DRDC-RDDC-2015-P084

Secure and Efficient Routing by Leveraging Situational Awareness Messages in Tactical Edge Networks

R. Song, J.D. Brown, H. Tang, and M. Salmanian
DRDC-Ottawa, Ottawa, Ontario, Canada

***Abstract*—A desired capability in military operations is the reliable and efficient sharing of Situational Awareness (SA) data at the tactical edge network. Many implementations of SA sharing in the literature use frequent broadcasts of SA messages in order to provide an up-to-date and comprehensive operating picture to all nodes. However, SA sharing may result in an increase in bandwidth requirements at the tactical edge, where power and bandwidth are scarce. Efficient realtime routing is also a challenge in a tactical edge network. We believe there is a good opportunity to leverage the realtime periodic SA messages for assisting routing services. To the best of our knowledge, little research has been done on this front. In this paper, we propose a secure and efficient routing by leveraging SA messages (SER-SA) in tactical edge mobile ad hoc networks. The SER-SA protocol utilizes realtime broadcast SA messages to not only transmit SA data but also to facilitate Multipoint Relay (MPR) node selection and route discovery for providing both realtime broadcast and unicast communication services. In SER-SA, broadcast forwarding is performed only by MPR nodes, which can reduce bandwidth usage compared to pure flooding methods such as Multicast Ad hoc On-Demand Distance Vector Routing (MAODV). In addition, we reduce bandwidth usage even further by both avoiding dissemination of specific designated routing messages in the network and enhancing the (traditionally local) MPR selection algorithm based on a global algorithm enabled by the shared global SA. We show through simulations that the proposed SER-SA protocol facilitates route discovery in a more bandwidth efficient manner. As a result, it performs better in terms of delivery ratio for providing both broadcast and unicast services in tactical scenarios compared to the existing MANET multicast routing protocols such as Multicast Optimized Link State Routing and MAODV.**

I. Introduction

Sharing Situational Awareness (SA) among allied (or "blue force") units is an important function in tactical operations, helping to enable the availability of a common operating picture (COP) for commanders and soldiers. The SA information—which can consist of data such as a user's location, identity, and status—is typically broadcasted periodically to ensure the COP is both up-to-date and complete. According to Thomas Hammel [1], broadcast messages of SA data among tactical units in a local area (of roughly the size of a platoon) are expected to occupy up to 75% of total tactical traffic in the near future. However, communication at the tactical edge (both broadcast and unicast) is complicated by the fact that nodes at the tactical edge face unreliable wireless links, and limited bandwidth and power. Mobile Ad Hoc Network (MANET) is seen as a promising technology that may help facilitate range extension in tactical networks, allowing multi-hop network connectivity to remote nodes as well as self-organization to all nodes to support on-the-fly network configuration. Despite these advantages, it is an open problem how to best and efficiently disseminate periodic time-sensitive SA messages among nodes in a tactical edge mobile ad hoc network (TEN), while at the same time providing both realtime broadcast and dynamic end-to-end unicast traffic (i.e., non-SA traffic) in a single protocol.

Although many efficient data collection and disseminating methods are proposed for wireless sensor networks (WSNs) recently (e.g., [2–4]), they do not satisfy the requirements of communication in TENs. For instance, a TEN needs to provide realtime unicast service for communications between any two nodes at any time, which usually is not a requirement in WSNs. A TEN usually has less than 50 nodes (e.g., a Platoon size) with longer transmission range (e.g., 1km) distributed in an area (e.g., 2km X 2km); nodes are mobile, resulting in network topology changes. The bandwidth of tactical networks is scarce and the nodes use more power for transmitting signals. For instance, the tactical narrowband waveform has data rate less than 30 kbps [5–7], and the soldier radio waveform has data rate less than 1 Mpbs [8, 9]. The overhead of most existing proactive routing protocols (used for providing both realtime broadcast and unicast communications in MANETs) occupies a lot of network bandwidth, and the redundant MPRs created by these protocols (e.g., MOLSR) make broadcast traffic very inefficient on network bandwidth usage.

This paper introduces a new routing protocol called Secure and Efficient Routing by Leveraging Situational Awareness Messages (SER-SA). The main idea of the SER-SA protocol is to use periodic realtime SA messages as a mechanism to not only disseminate blue-force SA, but also to provide global network topology information to all nodes; the nodes in turn use the global topology information for proactive routing of realtime broadcast and unicast traffic. Instead of designing a designated routing (with extra traffic overhead) for providing SA disseminating service as in [3, 4, 10, 11], SER-SA utilizes SA messages for providing realtime routing services in TENs. SER-SA takes advantage of the fact that network-wide knowledge of SA information can be used to perform global network enhancements (i.e., global MPR consolidation) which improve broadcast efficiency. In general, disseminating SA is an additional "cost" to the network (compared to the case where no SA is disseminated). However, we submit that in military networks (such as TENs) that have a requirement to disseminate SA, it is sensible to use the additional global information judiciously and provide global efficiencies, where possible. Figure 1 depicts the strategy of SER-SA compared with the traditional methods for providing SA and non-SA traffic (i.e., broadcast and unicast traffic) services in a TEN. SER-SA can reduce by over 50% the number of MPR nodes in a TEN, and consequently the resulting broadcast bandwidth usage, compared with the existing popular proactive MANET routing protocols such as OLSR [12] and MOLSR [10]. This global MPR consolidation method outperforms other existing MPR reduction algorithms such as those proposed in [13, 14].

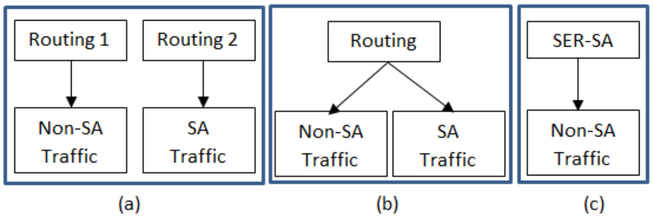

Fig. 1. The strategies for providing SA and non-SA traffic services in a TEN: (a) traditional separated routing, (b) traditional single routing, (c) SER-SA.

The rest of the paper is organized as follows. A TEN scenario under consideration is introduced in the next section. In Section III, the SER-SA protocol is discussed including MPR selection, SER-SA network topology acquisition, MPR consolidation and maintenance, and SER-SA self-healing under mobility. The performance of SER-SA is simulated in Section IV, and compared against other protocols such as MOLSR and MAODV. Finally, concluding remarks are given in Section V.

II. TEN Scenario

In this paper, we consider a TEN serving a light infantry platoon. This light infantry platoon consists of approximately forty to sixty members. In our scenario, local SA messages need to be distributed through the TEN such that all members have SA about all other members; we assume that this is achieved through some form of broadcast. This scenario is consistent with the vision presented in [1, 15]. The following additional assumptions have been adopted in this research.

- TEN Size: The TEN consists of 40 to 60 mobile nodes;
- Node Distribution: The mobile nodes are randomly distributed in a pre-defined area;
- Frequency of SA Messages: Each node generates and broadcasts its locally-generated SA message every 5 seconds;
- Traffic: Broadcast messages account for majority of the total traffic in the TEN, where the remaining traffic is unicast. The broadcast traffic consists of SA messages and global broadcast messages such as General Orders. Unicast messages consist of multimedia data such as text, voice, or video packets.

III. Secure and Efficient Routing by Leveraging Situational Awareness Messages

The SER-SA protocol provides a secure and efficient mechanism for jointly delivering broadcast SA, performing MPR selection and route discovery for non-SA traffic in a TEN by utilizing periodically broadcasted situational awareness messages. This section describes the operation of SER-SA in detail. We have divided the description into five parts:

(A) *Situational awareness message security*: describes the general structure of an SA message with security protection;

(B) *SER-SA SA dissemination, MPR selection, and topology sharing*: describes how MPRs are initially selected based on the SA messages; how SER-SA uses the SA messages and MPR information to maintain a global situational awareness picture at every node;

(C) *SER-SA MPR consolidation and maintenance*: describes a global MPR reduction process; this global reduction process is unique to SER-SA and is enabled by the global situational awareness that is provided to each node. This is one of the primary contributions of this paper;

(D) *SER-SA network self-healing under mobility*: describes how nodes change their MPR status under mobility conditions to make sure the network connection self healed quickly;

(E) *Broadcast and unicast routing*: describes how SER-SA facilitates broadcast and unicast of non-SA traffic.

A. Situational Awareness Message Security

In future TENs, it is believed that situational awareness messages such as location and health vitals will be generated and broadcasted by each mobile node every few seconds [16] for blue force tracking. These SA messages contain sensitive information and must be protected by cryptographic mechanisms regardless of whether or not the provided routing protocols are protected. Key management and cryptographic strategy for TENs is out of scope of this paper. Here, we present a general security protection structure of an SA message in TENs.

In the above TEN scenario, we assume each SA message encrypted with a group traffic encryption key ($GTEK$) and broadcasted to all other members in the TEN. Without loss of generality, the SA broadcast message can be sent with the following format: $\{(SA)_{GTEK}, N, H_{GTEK}\}$ or $\{(SA)_{GTEK}, N, SIG_{src}\}$, where the encryption, $(SA)_{GTEK}$, protects the SA, and the integrity is protected by the nonce, N, and keyed hash (H_{GTEK}) or signature (SIG_{src}) depending on the protection level and security policy in the TEN.

B. SER-SA SA Dissemination, MPR Selection, and Topology Acquisition

We present how SER-SA uses SA messages to select MPRs, learn the network topology, and share situational awareness. In this section we explain how an appropriately structured SA broadcast message can be used for these purposes: (1) to disseminate SA in the TEN as a fundamental requirement, (2) to obtain a 1- and 2-hop neighbor list of each node (for MPR selection), and (3) to calculate a TEN topology that will enable the creation of a routing table. The periodic SA message can effectively replace dedicated routing messages such as Hello and TC in MOLSR, and RREQ and RREP in MAODV. These messages of existing standards are designed to carry more information (e.g., neighbour list) than what we propose with flags for the same purpose. We propose two stages of operation whereby the SA messages are used for an “MPR Selection Stage”, when the network is initiated, and then are used for a “Topology Acquisition Stage” once the initial MPRs have been identified. The duration of each stage can be set by policy and may depend upon network size and mobility. Early experimentation suggests that an MPR Selection Stage of 15 seconds is appropriate for the networks we explored (i.e., each node generates and broadcasts its own SA messages every 5 seconds for 3 times).

B.1) SER-SA MPR Selection Stage

In the SER-SA MPR Selection Stage, each node builds its 1-hop and 2-hop neighbour list based on the hop flag inserted into the SA message, and further selects its MPR nodes based on the greedy algorithm presented in [17]. When a TEN is initiated, each mobile node (e.g., node A) periodically generates and broadcasts the following SA message (in which we insert two flag status F to the original SA message format) to its neighbors, according to a period defined by policy:

$$\{S_A, f\}, \{(F_{stage}, F_{hops}, SA)_{GTEK}, N, H_{GTEK}\}.$$

The first part of the message contains header information; specifically, the source address S_A of the node A, and the broadcast address f (indicating that this is a broadcast, not unicast, message). The second part of the message is the SA payload information, containing a nonce or timestamp denoted by N, SA data denoted by SA, two “flags” to indicate the protocol’s current operating state denoted by F_{stage} and F_{hops}, and a hash keyed over the whole message denoted by H_{GTEK}, where SA data and two flags are encrypted with the group traffic encryption key denoted by $(F_{stage}, F_{hops}, SA)_{GTEK}$. More detail about the flags are provided below.

The F_{stage} flag is used to indicate whether the protocol is operating in the MPR Selection Stage or the Topology Acquisition Stage. In the MPR Selection Stage, the F_{stage} flag is set to 0. The F_{hops} value is employed to allow nodes in the network to determine their distance from the source node, A, in terms of number of hops. F_{hops} is set to 1 when the source node (A in our case) broadcasts the above SA message. If another node, B, receives this message, it will change the F_{hops} value to 2, recalculate the hash value H_{GTEK}, and re-broadcast the changed SA message to its neighbors. Nodes receiving an SA message with F_{hops} set to 2 will set F_{hops} to 0, recalculate the hash and re-broadcast. Further rebroadcasts will leave the F_{hops} value set to 0. We note that in the MPR Selection Stage, the broadcast of SA is performed as flooding such that each node in the network will have forwarded the above message exactly once. The purpose of the MPR Selection Stage is twofold: it serves to allow nodes in the network to determine their 1- and 2-hop neighbours, while at the same time disseminating SA. It uses a pure flooding mechanism to disseminate the SA. Although pure flooding is an inefficient way to disseminate broadcast information, it is used only in the MPR Selection Stage; in the subsequent stage a more efficient broadcast is proposed. Flooding is necessary initially in order to simultaneously disseminate SA and perform initial MPR selection. Based on the SA messages, each node will obtain SA about the network and will calculate its 1-hop and 2-hop neighbors based on the following rules:

(1) A node will forward a unique SA broadcast message only once. Specifically, upon receiving an SA broadcast message, a node will examine the source address and the nonce–if it has already forwarded the message it will not re-broadcast it;

(2) Each node adds the source address of an SA message to its 1-hop list if it receives the SA message with $F_{hops} = 1$;

(3) Each node adds the source address of an SA message to its 2-hop list if it receives the SA message with $F_{hops} = 2$ and if the source node is not already listed on its 1-hop list. When adding the source address to its 2-hop list, the node will also note the 1-hop neighbour that sent the message. Note that a 2-hop neighbor may be associated with multiple 1-hop neighbors;

(4) A node makes no changes to its 1-hop and 2-hop list if it receives an SA message with the F_{hops} value set to 0.

After each node has initiated several SA broadcasts, all the nodes in the TEN should have a complete list of their 1-hop and 2-hop neighbours (and knowledge of the routes to the 2-hop neighbours). Once a node has built its 1-hop and 2-hop neighbour list it will locally compute its MPR nodes based on the greedy algorithm presented in [17]. After a pre-defined condition occurs (e.g., a certain time elapses), nodes will enter the Network Topology Acquisition Stage, as described below.

B.2) SER-SA Network Topology Acquisition Stage

In the Network Topology Acquisition Stage, each node learns the network topology based on the MPR information inserted into the SA message, and further builds its routing table based on the topology information and Dijkstra’s algorithm [18]. When a TEN enters the network topology acquisition stage, each mobile node (e.g., node A) periodically generates and broadcasts the following SA message (in which we insert three flag status F and 1-hop MPR info to the original SA message) to its neighbors in order to share SA, MPR information, and any changes to network topology or MPR state.

$$\{S_A, f\}, \{(F_{stage}, F_{M1}, F_{M2}, B_1, ..., B_n, SA)_{GTEK}, N, H_{GTEK}\}$$

The first part of the message is the same as that in the MPR Selection Stage (i.e., source address S_A and broadcast address f). The second part of the message contains the stage flag F_{stage} (where F_{stage} is set to 1 for this stage), the SA data, the nonce, and the hash as before; in addition, there are three new data fields: two MPR flags F_{M1} and F_{M2}, and a 1-hop MPR nodes field $\{B_1, ..., B_n\}$, as described below.

The values of F_{M1}, F_{M2}, and $\{B_1, ..., B_n\}$ are used for nodes to share information with the entire network regarding their own MPR status, their 1-hop MPR set status, and the identities of their current 1-hop MPRs. When initiating an SA message, a node follows the following rules in populating F_{M1}, F_{M2}, and $\{B_1, ..., B_n\}$:

(1) F_{M1} is set to 0 if a node is uncertain of its own MPR status (i.e., the node does not know whether or not it is serving as an MPR for one of its 1-hop neighbours); the node populates $\{B_1, ..., B_n\}$ with the source addresses of its known 1-hop MPR nodes;

(2) F_{M1} is set to 1 if a node is not an MPR for any of its neighbours; the node populates $\{B_1, ..., B_n\}$ with the source addresses of its known 1-hop MPR nodes;

(3) F_{M1} is set to 2 if a node is an MPR for at least one of its neighbours; the node populates $\{B_1, ..., B_n\}$ with the source addresses of its known 1-hop MPR nodes

(4) F_{M2} is set to 0 if the 1-hop MPR set of a node has not changed since its last update; the node leaves $\{B_1, ..., B_n\}$ empty, with the understanding that the status is unchanged since last update.

(5) F_{M2} is set to 1 if the 1-hop MPR set of a node has changed since its last update; the node populates $\{B_1, ..., B_n\}$ with the source addresses of its known 1-hop MPR nodes.

In addition, each node forwards SA messages and calculates the MPR connections of other MPR nodes based on the following rules:

(1) Each non-MPR node does not forward SA broadcast messages which are set to the network topology acquisition stage (i.e., with $F_{stage} = 1$) except the network connection healing messages under mobility condition (see detailed info in Section III.D);

(2) Each MPR node forwards SA broadcast messages with $F_{stage} = 1$ to its MPR neighbors without any change. An MPR node can check whether or not it has forwarded the message by examining the source address and nonce of the message;

(3) Based on the information contained in the F_{M1} and $\{B_1, ..., B_n\}$ data fields, each MPR node calculates the number of MPR connections held by all other MPR nodes; for instance, if an SA message from node A has $F_{M1} = 2$ then the cardinality of $\{B_1, ..., B_n\}$ gives the number of MPR connections for A;

(4) Each MPR node calculates the network topology and routing tables based on the same method used in OLSR.

At this point, once the MPR Selection Stage has completed and the Network Topology Acquisition Stage has had a chance to run for a few seconds, any broadcast message (including SA messages) can be delivered to all nodes in the network by relying on the MPR nodes to forward the message; likewise, any unicast message can be delivered to its destination with shortest path based on the routing tables calculated by each node with Dijkstra's algorithm [18]. This is accomplished using only SA messages to achieve both dissemination of SA and the computation of MPRs and routes. However, we have not yet discussed how SER-SA responds to mobility, nor have we reduced the number of MPR nodes through the global consolidation process discussed in the next Section.

The MPR selection performed by OLSR, MOLSR, and performed by SER-SA in the MPR Selection Stage of SER-SA is a local selection; consequently, this MPR set contains redundant MPR nodes that can be removed from the MPR set without reducing network coverage. For instance, based on our simulations in MATLAB, in a network over 40 nodes randomly distributed in a (2km X 2km) square field with over 700 meters radio transmission range of each node, over 50% of the locally computed MPRs are redundant when compared to our proposed globally computed MPR set. If we can reduce the number of MPR nodes in the network, this means we can also reduce the retransmissions of broadcast traffic. This is discussed in the following section.

C. SER-SA MPR Consolidation and MPR Maintenance

Unlike a pure flooding technique, relying on MPRs for forwarding can reduce broadcast messages in the network. A smaller MPR set results in fewer retransmissions required. Minimizing the MPR set is quite desirable and has been extensively researched. Qayyum et al. [17] have proved that selecting the minimum MPR set is an NP-complete problem. Several MPR set reduction solutions have been proposed. For instance, Li et al. [13] proposed a necessary first algorithm (NFA), which can reduce the number of MPR nodes in the network by 0.7% up to 11.2% under different scenarios when compared to the original greedy algorithm [10, 17]. Bai et al. [14] proposed a method based on node density, which can reduce approximately 10% of MPR nodes when compared to the original greedy algorithm. In both cases, however, these methods require the network to have a very high density, in order to reach a 10% MPR reduction (e.g., NFA requires 75 1-hop neighbors per node on average), which is not the case in our scenario.

We propose an alternate method to reduce the MPR set size. Unlike the above solutions, which reduce MPR nodes from the point of view of each source node, our method uses the entire network topology and reduces the MPR set using a centralized "global" algorithm. The centralized algorithm takes advantage of the fact that network-wide SA can provide more than just 1-hop and 2-hop knowledge, that allowing for a global-level MPR node reduction. The MPR reduction procedure begins after all nodes have had a chance to report their MPR status (i.e., they have sent an SA message with $F_{M1} = 1$ or $F_{M2} = 2$) and report on their locally computed MPRs (i.e., they have included the data field $\{B_1, ..., B_n\}$ in their SA message).

The following steps are performed to reduce the MPR set using a centralized algorithm. Note that the network is operating in the Network Topology Acquisition Stage when this algorithm is performed (i.e., $F_{stage} = 1$).

(1) A Group Controller (GC) in a TEN network creates an ordered list of all MPR nodes, sorted by the number of the MPR connections (i.e., the cardinality of the set $\{B_1, ..., B_n\}$). It then carries out the following MPR reduction procedure. All MPR nodes continue operating as normal until they receive further instructions from the GC node;

I. Check the MPR node with the smallest number of MPR connections (i.e., cardinality of $\{B_1, ..., B_n\}$ is smallest);

II. Delete the MPR node in Step I if this deletion would neither reduce the coverage of the network nor break network connection by the remaining MPRs[1];

III. Repeat Steps I and II for each MPR in the network, working up towards the MPR with largest number of connections until all MPRs have been checked.

(2) The GC node creates a list of MPRs that could be deleted without affecting network coverage. The GC node then broadcasts the following MPR reduction message throughout the network:
$\{S_{GC}, f\}, \{(F_{stage}, F_{M1}, B_1, ..., B_n)_{GTEK}, N, SIG_{GC}\}$
where $F_{stage} = 1$ and $F_{M1} = 3$ indicating that this is an MPR reduction message and $\{B_1, ..., B_n\}$ are the MPR

[1] Note that it is possible for the GC node to determine the coverage offered by a reduced MPR set based on knowledge of the MPRs of all nodes in the network. The sharing of F_{M1} and $\{B_1, ..., B_n\}$ by all nodes in the network in the Topology Acquisition Stage makes it possible for the GC node to compute a connectivity graph for all nodes and MPRs.

nodes to be disabled;

(3) An MPR node disables its MPR function if it receives the MPR reduction message and it is on the MPR disable list, i.e., the MPR node changes its flag value of F_{M1} from 2 to 1, and updates its MPR status through its SA message;

(4) Each node (including both MPR and non-MPR) deletes the MPR nodes (who are on the MPR disable list) from its 1-hop MPR set when it receives the MPR reduction message, i.e., the node sets its flag value of F_{M2} to 1, and updates its 1-hop MPR set status through its SA message;

(5) The MPR reduction process will repeat as necessary based on a pre-defined trigger. The reduction can be triggered by a threshold such as a timer (e.g., every X minutes) or percentage of increase in the number of MPR nodes (e.g., after the number of MPR nodes has increased by 20%) due to mobility. The MPR reduction can start from the current MPR stage, or it may require the network start over in the MPR Selection Stage depending on the battlefield operational requirements.

As will be discussed in section IV, simulations in MATLAB show that the SER-SA global consolidation of MPR selection can reduce the number of MPRs in the network by over 50% depending upon topology and density. Note that reducing MPRs does not affect the load of the remaining MPRs for forwarding broadcast traffic; regardless of how many MPRs are in the network, each MPR node needs to forward all broadcast traffic to its neighbors. The MPR reduction, however, may affect the load of some MPRs on forwarding unicast traffic. As we mentioned before, different from traditional Internat traffic pattern, broadcast messages occupy the majority of total tactical traffic in TENs. That means the redundant MPRs can cause more congestion in their local area for forwarding the majority broadcast traffic than that caused by unicast traffic.

D. SER-SA Network Connection Self-Healing Under Mobility

To account for the mobility of each node in a TEN, the SER-SA protocol uses the following strategy for quick network connection self-healing in case of the MPR set of a node is changed under mobility. Note that the SER-SA network connection self-healing is operating under the Network Topology Acquisition Stage as well (i.e., $F_{stage} = 1$).

For a non-MPR node, it changes and updates its 1-hop MPR set based on the following rules when its 1-hop MPR set is changed during mobility:

(1) The non-MPR node updates its current available MPR set through SA message (i.e., set $F_{M2} = 1$) if it has at least one 1-hop MPR available during mobility.

(2) The non-MPR node selects one of its 1-hop nodes that has the most MPR connections (and higher ID if they have same MPR connections) as its MPR to connect it to the network if it does not have any existing 1-hop MPRs available. The non-MPR node updates its 1-hop MPR set through its SA message (i.e., add the node to its 1-hop MPR list and set $F_{M2} = 1$). The node selected as MPR needs to updates its MPR status as well (i.e., change its F_{M1} value from 1 to 2).

For an MPR node, it changes and updates its 1-hop MPR set based on the following rules when its 1-hop MPR set is changed during mobility:

(1) The MPR node updates its current available MPR set through SA message (i.e., set $F_{M2} = 1$) if the MPR node has at least one 1-hop MPR available during mobility and the network connection is not broken.

(2) The MPR node updates its MPR set based on the following rules if the network connection is broken during mobility:

I. The MPR node (who lost connections through its subnet with other MPRs listed in its 1-hop MPR set) first checks whether its subnet has common 1-hop nodes with the subnets of the lost connected MPRs. If there is, it selects one or more (as needed for healing broken connections in case of more than 2 broken subnets) of the common 1-hop nodes that have the most MPR connections (and higher ID if they have same connections) as MPR nodes, creates and sends unicast MPR selection messages to the selected MPR nodes. The new selected MPR nodes update their MPR status after receiving the MPR selection messages.

II. If there is no common 1-hop node available between the subnets of the lost connected MPRs after Step I, the lost connected MPRs generate a network connection healing message with F_{M2} value set to 3 and insert a healing flag $F_h = 1$ into the healing message. They list the lost connected MPRs that cannot be reached into the healing message, and broadcast the healing message to their subnets. Each node processes the healing message based on the following rules once receiving the message

i Each MPR node rebroadcasts the healing message with $F_h = 1$ only once without any change;

ii Each non-MPR node changes the value of F_h from 1 to 2, and rebroadcasts the changed healing message to its 1-hop neighbours after it receives the healing message with $F_h = 1$.

iii Each MPR nodes ignores the healing message with $F_h = 2$.

iv Each non-MPR node checks whether its subnet contains the MPRs listed in the lost connection list once it receives a healing message with $F_h = 2$. If not, it drops the message. If its subnet contains the MPRs listed in the healing message, it sets itself as MPR and updates its MPR status. At the same time, it selects the non-MPR node (who rebroadcasts the healing message to it) as MPR node, creates a MPR selection message, and sends the MPR selection message to the non-MPR node.

E. SER-SA Broadcast and Unicast Routing

In the SER-SA protocol, each node recalculates its routing table based on the updated network topology and the Dijkstra's algorithm [18], and both broadcast and unicast messages will be forwarded by MPR nodes only. For broadcast messages, each MPR node first checks whether it already broadcasted the message after it received the message. If so, it drops the message. If not, then it broadcasts the message to all its neighbours. For all unicast messages, each node delivers all unicast messages based on its updated routing table.

IV. SER-SA Performance

In order to evaluate the performance of the SER-SA protocol, we conducted simulations in both MATLAB and

NS-2. MATLAB was used to examine the percentage of reduction in the number of MPR nodes that could be achieved using the global reduction algorithm presented in III.C as opposed to a local greedy algorithm for MPR selection. NS-2 simulations were used to evaluate the bandwidth usage and delivery ratio of SER-SA and to compare with the existing popular proactive routing protocol MOLSR and reactive routing protocol MAODV which can provide both broadcast and unicast services in a single protocol. The simulation scenarios and results are described below.

A. SER-SA MPR Consolidation Performance

We simulated the SER-SA MPR reduction algorithm in MATLAB, where networks with 40 to 60 nodes were created with nodes randomly distributed in a square field. Simulations of each network size (i.e., 40 nodes, 50 nodes, and 60 nodes) were run 500 times with different network scenarios (i.e., each run with different network topology created by random algorithm) and the results were averaged. Table 1 presents simulation results showing the percentage of MPR reduction obtained by the SER-SA protocol after running the global reduction algorithm. From Table 1, we can see that our proposed MPR consolidation method can achieve promising results at much lower densities than the methods proposed in [13, 14]. For instance, with 50 nodes, SER-SA achieves 20% MPR reduction when nodes have an average of four 1-hop neighbors and can reach a reduction of over 58% when the average 1-hop neighbors per node reaches 20.

TABLE I. PERCENTAGE OF MPR REDUCTION BY SER-SA

Number of Nodes in Network	Average 1-hop Neighbors per Node	Ratio of Average 1-hop Neighbors to Total Number of Nodes	MPR Reduction Percentage by SER-SA
40	4	10%	20%
40	8	20%	46%
40	12	30%	52%
40	**16**	**40%**	**54%**
50	4	8%	21%
50	8	16%	46%
50	12	24%	54%
50	**20**	**40%**	**58%**
60	4	7%	22%
60	8	13%	48%
60	12	20%	56%
60	**24**	**40%**	**60%**

Figure 2 depicts the average percentage in MPR reduction achieved by SER-SA (compared to the greedy algorithm) as a function of the average number of 1-hop neighbors, where once again nodes are randomly distributed over a square field. The simulation shows that the proposed MPR reduction method reaches peak effectiveness when the ratio of average 1-hop neighbors to the total number of nodes in the network reaches approximately 40%.

B. SER-SA Bandwidth Usage and Traffic Delivery

Next, we simulated the performance of SER-SA under mixed traffic conditions, i.e., the traffic used in the simulation contains 75% SA broadcast messages, 5% General Order broadcast messages, and 20% unicast messages as described in [1]. In particular, we were interested in the bandwidth usage, traffic forwarding load, and traffic delivery ratio of SER-SA. We compared the bandwidth usage, traffic forwarding load, and traffic delivery ratio of SER-SA to MOLSR and MAODV. Due to a lack of network simulation platform with soldier radio waveform model for TENs, we use NS-2.35, 802.11b low data rate with long range transmission instead. The simulation setup is described below.

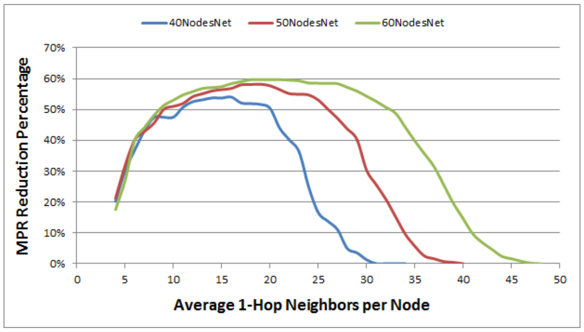

Fig. 2. SER-SA MPR reduction percentage over greedy algorithm by average 1-hop neighbors and their related network size.

- Simulation Platform: NS-2.35;
- Communication Channel: 802.11b with 1 Mbps data rate and 900 meters transmission range;
- Node Distribution: 50 nodes were randomly distributed in a (2km X 2km) square field in NS-2;
- SA Broadcast Message: Each node periodically sent a SA broadcast message every 5 seconds. Each SA message is 64 Bytes, which is big enough for transmitting geolocation and other vital SA information;
- General Order Broadcast Message: In order to simulate 5% General Order (GO) broadcast traffic, we indicated one node to periodically generate and broadcast a 210 Byte GO message every 5 seconds;
- Unicast Message: We randomly chose four source and destination nodes for generating unicast traffic. The total unicast payload traffic occupies 20% of the total traffic in the network;

The performance metrics include bandwidth usage, traffic forwarding load, and traffic delivery ratio for each node, which are defined below.

- Bandwidth Usage: The amount of data transmitted and received by a node including all inbound and outbound traffic such as routing and application data. It is calculated as the total inbound and outbound traffic by each node divided by the simulation time. Note that the bandwidth usage is calculated in network layer only. It does not include the lower layer overhead such as MAC layer frame, Physical layer preamble, etc.;
- Traffic Forwarding Load: The average load for forwarding the mixed traffic (broadcast and unicast) by each node during a simulation period. It is calculated as the total forwarded traffic (in Bytes) by each node divided by the simulation time;
- Traffic Delivery Ratio: The ratio of total received traffic (in Bytes) by each node to the total traffic sent to the node. Note that here the traffic includes SA, GO broadcast, and unicast messages only.

Figure 3 depicts the bandwidth usage on each node for delivering the mixed traffic with the SER-SA, MOLSR, and

MAODV protocols. Figure 4 depicts their maximum, minimum, and average bandwidth usage. Figure 3 and 4 show that the SER-SA protocol can save over 50% bandwidth on delivering the mix traffic comparing with using the MOLSR protocol. It also uses less bandwidth when compared to the MAODV protocol.

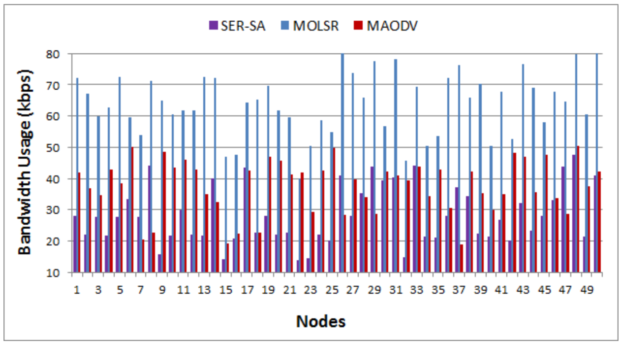

Fig. 3. The bandwidth usage on each node for delivering the mix traffic with the SER-SA, MOLSR, and MAODV protocols.

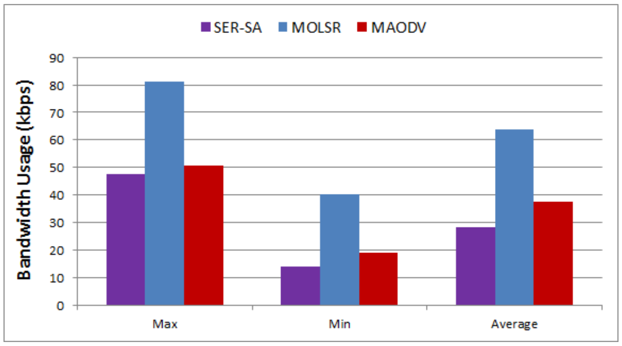

Fig. 4. The maximum, minimum, and average bandwidth usage for delivering the mix traffic with the SER-SA, MOLSR, and MAODV protocols.

Figure 5 depicts the traffic forwarding load of the SER-SA, MOLSR, and MAODV protocols for each node. Figure 6 depicts number of nodes used for forwarding the mixed traffic in each protocol. Figure 5 and 6 show that every node in MAODV is involved in traffic forwarding. The traffic forwarding load in MAODV is over 6 kbit/s on average. In MOLSR, there are 42 MPR nodes forwarding the traffic. In SER-SA, there are only 9 MPR nodes forwarding the traffic since the global MPR reduction is performed in SER-SA. Even with over 70% MPR reduction compared to MOLSR, SER-SA still provides 2-4 redundant MPRs in Figure 6 based on the lower bound of MPR set [17] for providing the redundancy, diversity, and connectivity of TENs.

Figure 7 depicts the traffic delivery ratio of the SER-SA, MOLSR, and MAODV protocols for delivering the mix traffic. Figure 8 depicts their maximum, minimum, and average traffic delivery ratio. Figure 7 and 8 show that SER-SA has much better performance on traffic delivery ratio when compared to MAODV. The reason for this improvement over MAODV is that the increase in retransmissions in MAODV can result in more collisions in the network, where broadcast messages are not guaranteed. SER-SA has similar delivery ratio with MOLSR.

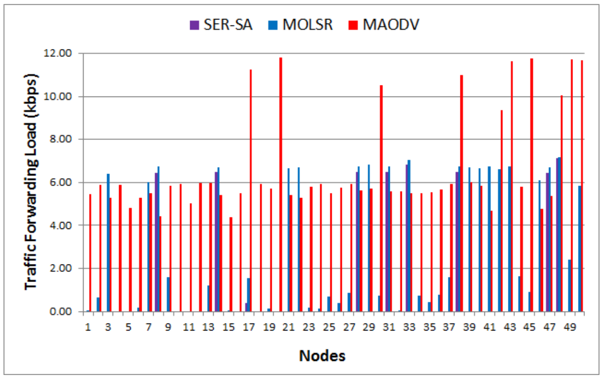

Fig. 5. The traffic forwarding load of SER-SA by each node compared with MOLSR and MAODV.

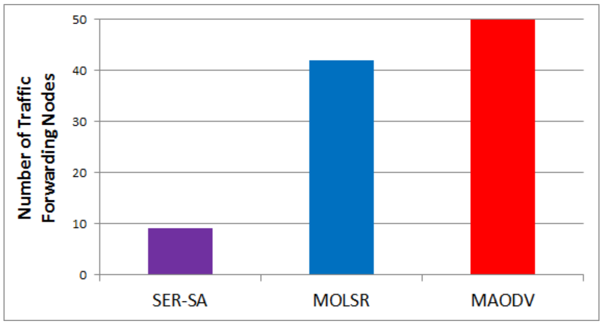

Fig. 6. Number of nodes used for forwarding the mixed traffic in SER-SA, MOLSR, and MAODV protocols.

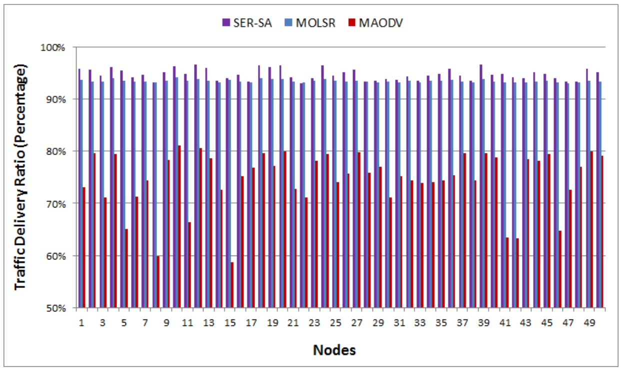

Fig. 7. The traffic delivery ratio of the SER-SA, MOLSR, and MAODV protocols for delivering the mix traffic.

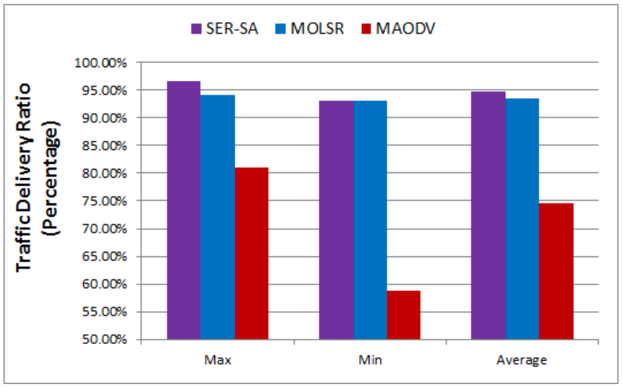

Fig. 8. The maximum, minimum, and average traffic delivery ratio for delivering the mix traffic with the SER-SA, MOLSR, and MAODV protocols.

Given the results, SER-SA has better performance on bandwidth usage, traffic forwarding load, and traffic delivery ratio in TENs compared to MOLSR and MAODV protocols. It saves over 50% bandwidth on delivering mixed traffic in a TEN compared to MOLSR without degrading the traffic delivery ratio, and has much better traffic delivery ratio compared to MAODV. SER-SA adds certain complexity with its global MPR consolidation process. Considering a TEN has less than 60 nodes, it only causes less than one second delay based on our testing and simulation in MATLAB. In addition, the built-in security of SA messages in SER-SA at the same time protects the routing information (e.g., 1- and 2-hop neighbors, network topology) against external attacks. The built-in security reduces the overhead of the security functions used to protect routing messages in the traditional routing protocols such as in [19, 20].

V. Conclusion

In order to provide both secure and efficient routing and situational awareness sharing services in mobile tactical edge networks, we propose the SER-SA protocol, which utilizes secure and periodically broadcasted SA messages for MPR node selection and routing table calculation, avoids routing messages on the network, and protects network-related information such as topology by the built-in security of SA messages. In addition, we propose a centralized MPR node reduction algorithm to further reduce node carried load in the network. Based on simulations with MATLAB and NS-2, we demonstrated that SER-SA improves performance greatly on bandwidth usage and delivery ratio when compared to exiting popular routing protocols such as MOLSR and MAODV.

We note that SER-SA obtains its efficiency gains by capitalizing on globally available situational awareness, which allows for a reduction in the number of MPRs in the network when compared to a local MPR selection algorithm. The SER-SA protocol provides a potentially valuable solution for future military networks in which global situational awareness may soon be a requirement, since SER-SA proposes to transmit SA in an efficient fashion whereby the knowledge of SA can be used to improve broadcast efficiency and to avoid routing traffic.

We believe that SER-SA has great potential for increased efficiency in routing and situational awareness sharing in TENs. We will continue to enhance the protocol and study its performance, examining the impact of mobility and other features.

Acknowledgement

The authors would like to thank Kathryn Perrett and Peter C. Mason for their helpful comments and review.

References

[1] T. Hammel, *Farther Out Networking*, August 7, 2013. Retrieved from http://www.darpa.mil/WorkArea/DownloadAsset.aspx?id =2147487187.

[2] D.P. Dubhashi, O. Hggstrm, L. Orecchia, A. Panconesi, C. Petrioli, and A. Vitaletti, *Localized Techniques for Broadcasting in Wireless Sensor Networks*, Algorithmica 49(4): 412-446, 2007.

[3] A. Camill, M. Nati, C. Petrioli, M. Rossi, and M. Zorzi, *IRIS: Integrated data gathering and interest dissemination system for wireless sensor networks*. Ad Hoc Networks 11(2): 654-671, 2013.

[4] J. Crowcroft, M. Segal, and L. Levin, *Improved Structures for Data Collection in Wireless Sensor Networks*, In Proc. of the 33rd Annual IEEE International Conference on Computer Communications (INFOCOM'14), Toronto, Canada, April 27 - May 2, 2014.

[5] J. Leduc, M. Antweiler, and T. Maseng, *Spectrum Issues of NATO Narrowband Waveform: On the spectral efficiency of CPM-Modulation with small modulation indices*, In Proc. of the 2012 Military Communications and Information Systems Conference (MCC'12), Gdansk, Poland, Oct. 8-9, 2012.

[6] C. Brown and P. Vigneron, *Spectrally Efficient CPM Waveforms for Narrowband Tactical Communications in Frequency Hopped Networks*, Military Communications Conference (MILCOM 2006), 23-25 Oct. 2006.

[7] NATO C3B, *Requirements for a Coalition Tactical Radio Waveform*, (AC/322-N(2011)0010-REV1), January 2011.

[8] Joint Tactical Radio System. Retrived from website: http://en.wikipedia.org/wiki/Joint_Tactical_Radio_System in October 28, 2014.

[9] G. Rassatt, *JTRS Family of Programs Spectrum Overview*, December 14, 2011.

[10] P. Jacquet, P. Minet, A. Laouiti, L. Viennot, T. Clausen, and C. Adjih, *Multicast Optimized Link State Routing*, Internet Draft, website: http://tools.ietf.org/html/draft-jacquet-olsr-molsr-00. November 21, 2001.

[11] E. M. Royer, S. Barbara, and C. E. Perkins, *Multicast Ad hoc On-Demand Distance Vector (AODV) Routing*, Internet Draft, website: https://tools.ietf.org/id/draft-ietf-manet-maodv-00.txt. July 15, 2000.

[12] T. Clausen and P. Jacquet, *Optimized Link State Routing Protocol (OLSR)*, IETF RFC 3626, October 2003.

[13] Z. Li, N. Yu, and Z. Deng, *NFA: A new algorithm to select MPRs in OLSR*, In Proc. of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008), Dalian, China, October 12-14, 2008.

[14] Y. Bai, Y. Liu, and D. Yuan, *An Optimized Method for Minimum MPRs Selection Based on Node Density*, In Proc. of the 6th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2010), Chengdu, China, September 23-25, 2010.

[15] ISSP: The Integrated Soldier System Project. Retrived from http://www.canadiandefencereview.com/news.php/news/877 in August 15, 2014.

[16] S. Wood, J. Mathewson, J. Joy, and M.O. Stehr, *ICEMAN: A System for Efficient, Robust and Secure Situational Awareness at the Network Edge*, In Proc. of the 2013 IEEE Military Communications Conference (MILCOM 2013), San Diego, CA, USA, November 18 - 20, 2013.

[17] A. Qayyum, L. Viennot, A. Laouiti, *Multipoint Relaying for Flooding Broadcast Messages in MobileWireless Networks*, In Proc. of the 35th Annual Hawaii International Conference on System Sciences (HICSS'2002), Hawaii, USA, January 7-10, 2002.

[18] E. W. Dijkstra, *A note on two problems in connexion with graphs*. Numerische Mathematik 1: 269271. doi:10.1007/BF01386390. 1959

[19] R. Song and L. Korba, *A Robust Anonymous Ad Hoc On-Demand Routing*, In Proc. of the 2009 IEEE Military Communications Conference (MILCOM 2009), Boston, USA, October 18-21, 2009.

[20] R. Song and P.C. Mason, *ROLSR: A Robust Optimized Link State Routing Protocol for Military Ad-Hoc Networks*, In Proc. of the 2010 IEEE Military Communications Conference (MILCOM 2010), San Jose, CA, USA, October 31 - November 3, 2010.