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

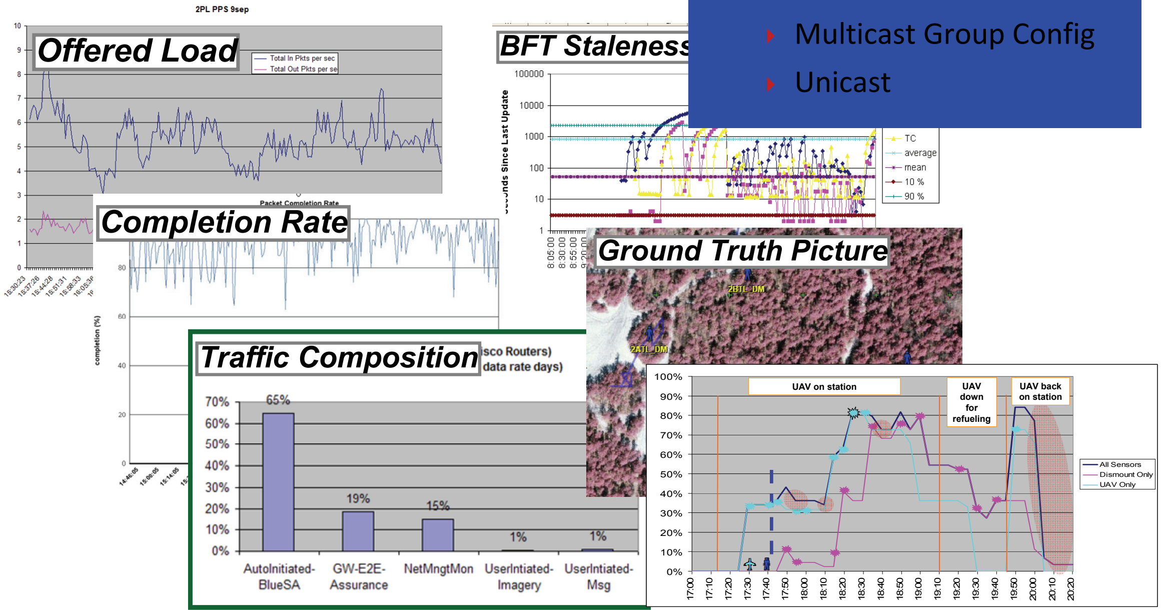
- Static – simple LOS & heavy foliation
- Mobile – racetrack through open & foliated

Packet Size

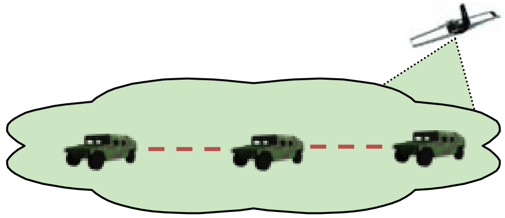
Window Size

Data Dissemination

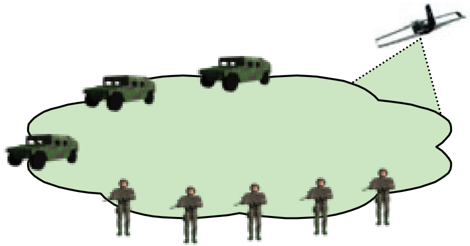
- Multicast Group Config
- Unicast



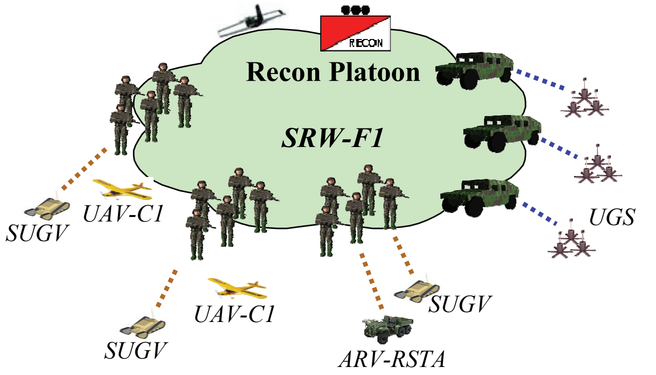
Point-to-Point & Multi-Node



Vehicular + Dismount (3+5 node network)

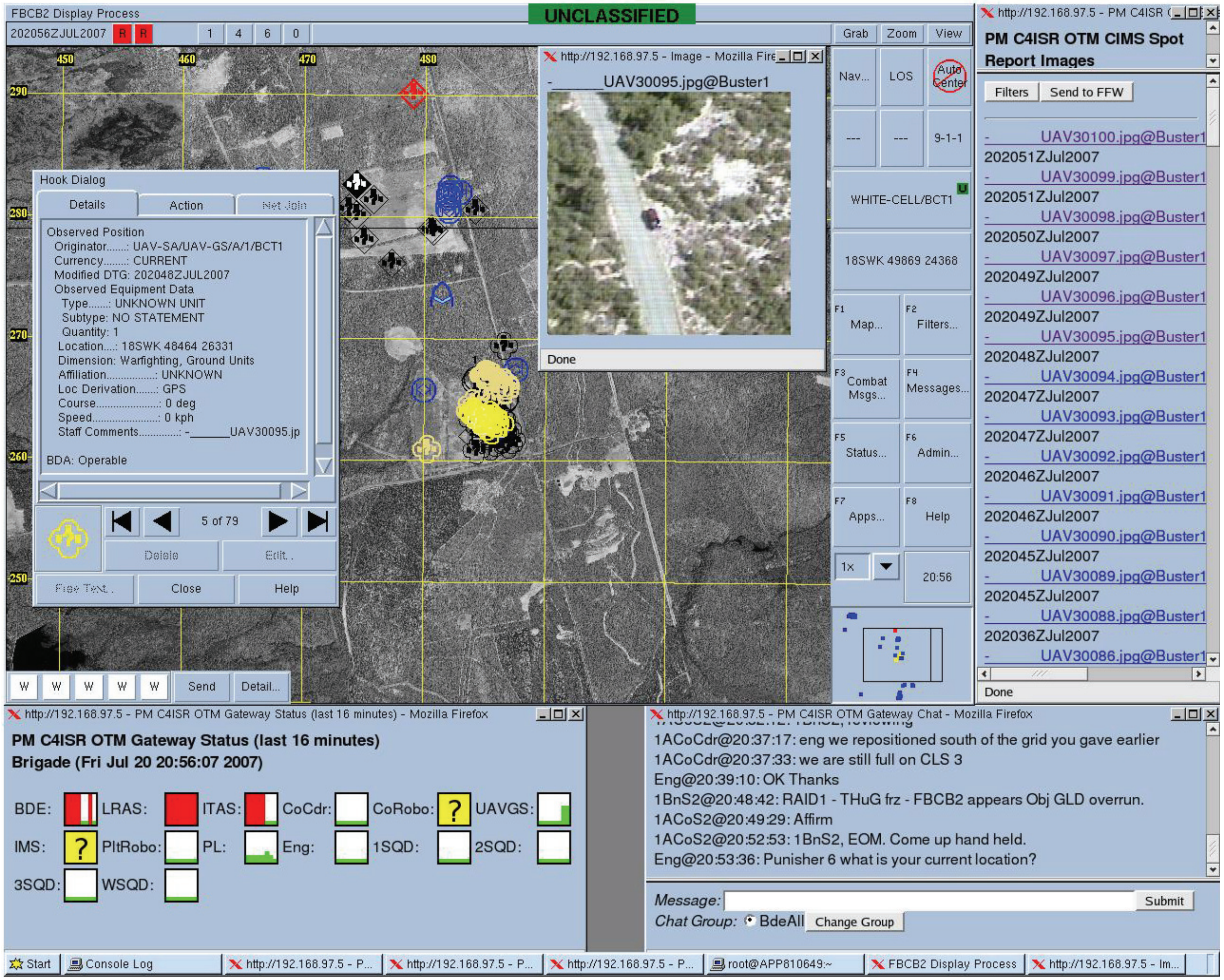


Full Recon Platoon (4+15 node network)



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



Hook Dialog

Observed Position
Originator.......: UAV-SA/UAV-GS/A/1/BCT1
Currency........: CURRENT
Modified DTG: 202048ZJUL2007
Observed Equipment Data
Type.......: UNKNOWN UNIT
Subtype: NO STATEMENT
Quantity: 1
Location....: 18SWK 48464 26331
Dimension: Warfighting, Ground Units
Affiliation................: UNKNOWN
Loc Derivation.......: GPS
Course.....................: 0 deg
Speed......................: 0 kph
Staff Comments.............: -______UAV30095.jp

BDA: Operable

5 of 79

http://192.168.97.5 - Image - Mozilla Fire

-______UAV30095.jpg@Buster1

http://192.168.97.5 - PM C4ISR

PM C4ISR OTM CIMS Spot Report Images

- UAV30100.jpg@Buster1
202051ZJul2007
- UAV30099.jpg@Buster1
202051ZJul2007
- UAV30098.jpg@Buster1
202050ZJul2007
- UAV30097.jpg@Buster1
202049ZJul2007
- UAV30096.jpg@Buster1
202049ZJul2007
- UAV30095.jpg@Buster1
202048ZJul2007
- UAV30094.jpg@Buster1
202047ZJul2007
- UAV30093.jpg@Buster1
202047ZJul2007
- UAV30092.jpg@Buster1
202046ZJul2007
- UAV30091.jpg@Buster1
202046ZJul2007
- UAV30090.jpg@Buster1
202045ZJul2007
- UAV30089.jpg@Buster1
202045ZJul2007
- UAV30088.jpg@Buster1
202036ZJul2007
- UAV30086.jpg@Buster1

http://192.168.97.5 - PM C4ISR OTM Gateway Status (last 16 minutes) - Mozilla Firefox

PM C4ISR OTM Gateway Status (last 16 minutes)
Brigade (Fri Jul 20 20:56:07 2007)

BDE: LRAS: ITAS: CoCdr: CoRobo: ? UAVGS:
IMS: ? PltRobo: PL: Eng: 1SQD: 2SQD:
3SQD: WSQD:

http://192.168.97.5 - PM C4ISR OTM Gateway Chat - Mozilla Firefox

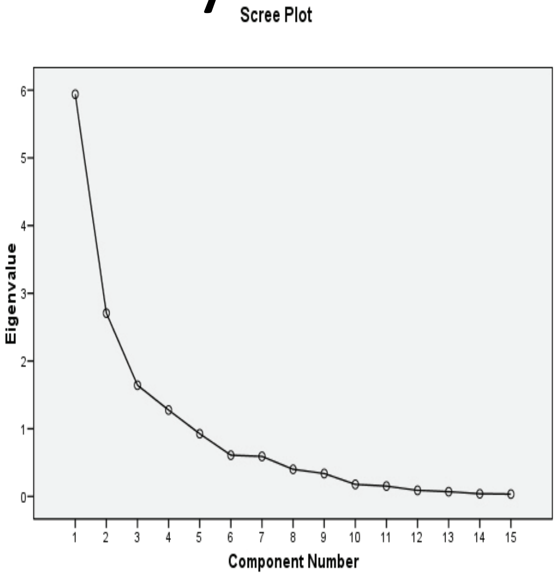
1ACoCdr@20:37:17: eng we repositioned south of the grid you gave earlier
1ACoCdr@20:37:33: we are still full on CLS 3
Eng@20:39:10: OK Thanks
1BnS2@20:48:42: RAID1 - THuG frz - FBCB2 appears Obj GLD overrun.
1ACoS2@20:49:29: Affirm
1ACoS2@20:52:53: 1BnS2, EOM. Come up hand held.
Eng@20:53:36: Punisher 6 what is your current location?

Message:
Chat Group: ● BdeAll

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



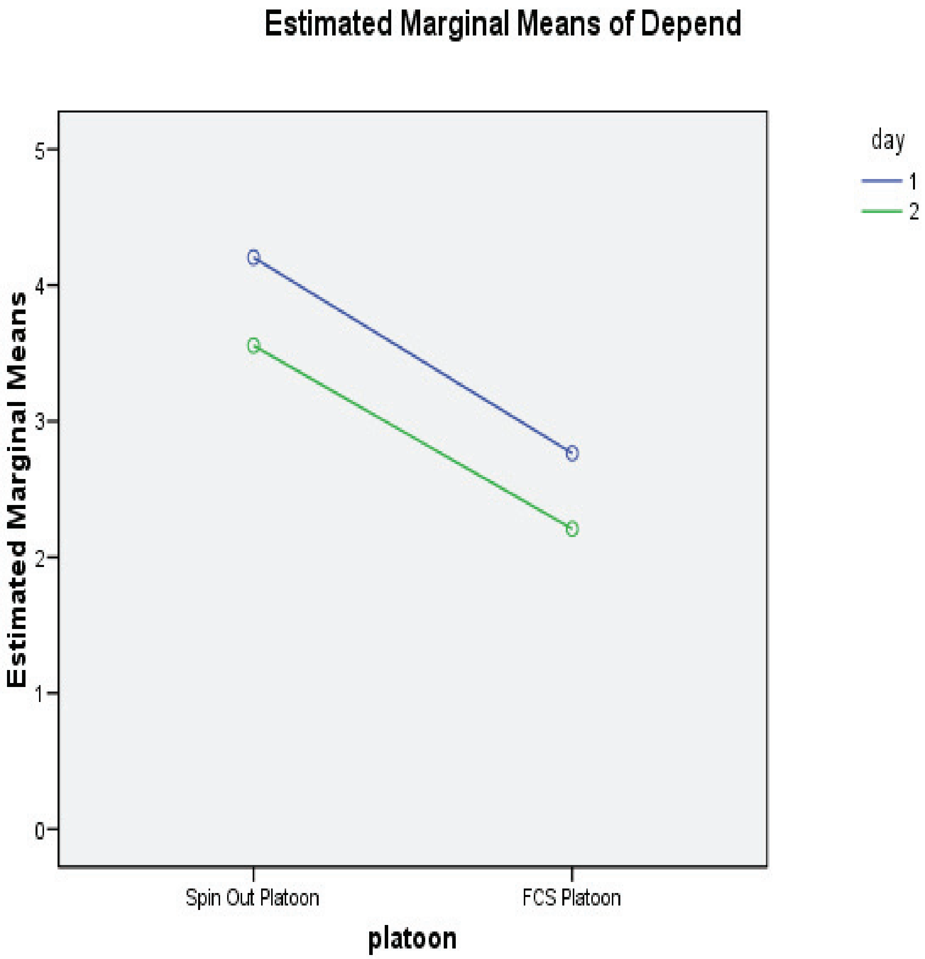
Variance Explained:
Depend: 39.6%
Reliable: 18.05%
Comms: 10.95%
Access: 8.51%
Total: 77.12%

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.