Proceedings of the 2014 Winter Simulation Conference
A. Tolk, S. Y. Diallo, I. O. Ryzhov, L. Yilmaz, S. Buckley, and J. A. Miller, eds.

SIMULATION IMPLEMENTATION AND PERFORMANCE ANALYSIS FOR SITUATIONAL AWARENESS DATA DISSEMINATION IN A TACTICAL MANET

Ming Li
Peter C. Mason
Mazda Salmanian
J. David Brown

Defence Research and Development Canada
3701 Carling Avenue
Ottawa, ON K1A 0Z4, CANADA

ABSTRACT

Situational awareness (SA) information in tactical mobile ad hoc networks (MANETs) is essential to enable commanders to make informed decisions during military operations. Sharing SA information in MANETs is a challenging problem because missions are run with dynamic network topologies, using unreliable wireless links, and with devices that have strict bandwidth and energy constraints. Development and validation of efficient data delivery methods in MANETs often require simulation; however, the literature is sparse regarding simulations specifically for SA dissemination. In this paper we present a simulation implementation for a newly proposed Opportunistic SA Passing (OSAP) scheme and investigate its efficiency in realistic scenarios. Moreover, we propose several metrics aimed at facilitating evaluation of SA dissemination schemes in general, and we demonstrate the applicability of the metrics in our simulation results. Our simulation provides a flexible framework and evaluation platform for experimental studies of SA data dissemination in tactical MANETs.

1 INTRODUCTION

Situational Awareness (SA) is an essential component in course-of-action decision making for achieving tactical objectives in military operations. The primary functions of SA as modeled by Endsley (1995) are Perception, Comprehension and Projection. In a tactical scenario, a useful definition for SA is "the ability to reliably, accurately and continuously collect information on the situation, enemy or friendly, when and where required" (Crovella 2002).

Mobile Ad hoc Networks (MANETs) are a promising technology for tactical operations and will likely be required to support SA dissemination as they are implemented in tactical networks. MANETs are particularly suited to tactical environments as they require no fixed communication infrastructure and are deployable with complex topologies in complicated terrain and adverse conditions. The benefits offered by MANETs come with corresponding challenges, however, including high routing overhead for multiple-hop connectivity, the need for distributed (as opposed to centralized) trust and security, and limited energy constraints. These networking challenges are especially difficult on tactical radio in Very High Frequency (VHF) ranges whose links have long-range propagation characteristics but are restricted in bandwidth (Li and Vigneron 2010).

.

Full SA data dissemination in MANETs is ordinarily achieved by a customized broadcast scheme. A plethora of research on broadcast methods in MANETs has been carried out: for example, Williams and Camp (2002); Lipmann, Liu and Stojmenovic (2008); and references therein. With a focus specifically on SA data dissemination in tactical MANETs, Böse et al. (2005) introduced an adaptive pulling protocol to save the network load while maintaining the freshness rate of the SA data. Wang et al. (2007) examined SA messaging requirements on legacy tactical waveforms in VHF/UHF narrowband, and presented messaging implementations with in-field testing. Larsen et al. (2010) investigated efficient SA flooding techniques based on the Simplified Multicast Forwarding (SMF) framework and suggested an adaptive algorithm using radio load as a metric. In Zhang et al. (2010) the authors proposed an energy efficient broadcast protocol based on the Optimized Link State Routing (OLSR) protocol (Clausen and Jacquet 2003) that compares favorably with other popular schemes such as classical flooding, SMF and coding-based broadcast.

Network simulation plays an indispensable role in the research into tactical MANETs, ranging from exploration of network behavior to validation of new protocols. The majority of the simulation work discussed in the literature has been implemented on the popular NS2/NS3 platforms, for instance, Li, Shi and Kunz (2012) and Zhang et al. (2010) for efficient broadcast/multicast schemes in a tactical radio setup; and a simulation for DisService, a middleware for tactical network applications including SA data sharing (Marchini et al. 2012). Examples on other platforms include an OpenGL-based graphical simulator (Vigelmann, Fitzek and Lucani 2010) for investigation of various application-level data dissemination methods; and the verification of mobile tactical networks by Li et al. (2012) on a QualNet (SNT 2008-2014) platform.

The existing simulation work often focuses on general mobile network performance, using typical metrics such as routing overhead, traffic throughput, packet delivery ratio (PDR) and latency. Simulations specifically for measuring the performance of SA information dissemination are largely lacking from the literature. In this paper we implement a newly proposed scheme called Opportunistic SA Passing (OSAP) (Brown, Salmanian and Li 2014) on the QualNet simulation platform. The simulation provides an effective and efficient framework for further investigation of SA data dissemination in tactical MANETs. We also propose specific metrics for the evaluation of efficiency, accuracy and freshness of the SA data sharing across the network, and demonstrate the importance of these metrics by analyzing experimental results from several scenarios.

The rest of the paper is organized as follows. In the next section we describe the methodology and design details of our simulation implementation for the OSAP scheme, and define the metrics for performance analysis of SA data dissemination. In section 3 we present the simulation scenarios with the analysis of the experimental data. Discussions and concluding remarks are given in the final section.

2 SIMULATION IMPLEMENTATION AND PERFORMANCE METRICS

This section provides the methodology, design and implementation details for our simulation of the OSAP scheme, and proposes specific metrics for SA dissemination performance evaluation. The simulation platform is EXata/Cyber version 4.1, a product in the QualNet family with emulation capability and cyber security add-ons. We will refer to the simulator as QualNet for simplicity. Our simulation design is actually platform independent, so long as the selected platform possesses common wireless network simulation functionalities: appropriate modeling of radio frequency; propagation and fading effects; realistic simulation of wireless channel functions; MAC (media access control) layer protocols for variety of wireless communication standards; topology selection and mobility models; TCP/IP stack and wireless routing protocols; and application layer software. On the software side, the selected platform would require an effective discrete event engine; accurate timers and schedulers; an efficient messaging system; and a complete suite of the networking stack.

2.1 The Opportunistic SA Passing (OSAP) Scheme

A detailed description of OSAP is presented in Brown, Salmanian and Li (2014). For completeness, we briefly review the design idea and key operations in this subsection.

We introduce terminology and notation as follows. Let the set $\boldsymbol{S} = \{n_1, n_2, \ldots, n_N\}$ denote all nodes in the tactical network. OSAP proceeds in "rounds" where a round is initiated by a node n_i ($i \in [1, N]$). We refer to one OSAP "cycle" as the completion of N rounds, where each node has initiated exactly one round of SA passing. With this terminology defined, the OSAP scheme proceeds as follows:

- In each cycle, all nodes in $\boldsymbol{S}$ take turns serving as the initiator of a round. The order in which the initiators take their turns is a design parameter of OSAP and is discussed in more detail later in this paper. The order of the initiators may or may not be the same within each OSAP cycle.
- When a node is the initiator, it sends a broadcast message, which contains its own SA data, and is identified by its node id and a sequence number, to all its neighbors. At a minimum, the SA data contains the time at which the SA data is generated (SA timestamp) and the location of the node. Depending upon mission requirements, other information such as channel conditions, trust and security values, topological and mobility parameters, etc., could be added as well.
- All nodes that receive a broadcast SA message re-broadcast the message based on the initiator's id and sequence number, such that a node would re-broadcast SA messages from the same initiating node/sequence number only once. All nodes append their own SA data when re-broadcasting, so an SA message contains a chain of SA data for all intermediary hops.
- Upon receiving an SA message from a neighbor node, each node processes the message and updates its SA cache if the received SA for a specific node has a more recent timestamp. The SA processing is carried out regardless of whether or not the node is to re-broadcast the SA message.

The scheduling within each cycle (i.e., the order in which the initiators are chosen and the time between rounds) has significant impact on the effectiveness and efficiency of the SA data dissemination. In this paper we simply assume a fixed time interval between consecutive rounds of SA broadcast, and call it ***update interval***, denoted by τ. From now on we refer to a node that initiates an SA broadcast / receives an SA message / re-broadcasts an SA message as sending node / receiving node / relay node, respectively. We also use the term broadcast and flood interchangeably in this paper.

2.2 SA Data Format and Message Handler

The SA messaging required for OSAP is similar to the Route Request (RREQ) message in the Dynamic Source Routing (DSR) protocol (Johnson, Hu and Maltz 2007). Consequently our implementation is based on re-use of, and enhancements to, the DSR routing programs in QualNet, namely routing_dsr.h and routing_dsr.cpp in the wireless library. In DSR, the RREQ message consists of header bytes followed by a list of intermediary hop addresses. We define a new SA message type in the DSR routing code. The SA message has a similar format to the RREQ message, while replacing the list of addresses by a list of SA data of the intermediary hops; this data contains node addresses, the timestamps of the SA data, the location of the hop and some reserved space for additional SA information for future use.

QualNet makes use of a messaging mechanism to simulate application data packets going through the networking stack within a node and between nodes across the network. We modify the DSR message handler with additional functions to process the new SA message type. At a receiving node, all SA data of the intermediary hops are extracted and compared with the cached SAs in a local repository; the received SA is either created or updated in the repository if it has a newer timestamp, or ignored if the cache copy is more recent. Note that at each round, a receiving node may obtain SA data for a same node multiple times, however it only relays SA data once for the same initiating node/sequence number. As previously mentioned, the relay node always generates its own SA data with the current timestamp and appends it to the SA message to be relayed.

2.3 The Controlled Broadcast Procedure

The QualNet simulator is equipped with a centralized clock providing synchronized timing for all nodes via the getSimTime API (application programming interface). We create an SA broadcast timer on each node which goes off at end of update interval τ and triggers SA flooding on the scheduled node. The order in which nodes initiate flooding (i.e., SA broadcast scheduling) is controlled in code by a specific global array consisting of a permutation of node set $\boldsymbol{S}$. This corresponds to, in a real-world deployment, a synchronized clock and pre-defined scheduling algorithm for all nodes in the tactical network.

We implement our controlled broadcast procedure for the new SA messages by adapting the RREQ messaging in DSR's route discovery process, with the following key modifications:

- The SA broadcast on a node is initiated by a scheduling algorithm instead of a request from upper layers. As result, the messaging overhead in the networking stack at the node is minimized.
- We set the destinations in the SA message header to be a "fictitious" node, i.e., a node beyond reach of all other nodes, thus ensuring the flooding reaches all connected nodes for each round.
- For SA messaging, the sending node is not expecting a reply from the destination node, i.e., the RREP (route reply) process in DSR is not utilized for SA data handling in the code.

We point out that the fictitious destination is purely for the simplicity of implementation, re-using the current DSR routing code. Alternatively we could set a dummy destination in the message header, and let the message type dictate the message handler's behavior. However, the alternative design involves much more code changes without adding any benefit, hence we did not pursue that approach.

The ordering of the sending nodes within a cycle could have significant impact on the performance of SA dissemination achieved by OSAP (for instance, if the first few initiating nodes were all localized in the same area, one side of the network would have more SA information than the other). In our design and implementation we set up two configurable parameters for the control of the SA flooding order: the "flooding option" parameter and "starting node" parameter. There are three types of "flooding option" as defined below:

1. Random flooding (flooding option = 0). In each cycle, the order of the initiating nodes is a random permutation of node set $\boldsymbol{S}$. The pseudo random number generator seed to obtain the permutation can be changed for each cycle such that each cycle has a different order for the initiating nodes. Selection of the starting node has no effect in this case.
2. Consecutive flooding (flooding option = 1). In this option, the order of the initiating nodes is a continuous round-robin in sequence: $n_j, n_{j+1}, \ldots, n_N, n_1, \ldots, n_{j-1}$, where n_j is the starting node.
3. Interleaved flooding (flooding option = k). Assume all nodes can be evenly divided into k (≥ 2) groups. For any given cycle, SA flooding starts from the starting node n_j which falls in one of the k groups. The next rounds take place by round-robin through the remaining $k-1$ groups, choosing the first node in each of those groups. The flooding is then repeated for n_{j+1} and the second node in the rest $k-1$ groups, and so on until all nodes take their turn to finish the cycle. This option necessarily requires the scheduler to have *a priori* knowledge of the distribution of the nodes among the k groups.

2.4 Radio Range Configuration on the Simulator

Wireless connectivity plays a key role in the effectiveness of SA dissemination techniques. To better simulate the topological and mobility features of the tactical network, we configure the radio range of the wireless nodes to a desired distance, achieved by utilizing QualNet's physical layer configuration tool in the graphical user interface (GUI). We select the *Abstract* radio type with data rate set to 2 Mbps and the frequency bandwidth set to 2 MHz. We then make adjustments to the following properties in order to calibrate and achieve a desired radio range: *Transmission Power*, *Antenna Height*, and *Antenna Efficiency*. The parameter values for each scenario presented in this paper are specified in section 3.

2.5 Metrics for Performance Analysis of SA Dissemination

A majority of the MANET data dissemination schemes and corresponding simulation results documented in the literature focus on networking performance in a general sense, such as messaging overhead, throughput, delivery latency and PDR. However for SA data distribution in a tactical network, our primary concerns for a node are the ***degree of completeness*** of SA information it possesses with regard to other nodes in the network, and the ***degree of freshness*** of the SA data. The completeness can be measured by the number of nodes for which a local node has received SA data (referred to as number of SAs possessed by the node). The freshness of a particular SA value, denoted by T_{SA}, can be quantified by the ***age*** of the SA data and is calculated as the current time minus the received time value in the timestamp of the SA.

SA information, by its nature, is time sensitive; therefore, we classify a particular node's cached SA by its age T_{SA}. For each scenario we will set two thresholds T_{fresh} and T_{stale} , and define SA with age T_{SA} as

- ***fresh*** if $T_{SA} \leq T_{fresh}$,
- ***stale*** if $T_{fresh} < T_{SA} \leq T_{stale}$,
- ***expired*** if $T_{SA} > T_{stale}$.

In a real-life deployment, the fresh and stale thresholds should be determined based on mission constraints and C2 (command and control) requirements. In our scenarios, we set $T_{stale} = N\tau$, which is the time required for a complete cycle of flooding. This is a reasonable choice since it should take no more than one complete cycle for any connected node to receive SA about any other connected node. In general, OSAP should do better than this, as our recent study revealed that 90-95% of SAs can be distributed across network after only four rounds of OSAP flooding under reasonable conditions (Brown, Salmanian and Li 2014). Therefore, threshold T_{fresh} could be set to the time required to distribute certain percentage of SA data throughout the network, e.g., $T_{fresh} = 4\tau$ for four rounds of flooding. Another possible selection for T_{fresh} is the time required for certain percentage of the nodes in the network to complete their rounds of SA broadcasting (such an example is shown later on in scenarios 1 and 2 in section 3).

At any given time a node can have various numbers of fresh/stale/expired SAs, because nodes may lose connectivity to others from time to time. For any node n_i ($i \in [1, N]$) in the node set $\boldsymbol{S}$, denote the number of SAs and sum of the age of the corresponding SAs in each category by $N_{fr}(i), A_{fr}(i), N_{st}(i), A_{st}(i), N_{ex}(i), A_{ex}(i)$, where the subscript *"fr"* refers to fresh SA, *"st"* refers to stale SA, and *"ex"* refers to expired SA. We define SA age for each category at a node as an averaged value, denoted by adding a macron, e.g., $\bar{A}_{fr}(i) = A_{fr}(i)/N_{fr}(i)$, and so on for the stale and expired SA age. Furthermore, the term "average SA count" or "average SA age" refers to the average value over all nodes in the network, e.g., "average fresh SA count" is given by $\bar{N}_{fr} = \sum_{n=1}^{N} N_{fr}(i)/N$ and "average fresh SA age" is given by $\bar{A}_{fr} = \sum_{n=1}^{N} \bar{A}_{fr}(i)/N$.

We also suggest using the number of transmitted (initiated and relayed) and received SA messages over a time window (i.e., average rate of transmitted and received messages) as a metric to indicate the workload on the network for SA dissemination. For node n_i we denote number of messages transmitted and received by $M_{tr}(i)$ and $M_{rc}(i)$, respectively; and define "average message count" by taking an average over all nodes, e.g., $\bar{M}_{tr} = \sum_{n=1}^{N} M_{tr}(i)/N$. For controlled flooding (re-broadcast is done for the same initiating node and sequence number just once at each relay node), the average transmitted message count is primarily dependent on the size of the network. On the other hand, the number of received messages can vary significantly according to the topology and connectivity changes. Note that in the context of this paper the message count is for SA messages only, not including other message types such as the control message for wireless network MAC or routing operations.

In summary, we define two configurable thresholds T_{fresh} and T_{stale} to classify all SAs possessed by nodes in the network, and define the following metrics for SA dissemination performance analysis:

- node-wise SA count $N_{fr}(i), N_{st}(i), N_{ex}(i)$, and the corresponding average values $\bar{N}_{fr}, \bar{N}_{st}, \bar{N}_{ex}$;
- node-wise SA age $\bar{A}_{fr}(i), \bar{A}_{st}(i), \bar{A}_{ex}(i)$, and the corresponding average values $\bar{A}_{fr}, \bar{A}_{st}, \bar{A}_{ex}$;

- node-wise SA message count $M_{tr}(i)$, $M_{rc}(i)$, and the corresponding average values $\overline{M}_{tr}, \overline{M}_{rc}$.

We point out that the above metrics are usually collected and calculated within a time period immediately before the current time, i.e., a "sliding window". In our implementation we add appropriate counters and time variables in the code to keep track of the above metrics. A natural choice for the sliding window size in OSAP is using the update interval τ , i.e., calculating the metrics per round basis.

3 SIMULATION SCENARIOS AND TESTING RESULTS

In this section, we test QualNet scenarios on a 40-node static network and a 10-node mobile network to demonstrate the OSAP scheme and investigate the experimental results using the performance metrics defined in section 2.5. The configuration parameter values are summarized in Table 1. For static scenarios we run the simulation for 201s, the time required to complete two full OSAP cycles for the 40-node network, plus an extra 1s to compensate for the processing time for the last round of flooding. For the mobile scenario, we run the simulation for 750s, the time required for mobile nodes to move across the concerned area according to a waypoint mobility model.

Table 1: Parameter values for scenario configuration.

	Scenario 1: 40 nodes Radio range 110 meters	Scenario 2: 40 nodes Radio range 220 meters	Scenario 3: 10 nodes Radio range 85 meters
Transmission power	11.5 dBm	14.56 dBm	10.0 dBm
Antenna height	0.8 meters	1.3 meters	0.7 meters
Antenna efficiency	0.8	0.85	0.74
Simulation time	201 seconds	201 seconds	750 seconds
Update interval τ	2.5 seconds	2.5 seconds	2.5 seconds
Fresh threshold T_{fresh}	75 seconds	75 seconds	10 seconds
Stale threshold T_{stale}	100 seconds	100 seconds	25 seconds

3.1 Static scenarios and the test results

Scenarios 1 and 2 are set up on a 40-node static MANET as shown in Figure 1. Node 41 is the fictitious (destination) node placed beyond the radio range of all other nodes and does not participate in SA flooding. The nodes are sparsely distributed but still mutually connected by multi-hop links, while there are more links in Scenario 2 because of the doubled radio range compared to Scenario 1.

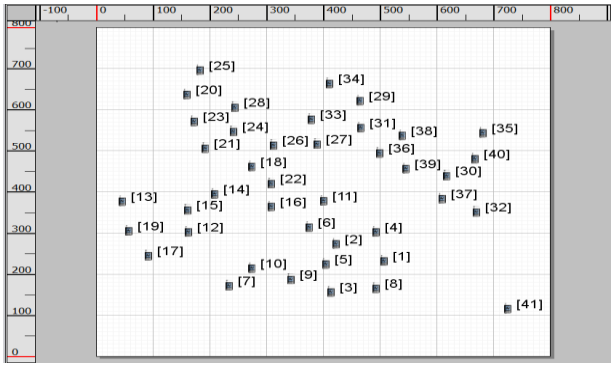

Figure 1: Node placement for Scenario 1 and Scenario 2, a snapshot taken from the QualNet GUI.

In the static scenarios we set T_{fresh} and T_{stale} values to 75s and 100s respectively, i.e. time required for 75% and 100% of the nodes to complete their rounds of flooding (each round requires τ = 2.5s). We run three tests in each scenario with the following OSAP flooding orders: random, consecutive order starting from node 1, and consecutive order staring from node 31. The results of average fresh SA count $\overline{N}_{fr}$ for

Scenario 1 are depicted in Figure 2. We observe that for this scenario, random flooding is superior to consecutive flooding because more SAs are disseminated in the network with faster pace. This result makes sense in the case where the nodes are grouped according to their id number as is the case in the network topology shown in Figure 1 (i.e., N1 is close to N2, which is close to N3, and so on). By randomizing the scheduler, we intentionally avoid the case of clustered initiating nodes. In Figure 2, at 25s (after 10 rounds of flooding), the average SA count reaches 15.98 for 'starting N1', 17 for 'starting N31', and 28.35 for 'random' flooding. The selection of the starting node in consecutive flooding has little effect on the results. Note that we don't have 100% SA (= 40) in the results, and we observe SA count variations in the second cycle (from 100 to 200 seconds), due to the fact that some SAs are no longer fresh (T_{SA} > 75s), which are thus excluded from the plot. Not surprisingly, for the network configuration in Figure 1, random order flooding is a better choice from the SA count perspective.

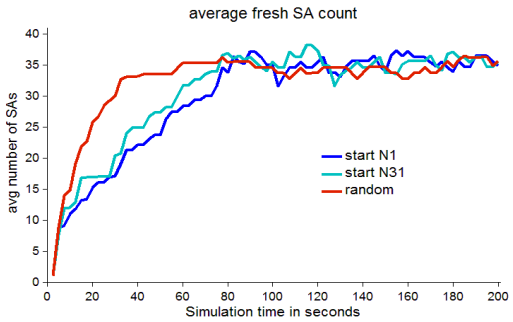

Figure 2: Average fresh SA count with different flooding orders in Scenario 1.

To investigate the effect of changes in the network on the results of the SA dissemination, we run the same tests on Scenario 2, which has the same topographical setup as in Scenario 1 but with doubled radio range. We present the average fresh SA count $\bar{N}_{fr}$ and average fresh SA age $\bar{A}_{fr}$ in Figure 3, where the four curves represent the results of Scenario 1 (110m radio range) and Scenario 2 (220m radio range), using random order and consecutive order starting from N1, respectively.

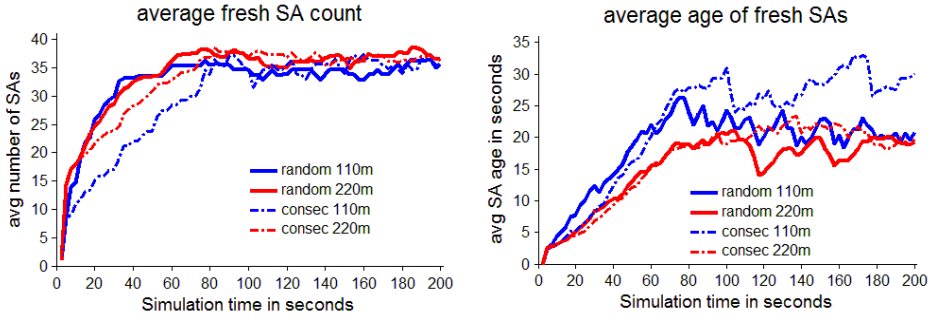

Figure 3: Comparison of average SA count and age in different flooding orders and radio ranges.

From the left subfigure in Figure 3 we observe that in the first cycle (up to 100s), when the radio range is doubled, the average fresh SA count increases for consecutive order flooding (dashed lines), because more nodes are involved at each round of flooding. However in random order case, the increase in radio range has little impact on the average fresh SA count (solid lines). Also the improvement of random flooding over consecutive flooding diminishes when radio range is doubled (solid vs. dashed lines in the same color). In the second cycle, the average fresh SA count is not affected significantly by either flooding order or radio range.

Although the average fresh SA count (for random order flooding) is not significantly affected by the radio range change, increasing radio range does improve the performance from the perspective of SA age,

as can be seen in the average SA age diagram in the right subfigure of Figure 3. We notice for the same kind of flooding order (random or consecutive), increase in radio range results in lower average SA age, i.e., improved freshness in the SAs. Moreover, the improvements in SA age due to the wider radio coverage are noticeable throughout the two cycles (blue lines vs. red lines).

3.2 Mobile scenario and the test results

In this scenario we examine the effect of mobility and intermittent disconnections in a tactical MANET. We consider two groups, each with five nodes, moving at a constant speed in a 1500m by 1000m rectangular region. We adapt the waypoint mobility model in QualNet to configure course of movement of the mobile nodes, as given in Figure 4. In the "loose" case, node 4 in group 1 and node 9 in group 2 are "scouting nodes" with higher degree of mobility. For each mobility pattern (tight and loose group topology) we perform test runs with consecutive (starting N1), interleaved (starting N1) and random flooding. The results are summarized in Figures 5, 6, and 7 below. The mean values for each type of data during the entire simulation are also shown in the figures for comparison purpose.

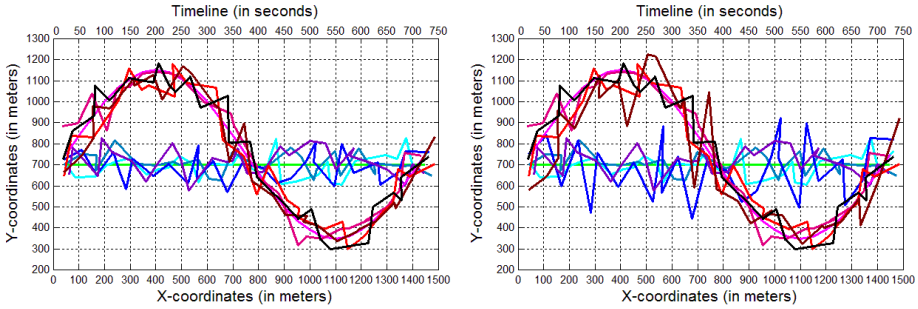

Figure 4: Mobility trajectories for Scenario 3: tight group (left) and loose group (right).

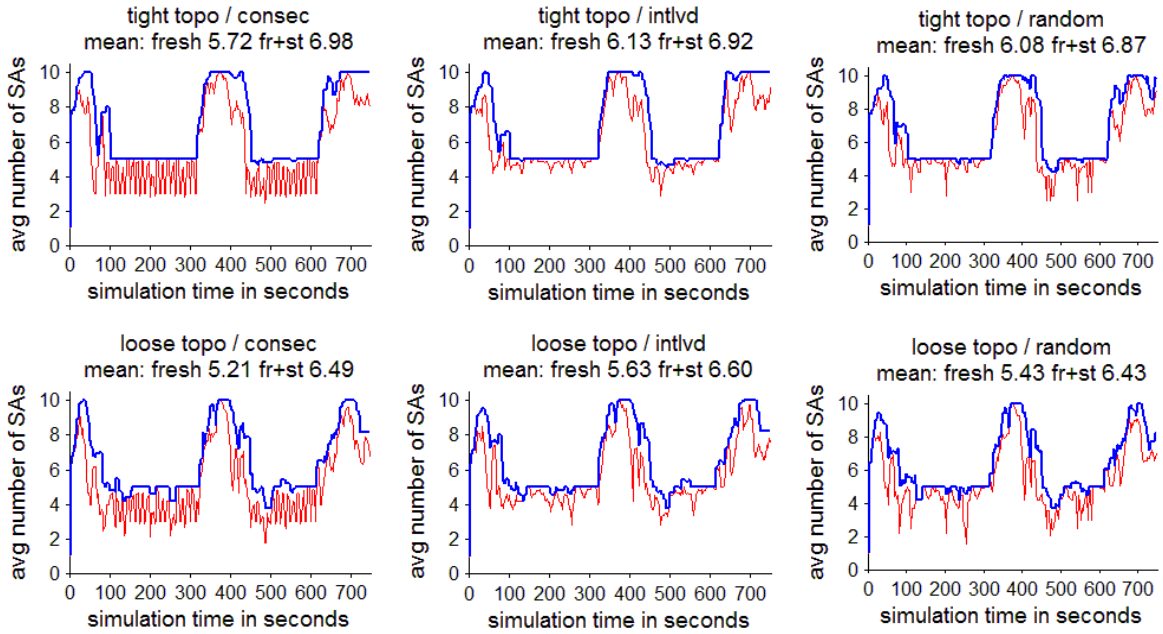

Figure 5: Average SA count – Fresh $\overline{N}_{fr}$ (in red) and Fresh-plus-Stale $\overline{N}_{fr+st}$ (in blue) for tight topology (above) and loose topology (below) in three different flooding orders.

Figure 5 shows the average SA count $\bar{N}_{fr}$ and $\bar{N}_{fr+st}$. The average SA count for fresh-plus-stale SAs is a practical metric to represent usable (unexpired) SAs, where stale SA may still be usable although not as current as fresh SA. At the time of group separation, nodes can only exchange SAs within their own group, i.e. five SAs is the maximum number we would expect to see in the best case. Generally speaking, interleaved flooding produces superior results, with the highest values of $\bar{N}_{fr}$ and $\bar{N}_{fr+st}$. As noted before, this would require the scheduler to know ahead of time which units were in which of the two groups. Consecutive flooding generates an oscillating pattern for $\bar{N}_{fr}$ in tight topology, while less regularly in loose topology. This is a result of the fact that each group contains consecutive initiating node ids, meaning that when the two groups diverge the initiating node remains in one group or the other for a length of 5τ instead of alternating between the two groups. Randomization reduces the oscillation and operates nearly as well as the interleaved scheduler. We note that the SA count in the loose topology is not as stable as that in the tight topology because the scouting nodes deviate frequently from the group and cause more events of connectivity loss. In summary, for Scenario 3, interleaved flooding and random flooding produce better SA counts than consecutive flooding, with interleaved performing slightly better than random; in addition, the tight topology results in more stable $\bar{N}_{fr}$ and $\bar{N}_{fr+st}$ than in the case of the loose topology.

The corresponding average SA age $\bar{A}_{fr}$ and $\bar{A}_{fr+st}$ are depicted in Figure 6, where a higher age value indicates older SAs. Random flooding produces the highest mean values for $\bar{A}_{fr}$, while consecutive flooding has highest mean values for $\bar{A}_{fr+st}$. Interleaved flooding results have less variations and the mean value of $\bar{A}_{fr+st}$ is the lowest among three flooding orders. Loose topology produces higher mean values than the tight topology, whereas in Figure 5 the SA counts are higher for tight topology.

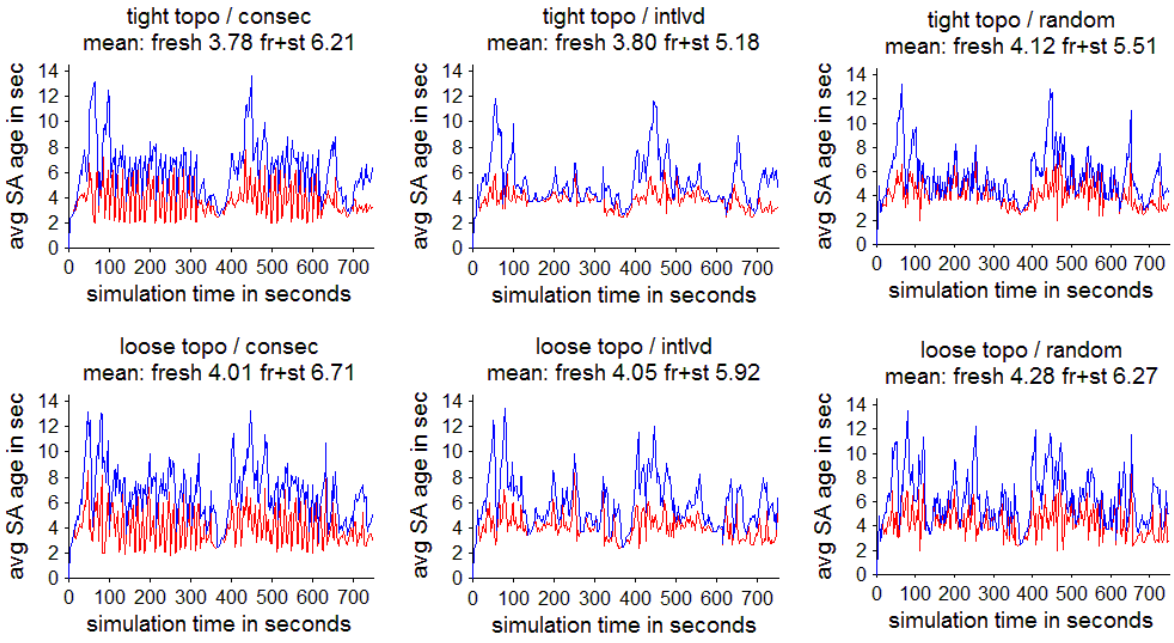

Figure 6: Average SA age – Fresh $\bar{A}_{fr}$ (in red) and Fresh-plus-Stale $\bar{A}_{fr+st}$ (in blue) for tight topology (above) and loose topology (below) in three different flooding orders.

While serving different purposes, both SA count and SA age should be considered when investigating the performance of an SA dissemination scheme. Both are dependent on the topology and mobility characteristics of a scenario, and provide different or complementary perspectives for performance quantification. For Scenario 3, in the loose topology case the scouting nodes frequently leave the group

resulting in a complete loss of connectivity for these node – this explains the increase in average SA age for all three schedulers (random, consecutive, and interleaved) in the loose topology.

Finally in Figure 7 we depict the average message count for transmitted and received SA messages $\bar{M}_{tr}$ and $\bar{M}_{rc}$, calculated over a sliding time window with size of T_{fresh} (in contrast, average SA count and SA age values in Figures 5 and 6 are calculated over the update interval τ). The tight topology cases have higher values in both $\bar{M}_{tr}$ and $\bar{M}_{rc}$ due to the better connectivity during the course of simulation. The peaks and troughs for received message count $\bar{M}_{rc}$ reflect separation and reunion of the two groups in the scenario. The peak value for $\bar{M}_{rc}$ is about 35 messages (over a 10s time window, the value of T_{fresh}). The values of average transmitted message count $\bar{M}_{tr}$ are basically determined by the size of connected network, with much less variations compared with the received message count $\bar{M}_{rc}$; furthermore, the transmitted message counts are not significantly affected by either the flooding order or the difference in topology (tight vs. loose).

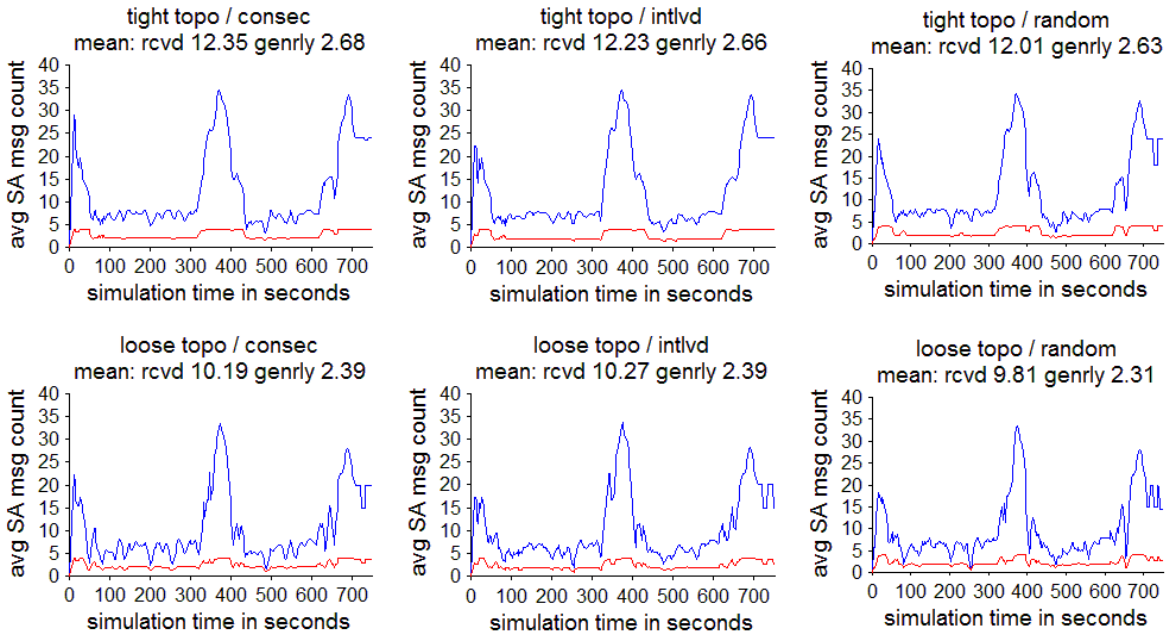

Figure 7: Average message count – Received $\bar{M}_{rc}$ (in blue) and Transmitted (generated/relayed) $\bar{M}_{tr}$ (in red) for tight topology (above) and loose topology (below) in three different flooding orders.

4 DISCUSSIONS AND CONCUSION REMARKS

Our simulation implementation for OSAP provides a flexible framework and platform for further studies on SA dissemination schemes in tactical MANETs. We applied our proposed SA performance metrics, defined in section 2.5, to the experimental results of the OSAP scheme in both static and mobile scenarios. While our focus was on the OSAP scheme, we believe that the SA performance metrics proposed and identified here would be valuable in analyzing the performance of other situational awareness dissemination techniques.

As expected, the performance of SA data delivery is impacted by the mobility pattern of wireless nodes and dynamic changes in topology which can affect network connectivity. The SA performance metrics we identified allow us to evaluate the quantity and quality of the SAs that are disseminated in particular scenarios. In the case of Scenario 3, for instance, we compared tight and loose topologies; the metrics helped us understand how differences between the network connectivity in both topologies can impact the delivery of situational awareness. The implication was not that "tight" is always better than

"loose" (in fact we tested similar scenarios with different sets of waypoints, and found that in some cases the loose topology provides better connectivity than in the tight topology), but that a standard set of metrics can help us to better interpret how well we are sharing information in the network.

The implementation of SA messaging in this work partly adopted the DSR route discovery process. Although no end-to-end routes were generated (because, by design, we omitted a legitimate destination node), it is nevertheless possible for a receiving node to obtain multiple valid routes leading to an initiating node through the list of intermediary hops – an ancillary benefit of using the OSAP scheme. A multi-path routing method can be developed using the candidate (unidirectional) routes. In addition, the existing SA information can be employed to meet specific security and policy requirements and provide a basis for secure routing or policy based routing. We will further investigate these applications in our future work.

The size of the SA message is an important cost factor: a metric we did not focus on in this paper. Although the SA message – containing a list of SA data – could conceivably be large in multi-hop cases, in tactical networks the total number of nodes is usually limited and within a manageable range; it is expected that the SA message will be relatively small in most circumstances. Moreover, various solutions can be explored to package the SA data in a compact form by efficient encoding techniques, such as the one described in Kidston and Rutagemwa (2011).

Finally we point out that the simulation methodology and software design presented in this work can be readily extended to investigate various SA dissemination algorithms other than the OSAP scheme, such as centralized broadcast and MPR-based (multi-point relay) broadcast schemes referenced in Brown, Salmanian and Li (2014). Comparison of OSAP with other SA dissemination schemes by means of the metrics proposed in this paper is a topic for future research.

REFERENCES

Böse, J-H., F. Bregulla, K. Hahn, and M. Scholz. 2005. "Adaptive Data Dissemination in Mobile ad-hoc Networks." In *GI Jahrestagung(2)'05*, edited by A. B. Cremers, R. Manthey, P. Martini, and V. Steinhage, 528–532. Bonn, Germany.

Brown, J.D., M. Salmanian, and M. Li. 2014. "Opportunistic Situational Awareness Dissemination at the Tactical Edge." In *Proc. of Military Communications Conference 2014*, Baltimore, MD (in press).

Clausen, T., and P. Jacquet. 2003. "Optimized Link State Routing Protocol (OLSR)." RFC 3626.

Crovella, L. 2002. "Introduction – Technical Overview and State of Art." In *Tactical Decision Aids and Situational Awareness*, RTO Lecture Series 227, NATO RTO-EN-019.

Endsley, M. 1995. "Toward a Theory of Situation Awareness in Dynamic Systems." *Human Factors Journal*, 237(1): 31–64.

Johnson, D., Y. Hu, and D. Maltz. 2007. "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4." Vol. 260. RFC 4728.

Kidston, D., and H. Rutagemwa. 2011. "A Location Service for VHF Tactical Networks." In *Proc. of Military Communications Conference 2011*, Baltimore, MD.

Larsen, E., L. Landmark, V. Pham, Ø. Kure, and P. E. Engelstad. 2010. "Optimized Group Communication for Tactical Military Networks." In *Proc. of Military Communications Conference 2010*, San Jose, CA.

Li, L., and P. Vigneron. 2010. "Properties of Mobile Tactical Radio Networks on VHF Bands." In *Proc. of the Information Systems and Technology Panel (IST) Symposium*, NATO RTO-MP-IST-092. Wroclaw, Poland.

Li, L., M. Shi, and T. Kunz. 2012. "Robust Networking for Bandwidth Constrained Mobile Tactical Radios." In *Proceedings. of Vehicular Technology Conference (VTC Spring)*, Tokohama, Japan.

Li, L., P Vigneron, C. Brown, M. Shi, and T. Kunz. 2012. "On Designing Bandwidth Constrained Mobile Tactical Networks for Complex Terrains." *Communications Magazine*, 50(2):188-194

Lipman J., H. Liu, and I. Stojmenovic. 2008. "Broadcast in Ad Hoc Networks." In *Handbook of Wireless Ad Hoc and Sensor Networks*, edited by S. Misra, I. Woungang and S. C. Misra, Chapter 6, 121-150. London: Springer-Verlag.

Marchini, M., M. Tortonesi, G. Benincasa, N. Suri, and C. Stefanelli. 2012. "Predicting Peer Interactions for Opportunistic Information Dissemination Protocols." In *Proc. of 17th IEEE Symposium on Computers and Communications (ISCC)*, 512-517. Cappadocia, Turkey.

SNT. 2008-2014. *QualNet and EXata/Cyber Network Simulator*. Scalable Networks Technologies, Los Angles, California. http://www.scalable-networks.com.

Vingelmann, P., F. H. P. Fitzek, and D. E. Lucani. 2010. "Application-level Data Dissemination in Multi-hop Wireless Networks." In *2010 IEEE Internaltional Communications Conference (ICC) Workshop*, Cape Town, South Africa.

Wang, H., B. Crilly, W. Zhao, C. Autry, and S. Swank. 2007. "Implementing Mobile Ad hoc Networking (MANET) over Legacy Tactical Radio Links." In *Proceedings. of Military Communications Conference 2007*, Orlando, FL.

Williams, B., and T. Camp. 2002. "Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks." In *Proc. of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc'02),* 194-205. Lausanne, Switzerland.

Zhang, X., T. Kunz, L. Li, and O. Yang. 2010. "An Energy-efficient Broadcast Protocol in MANETs." In *Proc. of Communication Networks and Services Research Conference(CNSR)*, IEEE, 199-206.

AUTHOR BIOGRAPHIES

MING LI is a Computer Scientist at Defence Research and Development Canada, Ottawa Research Center. He holds B.Sc. and M.Sc. degrees in Mathematics from Peking University, China and a Ph.D. degree in Computational and Applied Mathematics from Simon Fraser University, Burnaby, British Columbia, Canada. His email address is ming.li@drdc-rddc.gc.ca.

PETER C. MASON is a Defence Scientist at Defence Research and Development Canada, Ottawa Research Centre, and head of the Cyber Operations and Signals Warfare section. He is an Adjunct Professor with the University of Ottawa and the University of Ontario Institute of Technology, Oshawa, Ontario. He received a B.Sc. degree in Mathematics from Mount Allison University, Sackville, New Brunswick, Canada and the M.Sc. and Ph.D. degrees in Physics from McMaster University, Hamilton, Ontario, Canada. His email address is peter.mason@drdc-rddc.gc.ca.

MAZDA SALMANIAN is a Defence Scientist at Defence Research and Development Canada, Ottawa Research Center. He holds a Bachelor of Science degree in Electrical Engineering from The Ohio State University, Columbus, Ohio and a Master of Electrical Engineering degree from Carleton University, Ottawa, Ontario. His email address is mazda.salmanian@drdc-rddc.gc.ca.

J. DAVID BROWN is a Defence Scientist at Defence Research and Development Canada, Ottawa Research Center. He holds B.Sc. (Eng.) and M.Sc. (Eng.) degrees in Electrical and Computer Engineering from Queen's University, Kingston, Ontario, Canada and a Ph.D. degree in Electrical Engineering from the University of Toronto, Toronto, Ontario, Canada. His email address is david.brown@drdc-rddc.gc.ca.