UPPING THE IQ OF ARMY'S DIGITAL COMMUNICATIONS

improving tactical situational awareness and command and control using semantically managed autonomous and resilient tactical networking (SMARTNet)

Greg Judd, Rachna Lorke,Peter Boyd, and Vanja Radenovic
Land Division
Defence Science and Technology Group
Edinburgh, South Australia
Gregory.judd@dst.defence.gov.au

Kevin Chan
Network Sciences Division
Army Research Laboratory
Adephi, Maryland, USA
kevin.s.chan.civ@mail.mil

Since the advent of digital messaging over tactical radio networks the volume and rate of information has become too much for soldiers and commanders to effectively prioritise and control without automated help. Current tactical automated information systems however, do not manage this information anywhere near as intelligently as a human would if they could. This paper describes how Defence Science and Technology Group and its international, academic and commercial collaborators are investigating how the 'intelligence' of these automated information management systems can be improved. Using emerging machine learning techniques, this collaborative multi-year SMARTNet research program will address the three key research challenges preventing more intelligent solutions from being fielded. After briefly reporting on lessons learnt from an initial 'proof of concept' experiment, the paper concludes by warning that, without a more 'intelligent' autonomous information management system, new game changing technologies may not work effectively in a complex and contested, peer to peer, battlespace.

Keywords—information management; machine learning; autonomous systems

I. INTRODUCTION:

A. Machines do not currently manage tactical information as well as humans

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 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 network procedures and protocols, and an immediate awareness of the current state of the voice network gained from the presence, or lack, of voice acknowledgement.

Since the advent of digital messaging over tactical radio networks (using, for example, the Battle Management System and digital radios purchased under Australia's LAND 200 programme) the data deluge 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.

B. Why is this a Problem?

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; effects that are amplified 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.

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 disrupting these communications. Recent events in the Ukraine and in Syria have raised concern that allied communication systems are too vulnerable to jamming and hacking 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].

II. A POSSIBLE SOLUTION: SMARTNET

Defence Science and Technology (DST) 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 experience during the selection, development, and operational test and evaluation of the LAND 200 system, 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 can be developed that, like a human, 'understands' the current mission and network context, allowing it to autonomously prioritise, transform and control 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 information available from its 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). SMARTNet will use this contextual knowledge to dynamically decide what priority each message should have, whether the message needs to be transformed (reduced, compressed or filtered) to fit current network capacity, and when the message should be sent (see Figure 2).

A subtle difference between the aim of SMARTNet and other DST and international research teams improving the resilience of the *physical* network is that SMARTNet will improve *information* dissemination irrespective of the network's current bandwidth and data load. In other words, it will try to achieve the general information management mantra, across all levels of Defence, of: right information, right person, right time.

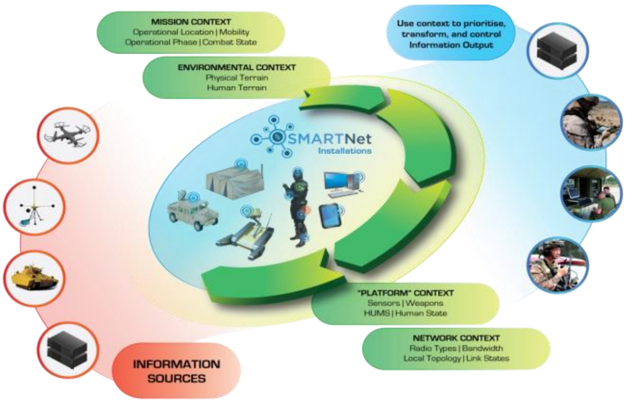

Fig. 1. SMARTNet: understands its context based on local data sources

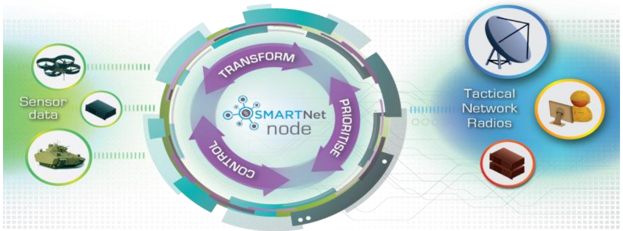

Fig. 2. SMARTNet: priotitises, transforms and controls information

There are three key research challenges that need to be met before SMARTNet's proposed approach can be successfully implemented in real information systems:

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

Completely optimising the transmission of information across a network requires real-time access to all available data about the current network state from every other node. On severely constrained tactical networks 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.

Challenge 2: Machine understanding of the current mission context

This is a key artificial intelligence challenge. How can SMARTNet 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? A rule might exist for example, 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 says sending out red force locations is also now very important? Most importantly however, how do we prove that these complexly interacting rules improve the quality and value of information received?

Challenge 3: Defining success - identifying the qualities and the value of the information required

To solve challenges 1 and 2 we need to define what 'optimum outcomes for information delivery' means in terms of the value of the information delivered to the recipient and the timeliness, accuracy and completeness qualities required. Once we have established these measures of success, we can then apply machine learning techniques to determine how SMARTNet should best prioritise, transform and control information. This also requires 'sanity-checking' by military subject matter experts.

III. Meeting the Challenge

Although a 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 (ARL) for example, are conducting ongoing network science research called Quality of Information for Semantically Adaptive Networks (QoI-SAN). This work optimises 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]. These context-specific metrics measure the actual quality and value (to the recipient) of the information exchanged[1].

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 (Challenge 2). The same University's Centre for Defence Communication and Information Networking (CDCIN) is using its expertise in tactical networks to help tackle Challenge 1. The team is also partnering with Consilium Technology; a small to medium size company with a proven ability to apply AI based solutions in the commercial world.

IV. Current Research

Using a SMARTNet proof of concept demonstrator, DST compared the performance of static (pre-set) and dynamically adjusted - own force location information priorities and update rates. In the static case, priority is always set to low and is sent every 30 seconds unless 200 metres is travelled first. With the dynamic rules, priority increases or decreases depending on contextual factors such as: whether the platform or soldier is in contact with an enemy; its current operational location and operational phase. The rate at which a node sends a location update also varies depending on: whether it is stationary or moving; the distance it has travelled since its last update; whether it is dismounted, and whether it is in contact with the enemy.

An experiment was conducted testing the effect of these different automated information dissemination rules during a simple Company level scenario consisting of planning, advance, assault, and pursuit vignettes. The experiment also investigated the effect of different levels of network connectivity and data load. It was expected that dynamically transforming the priority and location update rate would reduce the average location error and improve the time taken to deliver the highest priority information.

The following measures were used to compare the effect of these different approaches:

- *Location Error*: defined as the average difference between each node's knowledge of every other node's location and their actual location. This measures information *accuracy* and is a proxy for 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. This is one of the measures that can help determine information *timeliness*.
- *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 information *completeness*.

Preliminary spreadsheet modelling demonstrated that using dynamic dissemination rules should increase location update priority as operational tempo increased. It also showed a significant improvement in average location error during the advance and pursuit vignettes. During the assault vignette however, location error unexpectedly increased using the dynamic rules. This was because, using the dynamic rules, a dismounted node updated its location after moving 12.5 metres, but a mounted node only after 80. 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). This meant that location error, when averaged, was slightly reduced using the static rules.

V. Key Experimental Results

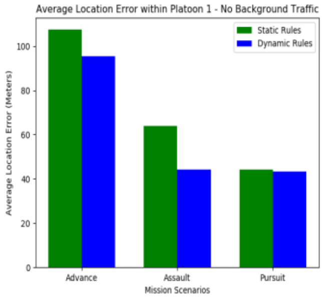

Fig. 3 Location Error: Platoon 1

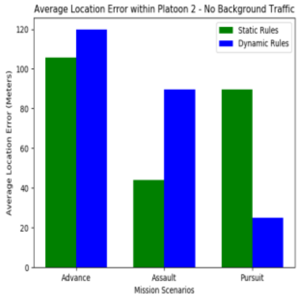

Fig. 4. Location Error: Platoon 2

Figures 3 and 4 summarise the key results from our initial experiment. They show the average location error within Platoon 1 and 2 during the advance, assault and pursuit

[1] This approach has 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]

vignettes. For Platoon 1 (Figure 3) the dynamic ruleset always produces a reduced average location error than the static ruleset. For Platoon 2 however (Figure 4) the average location error is worse using the dynamic ruleset during the advance and assault vignettes, but much better during the pursuit.

Initial analysis suggests that Platoon 2's unexpected result was due to complex interactions between different dynamic rules. 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 this meant that other node's knowledge of its location might range in error from a few metres up to 199 metres. It took 10 minutes to correct this error using the dynamic rules (because stationary nodes only update every 10 minutes to save bandwidth) but within 30 seconds using the static. This affected Platoon 2's results because it stopped moving much earlier than Platoon 1.

This effect also partly explains why the dynamic rules led to increased location error for Platoon 2 during the assault. The different dynamic update rates for mounted and dismounted nodes when moving at low speeds (explained above) however, also had an effect. During the pursuit vignette however, Platoon 2's much reduced average location error using the dynamic rules was, as expected, due to fast moving pursuing vehicle's updating their location every 80 metres rather than 200. This was not observed for Platoon 1 as it did not take part in the pursuit and remained relatively stationary.

The experiment confirmed that multiple, even relatively simple, dynamic rules can interact in unexpected ways and produce detrimental effects in some, but not all, situations. 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 (Challenge 3) so that machine learning techniques can be used to find the most effective combination of dynamic rules across the vast majority of likely situations.

VI. Future Work:

Working in close collaboration with our ARL, university, and industry partners, the SMARTNet research programme will incrementally develop increasingly more sophisticated computational intelligence approaches to dynamic tactical information management. This effort will culminate in field trials using real radios in the US in 2020 and Australia in 2021. As we progress, we will influence requirements for future tactical information systems, with the ultimate goal of a proven system fielded in a 'real-world' deployed capability.

VII. Conclusion:

The greatly increased speed and volume of digital information exchanged in the modern tactical battlespace requires automated support. Current tactical information support systems however, do not intelligently adapt to rapidly changing network and operational conditions. DST and its international, academic and commercial collaborators are investigating how this 'intelligent' support can 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. Our initial experimentation confirmed these techniques are needed to address the unintended detrimental effects that may arise from the interactions of dynamically changing rules.

Is all this worth the effort? We strongly argue that is! Without a way to manage digital information more effectively in a future complex and contested battlespace, against a peer, or near peer, adversary many of the potential future game changing technologies discussed in this conference 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.

References

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

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

[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. Accessed 15 May 2018

[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/ Accessed 15 May 2018

[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/ Accessed 15 May 2018

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

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

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

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

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

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