Building Robust Military Networks Using Advanced Software Tools

D. Vassis[*], A. Tsakrikadakis[*], K. Panagiotopoulos[*], G. Kormentzas[**], D. Vergados[**], F. Lazarakis[*]

[*] National Technical University of Athens
Dept. of Elec. Engineering & Computer Science
GR 157 73, Athens, GREECE

[**]University of the Aegean
Dept. of Information and Communication Systems Engineering,
GR-83200, Karlovassi, GREECE

Abstract: The paper discusses a design framework for building robust military networks. The proposed framework includes advanced software tools and methods for defining optimal alternative routing paths, for examining network's viability in cases of crisis and for performing network simulation. The application of the presented framework towards the design of a military network for the purposes of a national project concludes the paper.

Key-Words: Military Networks, Alternative Routing, Network Viability, Simulation, Link Importance.

1 Introduction

The routing constitutes one of the key parameters of efficient network design [1-2]. The identification of the optimal routes is one of the more challenging objectives of routing. In packet-oriented networks, the routes can differ in terms of packet delay time, which is the sum of the time needed for the packet to be transmitted in the underlying physical links and the time needed for the network nodes to store the packet in their buffers, to process it and retransmit it. In packet-based networks, the optimal route depends on the bandwidth of the underlying physical links, which constitute the route, and the number of included hops in the route.

Concerning the routing operation, two basic routing mechanisms can be identified: *dynamic and static*. In dynamic routing, the choice of the optimal routing path and the definition of the corresponding routing tables in the involved network nodes are done automatically by a standard routing protocol such as RIP, OSPF, BGP, etc. These protocols use basic routing algorithms such as the Bellman - Ford algorithm, the Dijkstra algorithm, etc. The dynamic routing is a scalable, efficient and robust mechanism, which is appropriate for networks of dynamic nature, where the topology changes as nodes are added or removed and links fail and recover. Internet constitutes a typical example of a dynamic network where dynamic routing suit perfectly.

In static routing, the definition of routing tables is done manually. Comparing with dynamic routing, static can be implemented easier (there is no need of setting up a routing algorithm) and with lower costs (there is no need for efficient network nodes with high processing capabilities). Static routing is appropriate for special-purposed networks (e.g., military [3-4], educational, governmental networks, etc) as it achieves secure/ confident information flows and better management and control of the routing paths.

The paper deals with the design of special-purposed networks, such as military. For robust and efficient military network design, special factors have to be considered for the definition of static routing tables. These factors concern criteria related to network's geographical position, various strict requirements for security and confidentiality, special military user's demands/needs/ purposes, etc [5-6]. In addition, for ensuring the continual communication between some crucial military network nodes [7], there must always be the guarantee of some optimal alternative routing paths. Furthermore, in some cases, a military network can be found in a "crisis" where many links fail simultaneously [8]. For taking into account such cases, a link viability analysis seems to be important and essential before building a military network.

Towards the same direction, the usage of a standards-based simulation tool (such as OPNET, COMNET , etc.) can provide an estimation of the network's behavior in real conditions. In order to recapitulate, the main factors for building robust military networks seem to be: i) the optimal alternative routing, ii) the viability analysis, and iii) the network simulation. The paper discusses the abovementioned three basic requirements and presents some software tools, which can facilitate and guarantee the efficient design of a military network.

The rest of the paper is organized as follows: Section 2 deals with the proposed software tools, while Section 3 applies these tools for the design of an example military network. Finally, Section 4 concludes the paper.

2 The Proposed Software Tools

In each individual subsection we discuss an important factor for building robust military networks and we propose the appropriate software tool, which can serve the corresponding factor.

2.1 Optimal alternative routing

In most networks, there is more than one alternative routing option between two nodes. The definition of the optimal one can be a very complex and time-consuming operation, heavily depending on the network's topology. For facilitating the definition of the optimal alternative routing paths, the paper proposes a C-based software tool.

The Bellman – Ford algorithm constitutes the basis of the proposed software tool. This tool evaluates the alternative routing paths and defines the optimal routes that connect each network node with a specific destination node. The tool can use various metrics for evaluating the candidate alternative routing paths in order to define the optimal ones. The using metrics depend on the network's special military purposes. For example, when a network designer has to build a military network in which the security and the confidentiality constitute the major objectives, the performance is not the key issue. In this context, typical security metrics can be the location of the network nodes, as well as the number of intermediate hops and not for example the packet delay, or the packet loss, or the bandwidth, which are performance metrics.

2.2 Viability analysis

As already mentioned, a military network can be found in actual conditions where many links fail simultaneously. As the number of the failed links remains small, it is speculated that there will be the ability of alternative routing. However, as the number of the failed links increases, some nodes will not have any more the ability of alternative routing, leading any traffic generated from them or with destination to them to being dropped. In a military network such a situation can be very crucial as there are nodes more important from the others (i.e., the network nodes situated in the headquarters of a military organization). Thus, it is important for a military network designer to define the crucial links in order to keep some nodes alive in extreme conditions.

A link viability analysis can give to the network designer the required view of the military network. The proposed analysis is based on the value of a new metric called *Network Stability*. This metric refers to the percent number of nodes, which remain alive in a scenario where a number of links are failed. A node is considered to be alive when there is at least one routing path between this node and a destination node. Considering that a destination node can be even a neighboring one, there are very few cases where a node will not be alive.

As it is evident, the network's stability analysis requires multiple scenarios where several links fail. In a wide area network, these scenarios can be thousands or even millions concerning that all link failure combinations have to be examined. However, our analysis concerns military networks in which a large number of physical links fail simultaneously. This fact can reduce the number of examined scenarios. The below described *node merging* method can effectively illustrate this reduction.

The application of the node merging method in a network causes in a virtual way the alternation of the network's topology as it reduces the number of network's links and nodes. The basic idea behind the node merging method is that the military network designer is not interested in single links failures but in a combination of many links. Concerning the part of the network depicted in Figure 1, nodes 1 and 4 are connected with the rest of the network via two links each other. If one of the links 1 ? 2, 2 ? 3 or 3 ? 4 fails, all nodes will still be alive. Ignoring two of the three links and considering one link to connect the nodes 1 and 4, nodes 2 and 3 are merged with one of the nodes 1 or 4 (e.g. 1). In such a case, nodes 1, 2 and 3 are merged creating a hyper-node, which is connected with node 4 via the new link 1 ? 4. If this link fails, both the hyper-node (consisting in nodes 1, 2, 3) and the node 4 are alive. In this way we have achieved the reduction of the link failures scenarios from three to one. However even more interesting is the fact that in the merged network the hyper-node will not be alive with three link failures (all the links connected to the hyper-node), while for the same result in the non-merged network five link failures were needed.

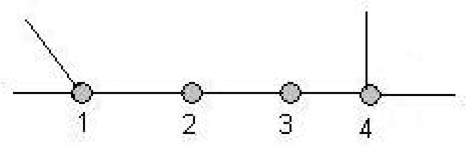

Figure 1. Node merging method

Summarizing node merging method, a node can be merged only if it is serially connected with two other nodes. A hyper-node is the first or last node of a serial node connection. The intermediate nodes are merged in the hyper-node. As concerns the destination nodes (crucial nodes for a military network), they are considered to be alive all the time. Furthermore, the links that connect each other are considered never to fail. Those links can be ignored and the connected destination nodes can be merged. (An application of the node merging method will be discussed in following section).

Returning to network's stability analysis, the paper develops a C-based software tool, which enables the calculation of network stability value for various link failures scenarios. The Bellman – Ford algorithm constitutes the basis of the proposed tool. This tool creates scenarios where several links fail and for each scenario the tool counts the unreachable (not alive) nodes and calculates the network stability value for this combination of links failure. The tool's produced results can be used for the examination of the network's viability.

The link importance evaluation constitutes one of the major aspects of a network's viability analysis. It is obvious that each link has different importance as concerns the total robustness and viability of a network. The point is how important is a specific link for the network's viability. It would be very helpful if a *relative importance* between the links could be defined. Based on the defined concept of network stability, the more often a link is presented in a link combination failure scenario, the more important can be this link for the overall network's viability. Furthermore, for a scenario where a specific link fails, the less the value of the network stability is, the more important for the network's viability is this link. Expressing all the above in a mathematic formula, we define for each network link the R*elative Importance* metric as below:

$$M = \frac{\sum_{i=1}^{K} S_i}{\sum_{i=1}^{N} S_i} \qquad \text{Eq. (1)}$$

In the above type, M expresses the link relative importance, K refers to the total number of link failures scenarios where the examined link is presented, N is the number of all different failure scenarios and S_i is the network stability for the i-th scenario. Using the results of the proposed software tool as input in the above type, one can easily estimate for the links of a military network their relative importance.

2.3 Network simulation

The third important factor for building robust military networks refers to network simulation. The simulation can be performed in an advanced platform such as OPNET, COMNET, etc. Several important results such as the links utilization, throughput, packet losses and delays can be obtained. A simulation platform enables the military network designer to apply several extreme scenarios (a large number of network links fail simultaneously due for example an enemy's sabotage) in order to examine the network's viability in actual difficult conditions. Note that the simulation results can be combined with the results of the proposed (in Subsection 2.2) software tool in order to give to the designer a general view of the network's robustness and viability.

3 Application of the Proposed Tools

This section discusses the application of the tools presented in Section 2 for the design of a wide area military network (see Figure 2). The examined military network consists of wireless and optical links. The network's destination nodes (always alive) are considered as main. In addition, the optical links connected the main nodes are also considered stable and always alive. The emphasis is given on the wireless links, which can fail. The solid lines in Figure 2 depict the static routing paths in normal conditions.

Passing now to the definition of the optimal alternative routing (one of the three basic military design factors according to Section 2), we use the software tool presented in Subsection 2.1. The tool's result concerning the optimal alternative links is depicted in Figure 2 with dashed lines.

Note that nodes between alternative links do not generate traffic and are used only for alternative link connection when the distance between two nodes does not allow a single wireless link to be used. In many nodes there are multiple alternative routes that can be followed. The selected route depends on the link (or combination of links), which fails in each case. For example the most efficient alternative route from node 16 to node 35, if link 6? 16 fails, is 6? 28? 27? 22? 21? 20? 35. The optimal route from node 3 to node 38, if link 2 ? 3 fails, is 3? 25? 24? 23? 1? 38.

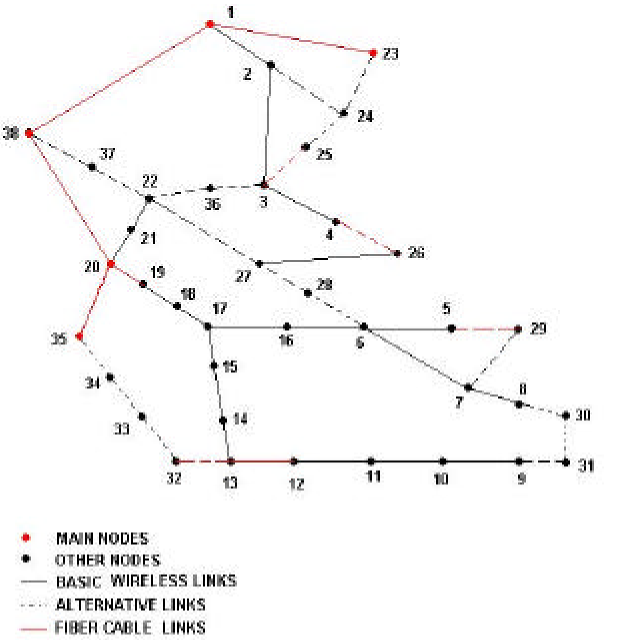

Figure 2. The examined military network

After the definition of the alternative links, the next step of the proposed military design framework refers to links viability analysis in order to examine the network's functionality under extreme usually unexpected conditions. In order to facilitate the use of the software tool presented in Subsection 2.2, we simplify the network topology depicted in Figure 2 by applying the discussed node merging method. The outcome of this method is depicted in Figure 3.

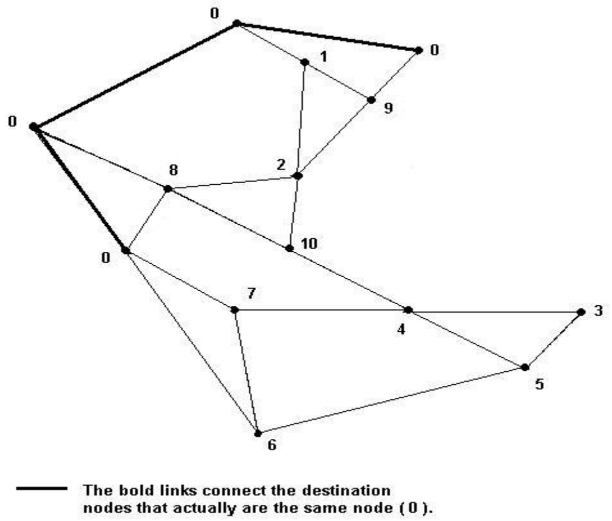
0
1
0
9
0
8
2
10
0
7
4
3
5
6
The bold links connect the destination nodes that actually are the same node (0).

Figure 3. The merged network

Table 1 presents the hyper-nodes of the merged network and the nodes of the network that were merged to hyper-nodes. As we can see, the actual network is consisted of 37 nodes and 45 links, while the merged network is consisted from 10 nodes and 18 links.

HYPER-NODE	MERGED NODES
0	1, 19, 20, 21, 23, 33, 34, 35,37
1	2
2	3, 4, 26
3	5, 29
4	6, 16
5	7
5	8, 9, 10, 11, 12, 13, 30, 31, 32
7	14, 15, 17, 18
8	22, 36
9	24, 25
10	27, 28

Table 1. Merged nodes and hyper-nodes

The links relative importance is depicted in graph in Figure 4.

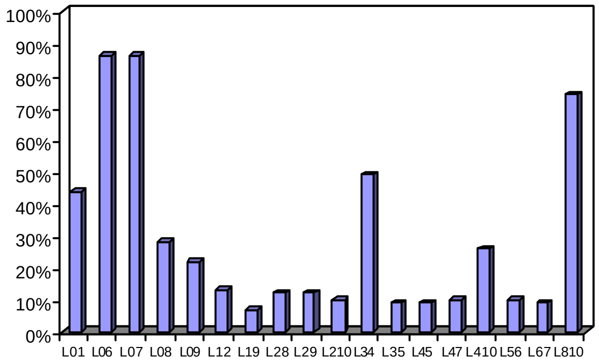

Figure 4. The Relative Importance graph

Simulation of the network constitutes the last step of the proposed military design framework. The designer is interested in analyzing the network's behavior under both normal and extreme conditions. For the examined military network, the simulation was performed in the OPNET advanced simulation platform. The applications running on the network were voice (64 Kbps and 19 Kbps quality, G.711 encoded speech), CBR video (10 frames/sec, 120 bytes frame size), database query transactions (the transaction size is defined by exponential – 16KBytes mean outcome distribution) and email messages (the email size is defined by exponential – 1024KBytes mean outcome distribution).

We ran three scenarios of simulation. In the first scenario we simulated the network making use of the basic links in order to study its behavior without the use of alternative links. In the second scenario we simulated the basic network, with failure of one link. In the third scenario we simulated the network with the basic and alternative links in use and failure of a large number of links, in order to examine links' behavior in extreme situations. In Figures 5 and 6 there are graphs of the utilization of representative links.

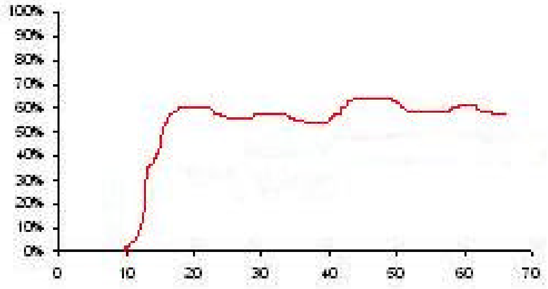

Figure 5. Utilization of link L1617

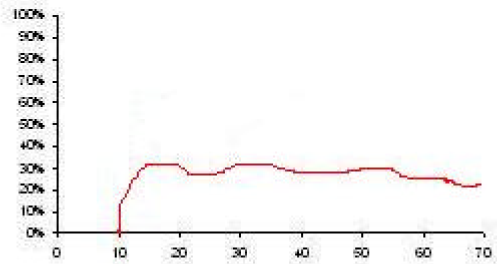

Figure 6. Utilization of link L3334

4 Conclusion

The definition of optimal alternative routing paths, the examination of network's viability and the performance of network simulation constitute three basic factors for the efficient deployment of an advanced military network. All these three factors have to be considered in the design time of a military network. The paper discusses software tools and methods, which can effectively serve the abovementioned design factors. Furthermore, it applies the proposed tools and methods for the design of a military network in the context of a national project.

References:

[1] K. Terplan, *Communications Network Management*, Prentice Hall, 1992.

[2] Vergados D. et al., "Technologies Supporting Programmability of Future Military Networks: A Review and a Critical View", *In SCCC Proc.*, 2001.

[3] P. Sass et al., "Communications for the digital Battlefield of the 21st Century", *IEEE Communications Magazine*, Oct 1995.

[4] Vergados D.D. et al., "New Generation Features for Tactical Wireless Communication Networks", *In Vehic. Tec. Conf. Proc.*, 2000

[5] EriTac – *A commitment to tactical communications*, RL402A, http://www.ericsson.com, Ericsson Corp.

[6] CECOM, *Battlefield Information Transmission System - Far - Term Strategy*, Ver. 1, Oct 1995.

[7] CTM 350S, *Radio Relay Equipment for Strategical and Semi-Mobile Operation*, see electronic information in http://www.siemens.com.

[8] Crisis Management System, RITA 2000 - *New Generation Tactical Communication Network*, http://www.tcc.thomson-csf.com, Thomson-CSF Corp.