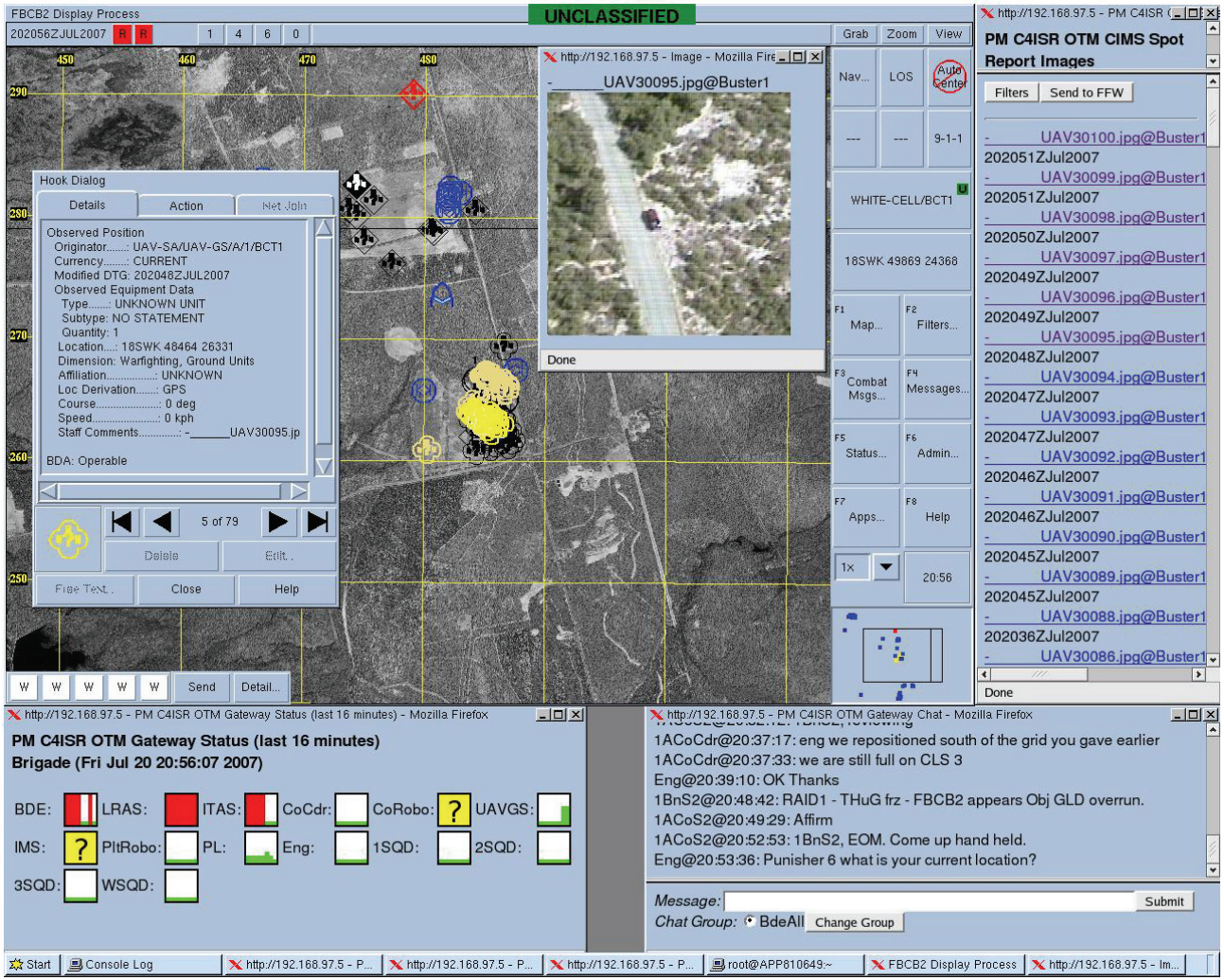
Full Recon Platoon (4+15 node network)





Impact of Network Performance on Humans

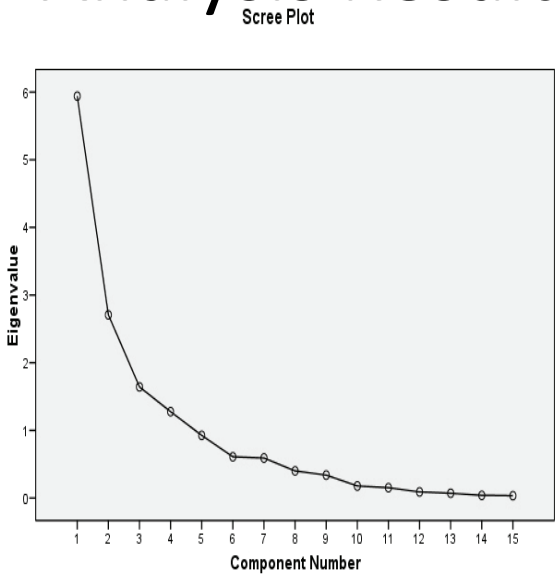
- Delays / dropped messages: fail to alert Soldiers to enemy detections by sensors
- Node drop-off: loss of comms, low SA
- Low bandwidth: images of enemy detections are delayed/lost
- Latency: blue position reports don't show the current force locations
- Loss of network connections: isolates dismounted and vehicle-based Soldiers from comms



Procedures

- 15 q. *Trust in Network* Survey administered daily at end of mission
- Principal Components Analysis used to determine factor structure of survey
- Repeated Measures Analysis of Variance conducted to examine differences between two platoons

Principal Components Analysis Results



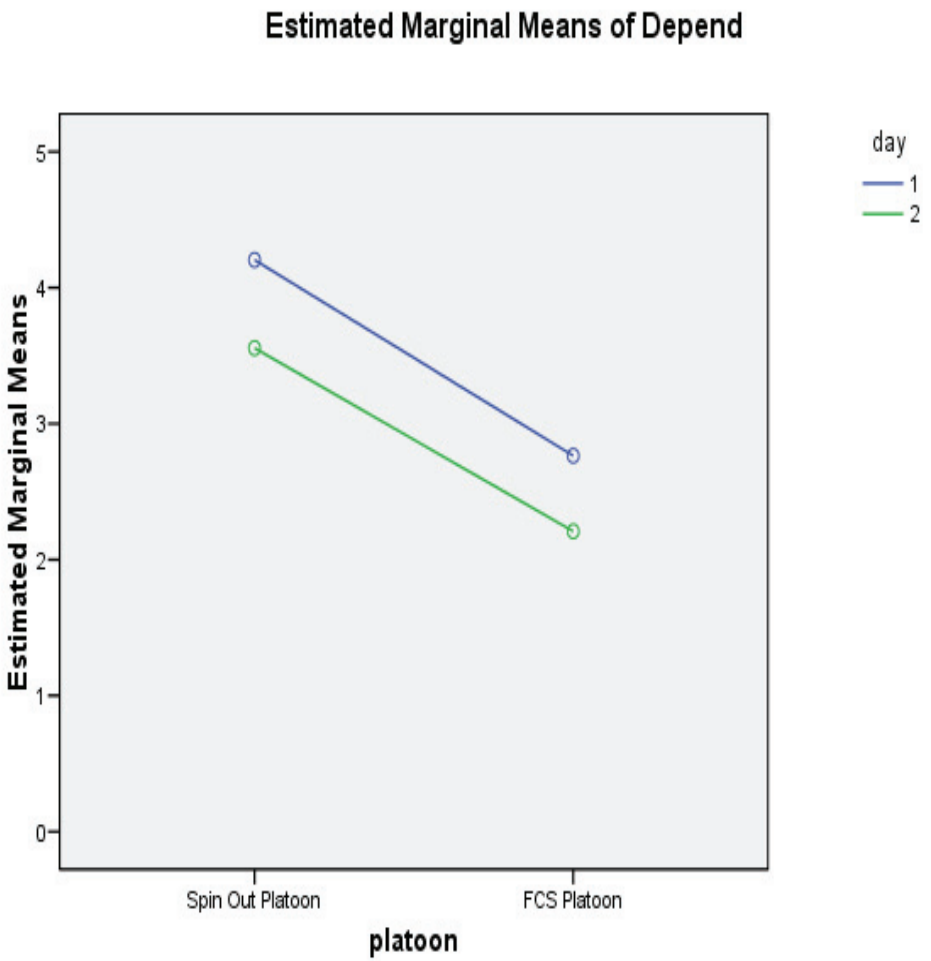
Variance Explained:
Depend: 39.6%
Reliable: 18.05%
Comms: 10.95%
Access: 8.51%
Total: 77.12%

Rotated Component Matrix(a)

	Component			
	Depend	Reliable	Comms	Access
Access	.085	.312	.089	.786
Received	.074	.240	.844	-.004
Send	-.012	.571	.643	.036
Comms	.320	.184	.587	.210
Open	-.107	-.005	.045	.857
Resend	-.151	.604	-.561	.138
Support	.124	.865	.250	.074
Reliable	.253	.837	.172	.161
Services	.237	.843	.223	.186
Secure	.910	-.055	.076	-.170
Integrity	.889	.014	-.018	-.146
Depend	.877	.107	.254	.105
Reliable	.790	.284	.318	.268
Trust	.765	.397	.141	.069
Familiar	.585	.245	-.151	.468

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a Rotation converged in 6 iterations.

Repeated Measures Analysis of Variance



- Limitations
  - Unexpected technology performance between platoons
  - Information Warfare attacks on one platoon
- Significant difference between first/last day *Wilk's λ* F (4,16) = 4.98, *p* =.008
- Platoons differed on factor of dependability, *Wilk's λ* F (1,19) = 7.58, *p* =.013
- Ratings declined for both platoons during the experiment
- SO platoon the mean score declined from 4.20 to 3.56
- FCS platoon mean score declined from 2.76 to 2.21

Conclusions

- Valuable first step in documenting human trust in networks
- Need to improve survey tool for parsimony and explanation of variance
- Consider survey administration; shorter tool at more frequent intervals is recommended to capture network fluctuations

Backup Slides

References

- Atoyan, H., Duquet, J-R., & Robert , J-M. (2006). Trust in new decision aid systems. In Jean-Marc Robert and Bertrand David (Eds.): Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine, Montreal, Quebec, Canada, 18-21 April 2006. ACM International Conference Proceeding Series 133 ACM 2006, ISBN 1-59593-350-6, [On-line] Available: http://www.informatik.uni-trier.de/~ley/db/conf/ihm/ihm2006.html#AtoyanDR06 p. 115-122.
- Blatt, N. (2004). Operational Trust: A new look at the Human Requirement in Network Centric Warfare. Proceedings of the 9th International Command and Control Research and Technology Symposium, San Diego, 15-17 June, 2004
- Conner, W. D. (2005). Understanding First in the Contemporary Operational Environment. Ft. Leavenworth, KS: School of Advanced Military Studies, US Army Command and General Staff College.
- Corritore, C. L., Kracher, B. & Wiedenbeck, S. (2003). On-line trust: Concepts, eveolving themes, a model. International Journal of Human-Computer Studies, 58, 737-758.
- Desouza, K. C., Roy, S. & Lin, Y. (2008). Performance Measures for Edge Organizations: A Preliminary Report. Proceedings of the 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.
- Ekman, O. & Uhr, C. (2008). Crisis specific social networks: The interplay between organizational legitimacy and personal trust. Proceedings of the 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.
- Hudgens, B. J. & Bordetsky, A. (2008). Feedback Models for Collaboration and Trust in Crisis Response Networks. Proceedings of the 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.
- Jian, J. Y., Bisantz, A. M., and Drury, C. G., 2000, “Foundations for an empirically determined scale of trust in automated systems,” International Journal of Cognitive Ergonomics, 1(4), 53-71.
- Kruse, J., Helquist, J. & Adkins, M. (2008). Large-Scale Collaboration for Ill-Structured Problems. Proceedings of the 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.
- Lee, J. D. & See, K. A. (2004). Trust in automation: designing for appropriate reliance. Human Factors, vol. 46, pp 50-80.
- Parasuraman, R., Sheridan, T. B., & Wickens, C. D. (2000). A model for types and levels of human interaction with automation. IEEE Tran. Syst. Man. Cybern. A. Syst. Hum., vol 30, pp 286-297.
- Riegelsberger, J., Sasse, M. A. & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. International Journal of Human-Computer Studies, vol 62 pp 381-422.
- Salamacha, C. O. & Teates, H. B. (2008). A Framework for Effective, Interoperable Collaboration. Proceedings of the 13th International Command and Control Research Technology Symposium, Seattle, Washington, June 17-19 2008, Washington, D.C: CCRP.
- Taylor, C. D. (2005). The transformation of reconnaissance: Who will fight for information on the future battlefield? Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College.

Trust in Network Survey

1. I was able to access services on my display
2. I am confident that I received all the communications meant for me.
3. I was able to send communications.
4. I could communicate with others in my platoon.
5. I was able to open sensor images on my display with no delays.
6. People asked me to resend images or messages.
7. The network's services supported the mission.
8. The network services were reliable.
9. I am confident in the services provided by the network.
10. The network is secure.
11. The network had integrity.
12. The network is dependable.
13. The network is reliable.
14. I can trust the network.
15. I am familiar with the network.

adapted from Jian, J. Y., Bisantz, A. M., and Drury, C. G., 2000, "Foundations for an empirically determined scale of trust in automated systems," International Journal of Cognitive Ergonomics, 1(4), 53-71.