EasyChair Preprint

№ 671

Investigating the C2 benefits of dynamic and autonomous information prioritization and control over disrupted, intermittent and limited tactical edge networks

Rachna Lorke, Gregory Judd, Vanja Radenovic and Peter Boyd

December 7, 2018

Conference:
23rd International Command and Control Research & Technology Symposium 2018, 6-9 November, Pensacola, Florida, USA

Topic: Topic 8: Methodology, Experimentation, Analysis, Assessment and Metrics

Title of Paper:
Investigating the C2 benefits of dynamic and autonomous information prioritization and control over disrupted, intermittent and limited tactical edge networks

Authors:

Rachna Lorke
Defence Science & Technology
Bld 81, Third Ave, Edinburgh SA 5111 Australia
PO Box 1500, Edinburgh SA 5111 Australia
Rachna.Lorke@dst.defence.gov.au

Greg Judd
Defence Science & Technology
Bld 81, Third Ave, Edinburgh SA 5111 Australia
PO Box 1500, Edinburgh SA 5111 Australia
Gregory.Judd@dst.defence.gov.au

Vanja Radenovic
Defence Science & Technology
Bld 81, Third Ave, Edinburgh SA 5111 Australia
PO Box 1500, Edinburgh SA 5111 Australia
Vanja.Radenovic@dst.defence.gov.au

Peter Boyd
Defence Science & Technology
Bld 81, Third Ave, Edinburgh SA 5111 Australia
PO Box 1500, Edinburgh SA 5111 Australia
Peter.Boyd@dst.defence.gov.au

Investigating the C2 Benefits of Dynamic and Autonomous Information Prioritization and Control over Disrupted, Intermittent and Limited Tactical Edge Networks

Rachna Lorke, Greg Judd, Vanja Radenovic and Peter Boyd

ABSTRACT

A prerequisite for exercising Agile C2, and thereby achieving decision superiority over the adversary, is the effective management of information across tactical networks. This in itself is a highly complex and challenging problem due to the limitations imposed by the Disrupted Intermittent and Limited (DIL) tactical networks and the increasing demands for information placed on those networks. In conjunction with the US Army Research Laboratory, Defence Science and Technology (DST) in Australia is developing an intelligent autonomous software agent, known as SMARTNet that will attempt to address some of these difficult challenges. The idea behind SMARTNet is to introduce dynamic transformation, prioritisation and dissemination of tactical information based on a current military operational context and a current network state. The first iteration of the middleware, which was developed solely by DST, addresses the important use-case of dynamic prioritisation of Position Location Information (PLI) of friendly forces, in contention with other friendly tactical traffic. This paper outlines current land tactical needs and challenges in the information space and motivates the use of intelligent autonomous information management as a key part of any potential solution. We explore the methodology applied in developing our initial concept demonstrator and the experimentation performed to evaluate the PLI use-case. We present initial findings from the experiments, discuss the implications of these and conclude with recommendations for future work in the SMARTNet program.

Key words: C2 Agility, Autonomous systems, Information management, C2 measures of performance

1. Introduction (Greg)

In the days of voice only tactical radio networks, information management was much simpler. Human information managers such as Army signallers, forward observers, logisticians and commanders successfully used voice to exchange information ranging from urgent calls for fire, made in the heat of battle, to routine resupply requests. The human communicator

controlled the flow of information across the network based on an acute awareness of the battle context, a keen understanding of information priority, a shared understanding of the network procedures and protocols, and a clear awareness of the current state of the voice network based on the receipt of immediate feedback (by the presence or lack of voice acknowledgement for example).

Since the advent of digital messaging over tactical radio networks the amount of data has become too much for humans alone to effectively understand and manage. While this ability to send and receive digital messages rapidly, and in parallel, is the major benefit of digitisation, the volume of data and speed of transmission mean that there are just too many decisions for a human communicator to make. At any one time, for example, should the network prioritise the distribution of enemy locations, above friendly force locations, or ensure that requests for assistance with casualties are received first? Should it always send requests for fire support first, or are there times when urgent resupply might be equally important?

Current tactical information systems typically manage these conflicting information priorities in an automatic but inflexible way. One type of information always has priority over another (for example enemy locations over friendly locations). These pre-determined priorities are sensibly chosen and well suited to many, but not all, situations. For example, automatically sending out a digital message about each platform's location at a pre-determined rate (say once a minute) may in some situations be too slow (e.g. when in combat) but in others too often (e.g. during deliberate planning) and in so doing flood the network with unnecessary data that could compromise the timely delivery of more important information.

Unfortunately, unlike the commercial mobile phone network, terrestrially based land tactical communication infrastructure is not fixed. This means that tactical edge data communications (at the Brigade and below level for example) are characterised by extremely limited bandwidth, variable latency, widely varying data loads, and substantial size weight and power constraints. These become even more of a problem when conducting highly mobile operations over complex terrain in the face of enemy action [1][2]. These Disrupted, Intermittent, and Limited (DIL) networks can potentially threaten operational success by (unpredictably) preventing, or delaying, the delivery of the right information to the right person at the right time at all stages of tactical operations.

During the Australian Army and its allies many years of experience in the middle-east and Afghanistan, highly constrained DIL communications have not been so much of an issue. Reliable, relatively high-bandwidth communications have been provided via satellite and terrestrial communications have been optimised and managed via a host of commercial field service representatives. More importantly perhaps, this has been done in the face of an adversary incapable of seriously disrupting these communications. Recent experience in the Ukraine and in Syria has re-awakened concern that allied communication systems are too

vulnerable to jamming and cyber-attacks and are too big and slow to avoid destruction in high intensity warfare against peer adversaries [3].
This has led to the realisation that instead of optimising the network to provide the best user experience in normal circumstances (such as in Afghanistan) it needs to be optimised to provide acceptable performance in extreme circumstances [4]. This essentially means making the network less vulnerable to electronic warfare (EW) which in turn requires techniques, such as burst transmission, that severely restrict the amount of information that can be exchanged. When a network is under attack therefore, transmissions will need to be highly prioritised to ensure that, at the very least, essential information, such as friendly and enemy locations, is sent and received [5]. When these EW techniques are applied to constrained terrestrial networks the need for automated, real-time prioritisation and control of information becomes paramount.

2. SMARTNet Concept

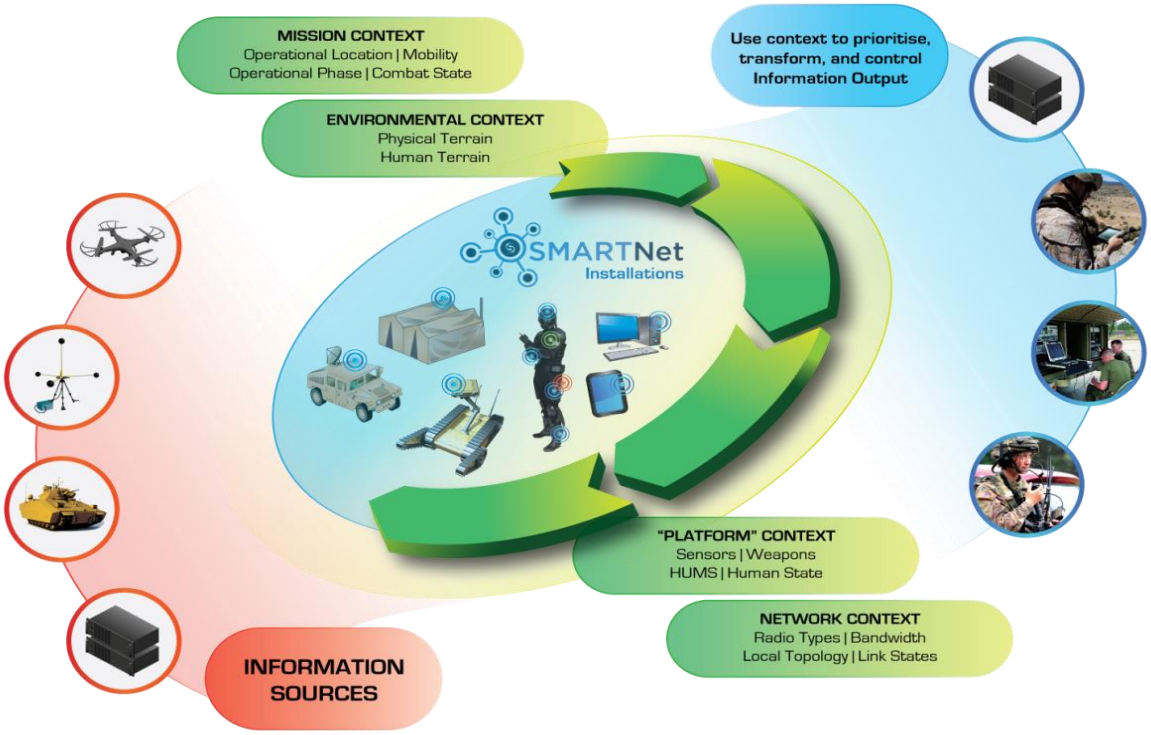

Figure 1: The SMARTNet Concept

Defence Science and Technology's (DST) - Systems Integration and Tactical Networking Group is developing an automated information management approach that can potentially restore the 'human-like' information management flexibility missing in existing digital systems [6][7]. Based on extensive involvement in the selection, development, and operational

test and evaluation of real world tactical information systems, the DST team has identified that recently emerging computational intelligence techniques could help Army cope with the complexity of these new systems. Using these techniques, a system could be developed that acts more like a human by 'understanding' the current mission and network contexts and then autonomously prioritising, transforming and controlling the flow of information at the tactical edge.

DST and our joint collaborators in the US Army Research Laboratory are calling this concept SMARTNet (Semantically Managed Autonomous and Resilient Tactical Networking). Running on every network-connected: soldier, vehicle and headquarters, SMARTNet will control that node's access to the tactical network. It will use the local information available to each node's: battle management systems, networks, and sensors to build up a representation of the current state of its: platform, mission, environment and network (see Figure 1 above). SMARTNet will use this knowledge of the current context to dynamically decide what priority each message should have, whether the message needs to be transformed (reduced, compressed or filtered) to fit within current network capacity, and when the message should be sent.

A key difference between the aim of SMARTNet and that of other DST and international research teams is that SMARTNet will ensure resilience in the *information* being communicated on top of any improved resilience to the *physical* network gained by improving communications connectivity, or available bandwidth. That is, given any network what-ever its capability, SMARTNet will provide help ensure that the right information gets to the right person, at the right time.

2.1 Key Research Problems

There are three key research problems that need to be met before dynamic tactical digital information management can be successfully implemented in real world tactical information systems:

Problem 1: Machine understanding of the current state of the tactical network

Completely optimising the transmission of information across a network requires every node in the network to be 'all knowing'. In other words, each node would require real-time access to all available data about the current network state from every other node. On severely constrained tactical networks all this shared network performance information would come at the expense of operational data. Thus, a delicate, ever changing, trade-off is required about how much network data can be requested, before the cost of getting that data actually outweighs the benefit. Solving this dilemma is currently an active area of research in network and computer science.

Problem 2: Machine understanding of the current mission context

How can the SMARTNet software determine the current battle context from the information available to it and then reason about it? How does SMARTNet represent the rules that it should use? What happens when these rules are contradictory or conflict? For example, a rule might exist to increase the rate a node sends out its own position if it is in contact with the enemy. How does the system 'know' that this has occurred and how does it reconcile this rule with another rule that also now prioritises red force locations? Furthermore, how do we know that these complexly interacting rules provide optimal information delivery outcomes for the tactical commander?

Problem 3: Defining success - identifying the quality and the value of information required

To solve problems 1 & 2 we also need to understand what 'success' looks like. In other words, we need to define what 'optimum outcomes for information delivery' means in terms of the value, or importance of the information delivered to the recipient (human or machine) and the quality attributes of that information such as the: timeliness, accuracy and completeness of information. Once we have established our measures of success, we can apply machine learning techniques to determine how SMARTNet should best prioritise, transform and control information in order to achieve these goals. This requires close involvement with military subject matter experts for validation / sanity checking.

2.2 Research Collaborations

Although a dynamic SMARTNet like approach has not been implemented (to our knowledge) in any currently deployed tactical system, similar research is occurring around the World. Our collaborators in the US Army Research Laboratory for example, are conducting ongoing network science research called Quality of Information for Semantically Adaptive Networks (QoI-SAN) This work is pursuing approaches that optimise the representation and transmission of information in tactical networks according to context-specific metrics rather than relying solely on simple, low-level, metrics such as throughput and latency [9].

This research helps meet Problem 3 by providing context-specific metrics that measure the actual QoI and the Value of Information (VoI) when information is exchanged. These measures have also been used in two recently completed NATO research activities: IST-118 "SOA Recommendations for Disadvantaged Grids in the Tactical Domain" [10] and NATO IST-124 "Heterogeneous Tactical Networks: Improving Connectivity and Network Efficiency" [11].

On the Australian side, the SMARTNet team has been working in conjunction with the University of Adelaide's Centre for Distributed and Intelligent Technologies to apply new and emerging distributed artificial intelligence (AI) techniques (Problem 2). The same University's Centre for Defence Communication and Information Networking (CDCIN) is using its expertise in tactical networks to help tackle Problem 1. The team is also partnering with Consilium Technology, a small to medium size company who has successfully built and installed commercial AI based solutions.

3. SMARTNet Concept Demonstrator

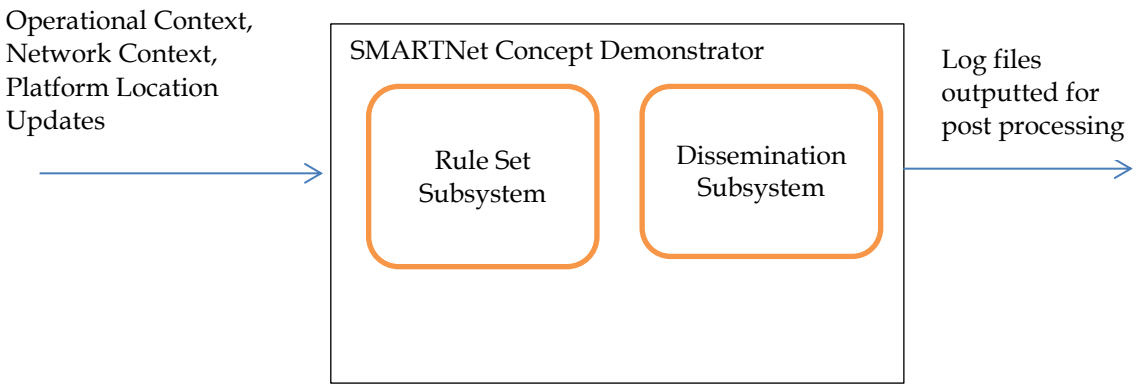

Figure 2 - High Level Software Architecture

Figure 2 above details the high level software architecture of the initial version of our SMARTNet concept demonstrator (focusing on the dynamic dissemination of PLI of friendly forces). In this iteration the concept demonstrator locally monitors changes in the operational and network contexts and updates platform position location messages received from an external source. Upon receiving the external changes the Dissemination subsystem dynamically adjusts the priority level and the update rate of the PLI messages based on the rules specified within the Rule Set subsystem. At the end of execution, the SMARTNet concept demonstrator outputs several log files capturing the states and important variables which are then used for data analysis.

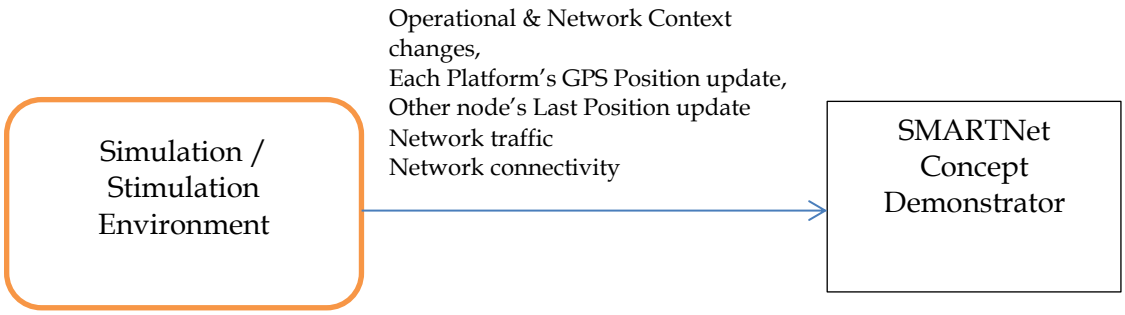

Figure 3 – Simulation/ Emulation environment and SMARTNet interaction

Figure 3 above, details the interaction between the SMARTNet concept demonstrator and its external simulator / stimulator. Developed in-house, the Simulator / Stimulator stimulates SMARTNet by informing it of changes to its own and other platform's location, operational context, and network context. It also simulates the message traffic and radio connectivity provided by a typical tactical network.

4. Experiment Design

4.1 Scenario Description

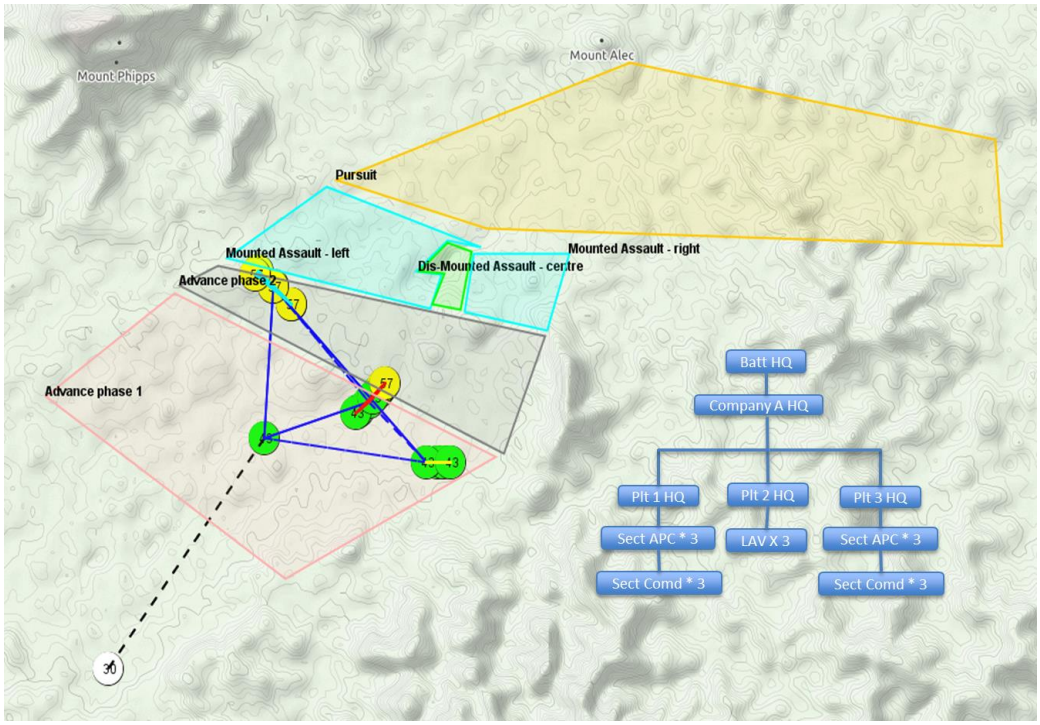

Figure 4: Intial SMARTNet Experiment Scenario

The initial experiment tested the effect of different automated information dissemination rules during a simple Company level scenario consisting of planning, advance, assault and pursuit vignettes (see Figure 4). During planning all nodes remained stationary. During the advance, the Company's three Platoons move along different routes towards an urban area where they expect to encounter the enemy. The company then moves to surround the town from the west, south, and east. Some forces dismount as they enter the town and other nodes remain mounted in close support. Finally, in the face of this assault, the enemy retreats from the town. Two mounted platoons follow in pursuit while another remains dismounted to secure the captured urban area.

4.2 Static versus dynamic-context-aware, prioritisation and update rate of own force locations

Using the concept demonstrator described above, we conducted a series of experiments comparing two different rulesets for updating and setting the priority of own force locations (often described as position location information or PLIs):

1. *Static Rules*: Own force location (PLIs) updates are always sent using a fixed ruleset[1] and with the same priority (50 out of 100). This roughly corresponds to the rules used by most current tactical information systems.

2. *Dynamic Rules:* These rules dynamically adjust PLI update rates and priorities to take into account changing operational conditions (based on rules suggested by subject matter experts in the Australian Army). The priority of the update, depends on a range of factors including: whether the node is in contact with an enemy; its operational location (rear, forward, or deep); and operational phase (planning or execution). The rate at which a node sends out a location update depends on: whether it is stationary or moving; the distance it has travelled since its last update; and whether it is in contact with the enemy. The goal is to increase the priority and update rate to provide better situation awareness when operationally relevant.

There were two other independent variables used during the experiment:

1. *Network connectivity*: was varied using either: perfect connectivity; the estimated line of sight between nodes as they moved; or a (repeatable) randomly determined level of average connectivity.

2. *Network load*: was varied by having each node send out background messages onto the network at different rates, ranging from once every 200 milliseconds (heavy traffic) to none, meaning the only message traffic was each node's own location message.

4.3 Performance measures

For this initial experiment the following quality and value of information measures were used:

- **Accuracy (or Location Error):** defined as the average difference between each node's knowledge of every other node's location and its actual location (based on the 'god's eye' view provided by the simulation). Accuracy is a proxy measure of own force Situational Awareness (SA).

- **Message Latency:** an average measure of the time taken from creation of a message to its receipt by another node. Measure Latency is a quality measure of information currency and is one of the measures that determine whether information meets the timeliness requirement of the recipient.

[1] When not moving a location update is sent every 30 seconds but when moving it is sent after 200 metres has been travelled, or after 30 seconds, whichever comes first. This ensures faster moving nodes are updated more quickly.

- **Messages Dropped**: is the average number of messages that are created but do not reach the intended destination. In the case of own force location messages this is a measure of completeness (but is actually binary, i.e. received or not).

4.4 Expected Results

The experiment investigated two hypotheses:

1. Dynamically transforming the rate at which each node updates its location onto the network will reduce the average location error across the system.

2. Dynamically changing the priority of location information, will improve the operational timeliness of location information delivered across the system.

We also hypothesised that the results would vary across each vignette:

- ***Planning:*** during this vignette, nodes are stationary so update rates have no effect on Location Error. The lower rate and priority placed on updates using the dynamic rules compared to the static rules are expected to lead to an increase in the timeliness of delivery of other types of, information. This behaviour aligns with the need to disseminate priority information such as mission plans and orders during planning.

- ***Advance (rear):*** While nodes are moving location update rates and priority are the same in both the static and dynamic cases, so little difference in any measure is expected.

- ***Advance (forward):*** as the company nears its objective, it is now considered to be in the forward area of the battlespace. Each platoon/ troop completes its advance at different times and waits for all other units to reach their assault starting positions. In the dynamic case, location information priority is increased and we therefore expect to see a small reduction in location latencies (perhaps also leading to a small reduction in location error).

- ***Assault:*** In the dynamic case, update rates and priorities increase both: when in contact with the enemy, and when dismounted. We therefore expect (and want) to see reduced location error and latency compared to the static case.

- ***Pursuit:*** In the dynamic case, update rates and priorities are much higher for the two pursuing platoons as they are considered to be in contact with the enemy. We therefore expect to see a significantly reduced average location error and Message Latency compared to the static case.

5. Data Analysis

Prior to running the actual experiment, we performed preliminary spreadsheet modelling that assumed perfect communications and no additional data. This approach allowed us to obtain theoretical results about the expected effect of the dynamic, compared to the static, rules. This modelling demonstrated that using dynamic dissemination rules should, as expected, increase PLI priority as operational tempo increased from planning until the assault (see Figure 5 below). It also showed that average location error across the Company during the advance and pursuit vignettes should be as predicted with a significant improvement during the pursuit vignette (see Figure 6 below).

The hypothesised large reduction in location error using the dynamic rules however was not found during the Assault phase. It was in fact unexpectedly worse! Further analysis showed that this was due to different update rates for mounted and dismounted nodes when moving at low speed. When in contact with the enemy using the dynamic rules, a dismounted node updated its location after moving 12.5 metres, but a mounted node had to wait until it travelled 80 metres. When both were moving at 5 km per hour the dismounted node updated every 9 seconds (good SA) but the mounted node every 55 (bad SA). Using the static rules however, all locations were updated every 30 seconds (average SA). In this particular case, when these differences were averaged across the whole Company the static rule set provided slightly reduced location error.

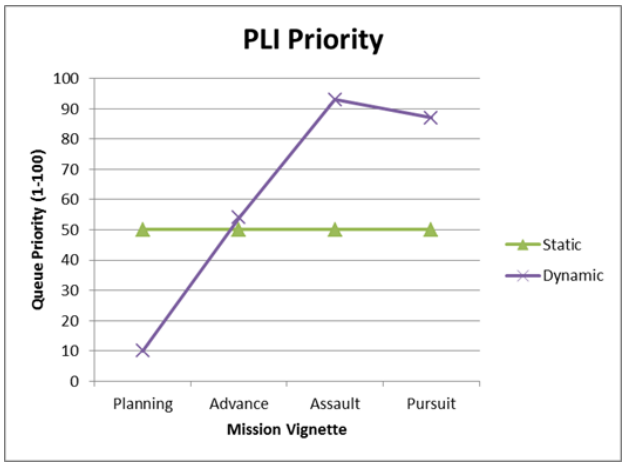

Figure 5: Expected effects of rules on PLI Priority

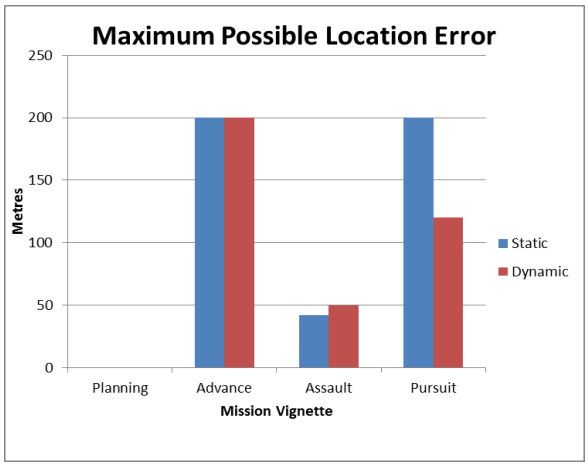

Figure 6: Expected effects of rules location error

This unexpected prediction was then tested during an experiment using the SMARTNet proof of concept system's more comprehensive modelling and simulation environment. During this experiment, log files were collected for each of the mission runs (Planning, Advance, Assault and Pursuit) with no traffic, high traffic and low traffic loads. Python scripts were used to post process information, compute Average PLI error, Average PLI latency and the total

number of dropped PLI messages within Platoon 1, Platoon 2, Platoon 3, the Company, and Battlegroup. From this post processed information, graphs were generated to compare the static and dynamic ruleset's effect on PLI error for each vignette across each traffic level.

6. Experiment Results

Space precludes the presentation of the full range of results. The key experimental results however, are summarized in Figure 7 and Figure 8 below which show the average internal[2] location error within Platoon 1 and 2 respectively during the Advance, Assault and Pursuit vignettes with no background traffic on the network.

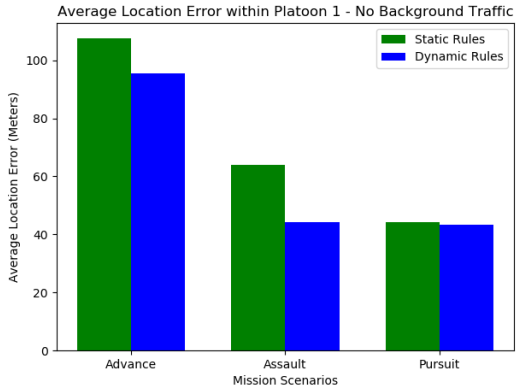

Figure 7 - Platoon 1 Average Location Error

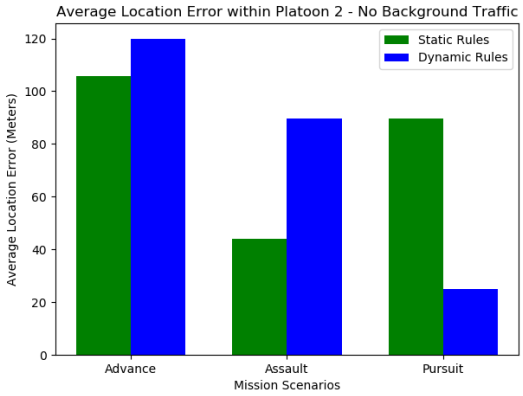

Figure 8 - Platoon 2 Average Location Error

In Figure 7 we observe that, as hypothesised, Platoon 1 has a better average location error for the dynamic ruleset than the static ruleset for all of the Advance, Assault and Pursuit vignettes. However, Figure 8 shows that this is not the case for Platoon 2, where the average location error is worse for the dynamic ruleset compared to the static ruleset for both the Advance and Assault vignettes, but very much better during the Pursuit scenario.

Identifying the reasons behind the unexpected results for Platoon 2 is quite difficult. More in-depth analysis suggests that this was due to complex interactions between different dynamic rules in certain circumstances. For example, during the Advance, in both the static and dynamic cases, all moving nodes updated their location after travelling 200 metres. Once each node stopped moving therefore other node's knowledge of its location might range in error from only a few metres up to 199 metres. Using the dynamic rules however, this error would

[2] Location error in this case is the average error in each node's current knowledge of all its other platoon members locations compared with their actual location.

not be corrected for another 10 minutes[3] while using static rules it was corrected after 30 seconds – making the dynamic rules perform 'unexpectedly' less effectively on average if there was a lengthy non-moving period after stopping. This effected only Platoon 2's results as it stopped moving much earlier than Platoon 1.

This effect also partly explains the considerably worse distance error using the dynamic rules for Platoon 2 during the Assault phase. Another contributing reason however, may have been the different dynamic update rates for mounted and dismounted nodes when moving at low speeds when in contact with the enemy discussed above. During the Pursuit vignette, Platoon 2's average location error was, as expected, considerably reduced using the dynamic rules. Clearly, updating a fast moving vehicle's location after every 80 metres travelled, rather than the standard 200 when in contact with the enemy, had a significant beneficial effect on SA. The same effect was not observed for Platoon 1 because it did not take part in the pursuit, but stayed in the Town.

7. Discussion

A key lesson learnt from this initial experiment was the risk of multiple (even relatively simple) dynamic rules interacting in unexpected ways to produce detrimental effects in some, but not all, situations. Once identified, these detrimental effects might be eliminated by modifying or adding rules. The advance vignette's problem, for example, might be solved by a rule requiring nodes to update their location as soon as they stop moving. The assault vignette's problem might be solved by both mounted and dismounted nodes updating their locations after moving 12.5 metres. This might however, lead to other unexpected, or unintended, effects. During the pursuit vignette for example, these higher update rates could flood the network with unnecessary updates potentially delaying the receipt of other important information such as the enemy's current location.

This reinforces the need to test and evaluate dynamic rules via comprehensive modelling, simulation, and experimentation across a large variety of different scenarios. It also reinforces the importance of being able to measure what success looks like (Problem 3) in order to use machine learning techniques to efficiently find the most effective combination of dynamic rules across the vast majority of likely situations. We also need to progressively investigate the system starting from simpler scenarios and then, once confirmed, move on to more complicated or realistic scenarios.

[3] Using the dynamic rules, a stationary node only updates its location after 10 minutes. This rule is intended to reduce unnecessary traffic on the network while occasionally indicating that the stationary node is still connected to the network.

8. Future Work

To meet these challenges, over the next three years DST will iteratively increase the fidelity and capability of the SMARTNet concept demonstrator and its modelling and simulation environment. Working in close collaboration with our ARL, University, and Industry partners, we will incrementally verify and validate our findings by moving from simple simulations, to complex network emulations (using ARL's large scale tactical network emulators). This effort will culminate in field trials using real radios in the US in 2020 and Australia in 2021. As we progress, we will continue to influence requirements for future tactical information systems with the ultimate goal of seeing a proven system fielded in a 'real-world' deployed capability.

9. Conclusion

In this paper we have argued that effectively managing the greatly increased speed and volume of digital information exchanged in the modern tactical battlespace is challenging. Rapidly changing network and operational conditions make the effective human management of this digital information increasingly difficult. Army's human information managers therefore need increased automated support to effectively prioritise, transform and control the flow of information across the tactical network.

To help meet this challenge, DST and its international, academic and commercial collaborators are investigating how this automated support can best be provided. Our iterative, multi-year, SMARTNet research effort will identify how to measure the quality and value of tactical information so that machine learning techniques can be used to capture, represent and reason about rapidly changing network and operational conditions in order to effectively prioritise, transform and control information across the tactical network.

Our initial, proof of concept, experiment has confirmed that successfully achieving the autonomous prioritisation and control of information across tactical networks is challenging. The interaction of even relatively simple context-aware dissemination rules can lead to counter-intuitive and unwanted effects. This confirms our initial view that, in order to ensure optimal outcomes, we need to develop and test machine learning algorithms in realistic modelling and simulation environments across many different network and operational scenarios.

Is the potential benefit worth all this effort? We argue that it is! Without a way to dynamically manage digital information in a future complex and contested battlespace (against a peer or near peer adversary) many future game changing technologies will not work effectively. New sensors and effectors will not be able to effectively share data, human- autonomous teams will not be able to self-coordinate and vital intelligence, gleaned from operational and strategic

big-data sources, or from the internet of things, will not be able to be shared with the war-fighter at the tactical edge.

10. References

[1] Suri, N., Benincasa, G., Lenzi, R., Tortonesi, M., Stefanelli, C., & Sadler, L. (2015). Exploring value-of-information-based approaches to support effective communications in tactical networks. *IEEE Communications Magazine, Volume 53, Issue:10*, 39-45.

[2] TR-IST-030. (2007). *Information Management over Disadvantaged Grids.* NATO RTO.

[3] Army-plans-to-halt-win-t-buy-shuffle-network: https://breakingdefense.com/2017/09/army-plans-to-halt-win-t-buy-shuffle-network/?utm_source=hs_email&utm_medium=email&utm_content=56798939&_hsenc=p2ANqtz-9ApQGSKeLKJtW4H0l5g1G3FjNTsfGXcxm76a0Sy0vRdp-UaU3euG4cvYczkUl8-Zh4n55_npk8EN1dQJUDoRCTaY6nHyUX0xyN2YnL_XJ_HKvIk54&_hsmi=56798939

[4] Army-to-build-bare-bones-network-small-satellites-for-multi-domain-battle: https://breakingdefense.com/2017/07/build-bare-bones-network-small-satellites-for-multi-domain-battle/

[5] Cant-stop-the-signal-army-strips-down-network-to-survive-major-war: https://breakingdefense.com/2018/03/cant-stop-the-signal-army-strips-down-network-to-survive-major-war/

[6] Judd, G., Finlay, L., & Coutts, A. (2015) *Coping with Uncertainty: Improving Trust in Digital C2,* 20th ICCRTS. Annapolis, Maryland: CCRP.

[7] Judd, G., & Chan, K. (2017) *Enhancement of Battlespace Information Management Systems for Coalition Networks using C2 Agility Design Concepts*, 22th ICCRTS. Los Angeles, California: CCRP.

[8] Network Sciences Collaborative Technology Alliance, www.ns-cta.org/

[9] Activities of the STO, www.sto.nato.int, 2018

[10] IST-118 (2013) SOA Recommendations for Disadvantaged Grids in the Tactical Domain. NATO RTO

[11] IST-124 (2016) Heterogeneous Tactical Networks: Improving Connectivity and Network Efficiency NATO RTO