

System Engineering Approach in Tactical Wireless RF Network Analysis

Philip Chan², Hong Man¹, David Nowicki¹ and Mo Mansouri¹

¹*Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ,*

²*University of Maryland University College (UMUC), MD,
USA*

1. Introduction

Engineers dealing with different scaled and interconnected engineering systems such as tactical wireless RF communication systems have growing needs for analyzing complex adaptive systems. We propose a systemic engineering methodology based on systematic resolution of complex issues in engineering design. Issues arise which affect the success of each process. There are a number of potential solutions for these issues, which are subject to discussion based on the result assembled from a variety of sources with a range of measures. There are needs to assemble and balance the results in a success measure showing how well each solution meets the system's objectives. The uncertain arguments used by the participants and other test results are combined using a set of mathematical theory for analysis. This process-based construction helps not only in capturing the way of thinking behind design decisions, but also enables the decision-makers to assess the support for each solution. The complexity in this situation arises from the many interacting and conflicting requirements of an increasing range of possible parameters. There may not be a single 'right' solution, only a satisfactory set of resolution, which this system helps to facilitate. Applying systems engineering approaches will definitely help in measuring and analyzing tactical RF wireless networks, smart and innovative performance matrixes through tactical modeling and simulation scenarios may also be developed and enhanced. Systematic utilize of systems engineering approaches with RF electronic warfare modeling and simulation scenarios can support future research in vulnerability analysis of RF communication networks. RF electronic tactical models are used to provide a practical yet simple process for assessing and investigate the vulnerability of RF systems. The focus is also on tactical wireless network within a system of systems (SoS) context research area and to provide a comprehensive network assessment methodology. Researchers have proposed a variety of methods to build network trees with chains of exploits, and then perform normal post-graph vulnerability analysis. This chapter presents an approach to use mathematical Bayesian network to model, calculate and analyze all potential vulnerability paths in wireless RF networks.

2. Main methodology

Tactical wireless network vulnerabilities continually being reported and critically studied with many U.S. government organizations. The need for a comprehensive framework of

network vulnerability assessment using systems engineering approach [24] [26] [27] [28] has been an increasing challenge to many research analysts. Researchers have proposed a more systematic way to manage wireless network nodes and trees with possible chains of events, and then perform normal post-graph vulnerability assessments with system of systems methodology. The most recent system engineering approaches are building attack trees by trying to number all potential attack paths with vulnerabilities identification, node probabilities calculations, inference analysis, and weights assignments by system experts. These are expert driven vulnerabilities analysis. Assessment and identification are one of the main key issues in making sure the property security of a given deployed tactical RF communication network. The vulnerability assessment process involves many uncertain factors reside within both the networks and the network nodes. Threat assessment or injecting threats is one of the major factors of evaluating a situation for its suitability to support decision-making and the indication of the security of a given tactical RF communication network system. One approach is using experienced decision makers database. This type of expert driven database recorded most of their decisions on vulnerability identification. The decision-makers use past experience for their decisions. The decision will be based upon previously good solutions that have worked in similar real life scenarios. The approach is to extract the most significant characteristics from the lay-down situation. Any similar situations and actions that have worked well in past cases will be considered in the assessment due to the present or the lack of certain essential characteristics. The assessment and identification is to create relevant relations between objects in the tactical RF network environment. Tactical communication RF wireless networks are best illustrated by Mr. David L. Adamy [11] in his book. Bayesian network (BN) and the related methods [17] is an effective tool for modeling uncertainty situation and knowledge. This paper discusses Bayesian's Theory [17], Bayesian networks and their ability to function in a given tactical RF communication network [11] for vulnerabilities analysis and identification. This short chapter presents an approach to use Bayesian network to model all potential vulnerabilities or attack paths in tactical RF wireless network. We will call such graph as "Bayesian network vulnerabilities graph" for a given tactical RF wireless network. It provides a more compact representation of attack paths than conventional methods. Bayesian inference methods can be used for probabilistic analysis. It is necessary to use algorithms for updating and computing optimal subsets of attack paths relative to current knowledge about attackers. Tactical RF wireless models were tested on a small example JCSS [12] network. Simulated test results demonstrate the effectiveness of approach.

2.1 Why systems engineering is used here

Systems engineering [7] [8] [27] [28] is applied here to assist the rapid design and development of complex systems such as tactical wireless communication systems. Systems engineering [29] uses engineering sciences techniques with operations research. Operations research also tackles with designing complex systems. Our goal is to utilize concurrent engineering principles in systems engineering analysis that covers our design goals and testing requirements in developing the RF communication system. The systems approach to solving complex problems are critical since integrating complex analysis and building of RF communication models requires synthesis of different methods. Systems approach is widely used and successful in fields of engineering, for example systems engineering. It is most

effective in treating complex phenomena in tactical wireless RF communication networks. All this requires the use of modular views that clearly illustrate the component features of the whole system. The views may be put into different parts with proper interfaces. Extended knowledge may be gained about the parts in order to further understand the whole nature of a given tactical RF communication system. The system and its details in many levels may then be decomposed into several subsystems and into sub-subsystems, and so on, to the last details. In the same time, we can change focus to view different levels so that users are not overwhelmed by complexity. From time to time abstracts level information may be hid to gain focus on a certain task for detailed analysis. We may just simplify the system by treating some of its parts as black boxes except their interfaces. Hiding information for certain RF tactical analysis is not discarding it. The same black box can be opened at later time for other uses. Systems engineering can make a complex system more tractable and some of the parts can be studied or designed with minimal interference from other parts. All these protective measures can control defective designs and improves system level performance. The systems approach is effective not only for understanding or designing tactical RF wireless communication systems but also for abstract construction in mathematics and theories. Instead of an actual RF communication physical module, a RF wireless network "subsystem" can be a concept within a conceptual scheme and its "interfaces" can be relations to other in the scheme. Analyses and concepts are sometimes needed to approximate in the beginning. We can then refine approximations step by step towards a better answer with our method of analysis. Systems approach is not merely system-level approach but rather delving into lower-level subsystems. The system-level is powerful and appropriate in some cases, but it also misses out on most structures plus dynamics of the system and it is not employed in our systems approach, modularity study here. Systems approach is an integral part of systems engineering. Our analysis here may also call reduction, and "lessening" to yet finer information that also mean the importance of detailed analysis.

3. System of systems in tactical wireless network

In general, system of systems [9] [10] is a compilation of task-oriented or dedicated systems that bundle their resources and capabilities together to obtain a newer, more complex system that offers more functionality and performance than simply the summation of basic systems. Currently, system of systems is a critical research discipline that supplements engineering processes, quantitative analysis, tools, and design methods. The methodology to define, abstract, model, and analyze system of systems problems is typically referred to as system of systems engineering. We are going to define features for a system of systems that are unique for our study of tactical wireless communication system. The goal will be linking systems into joint system of systems allows for the interoperability and integration of Command, Control, Computers, Communications, and Information (C4I) and Intelligence, Surveillance and Reconnaissance (ISR) Systems as description in the field of information management control in modern armed forces. The system of systems integration is a method to pursue better development, integration, interoperability, and optimization of systems to enhance performance in future combat zone scenarios that related to area of information intensive integration. As one can predict that modern systems that comprise system of systems problems are not merely massive, rather they have some common characteristics: operational independence of the individual systems and managerial independence of the

systems. System of systems problems are a collection of multiple domain networks of heterogeneous systems that are likely to exhibit operational and managerial independence, geographical distribution, and emergent and evolutionary behaviors that would not be apparent if the systems and their interactions are modeled separately. Taken together, all these background requirements suggest that a complete system of systems engineering framework is considered necessary to improve decision support for system of systems problems. In our case, an effective system of systems engineering framework for tactical RF communication network models are desired to help decision makers to determine whether related infrastructure, policy, and/or technology considerations are good, efficient, or deficient over time. The urgent need to solve system of systems problems is critical not only because of the growing complexity of today's technology challenges, but also because such problems require large resource commitments and investments with multi-years cost. The bird-eyes view using system-of-systems approach will allow the individual system constituting a system of systems that can be different and operate independently. The interactions expose certain important emergent properties. These emergent patterns have an evolving nature that the RF communication system stakeholders must recognize, analyze, and understand. The system of systems way of thinking promotes a new way of approach for solving grand challenges where the interactions of current technology, organization policy, and resources are the primary drivers. System of systems study is also integrated the study of designing, complexity and systems engineering with additional challenge of design. Systems of systems typically exhibit the behaviors of complex systems. However, not all complex problems fall into the area of systems of systems. System of systems by nature, are several combinations of qualities, not all of which are exhibited in the operation of heterogeneity networks of systems. Current research into effective approaches to system of systems problems includes: proper frame of reference, design architecture. Our study of RF communication network modeling, simulation, and analysis techniques will include network theory, agent-based modeling, probabilistic (Bayesian) robust design (including uncertainty modeling/management), software simulation and programming with multi-objective optimization. We have also studied and developed various numerical and visual tools for capturing the interaction of RF communication system requirements, concepts, and technologies. Systems of systems are still being employed predominantly in the defense sector and space exploration. System of Systems engineering methodology is heavily used in U.S. Department of Defense applications, but is increasingly being applied to many non-defense related problems such as commercial PDA data networks, global communication networks, space exploration and many other System of Systems application domains. System-of-Systems engineering and systems engineering are related but with slightly different fields of study. Systems engineering addresses the development and operations of one particular product like the RF communication networks. System-of-Systems engineering addresses the development and operations of evolving programs. Traditional systems engineering seeks to optimize an individual system (i.e., the target product), while System-of-Systems engineering seeks to optimize network of various interacting legacy and new systems brought together to satisfy multiple objectives of the program. It enables the decision-makers to understand the implications of various choices on technical performance, costs, extensibility and flexibility over time and the effective of methodology. It may prepare decision-makers to design informed architectural solutions for System-of-Systems context type problems. The objective in our research is to focus on tactical wireless network within a system of systems (SoS) context research area. The ultimate goal is to provide a

comprehensive network assessment methodology and possible framework with systems engineering approach.

4. Approach with system engineering

Systems engineering [7] [8] [9] is employed here to look into wireless network vulnerabilities with simulation and modeling work-processes. Sets of useful tools are developed to handle the vulnerability analysis part of the RF wireless network. In the research, we have summarized a variety of methods to build network trees with chains of possible exploits, and then perform normal post-graph vulnerability assessment and analysis. Recent approaches suggest building more advanced attack trees by trying to number all potential attack paths with vulnerabilities identification, node probabilities calculations, inference analysis, weights assignments by system experts. Vulnerabilities analysis, assessment and identification are one of the key issues in making sure the security of a given tactical RF communication network. The vulnerability assessment process involves many uncertain factors. Threat assessment is one of the major factors of evaluating a situation for its suitability to support decision-making and the indication of the security of a given tactical RF communication network system. Systems engineering methodology in the research plays a critical role to help develop a distinctive set of concept and methodology for the vulnerability assessment of tactical RF communication networks. Systems engineering approaches have been developed to meet the challenges of engineering functional physical systems of tactical RF communication networks with complexity. The system engineering process employs here is a brand of holistic concept of system engineering processes. With this holistic view in mind, the systems engineering focuses are on analyzing and understanding the potential U.S. government customer needs. Re-useable RF connectivity models with requirements and functionality are implemented early in the development cycle of these RF communication network models. We then proceed with design synthesis and system validation while considering the complete problem, the system lifecycle. Based upon the concept by Oliver et al. [23], systems engineering technical process are adopted during the course of the research. Within Oliver's model [23], the technical process includes assessing available information, defining effectiveness measures, to create a behavior Bayesian vulnerabilities model, create a structure model, perform trade-off analysis, and create sequential build & test plan. At the same time, a RF communication system can become more complex due to an increase in network size as well as with an increase in the amount of vulnerabilities data, engineering variables, or the number of fields that are involved in the analysis. The developments of smarter matrices with better algorithms are the primary goals of the research. With disciplined systems engineering, it enables the use of tools and methods to better comprehend and manage complexity in wireless RF network systems for in-depth analysis. These tools are developed using modeling and simulation methodologies, optimization calculations and vulnerabilities analysis. Taking an interdisciplinary engineering systems approach to perform vulnerabilities analysis using Bayesian graph with weights calculation is inherently complex. The behavior of and interaction among RF wireless network system components can be well defined in some cases. Defining and characterizing such RF communication systems and subsystems and the interactions among them that supports vulnerabilities analysis is one of the goals of the research.

5. Insights behind research

Decision matrix is used for vulnerabilities analysis in the research. Decision matrix is an arrangement of related qualitative or quantitative values in terms of rows and columns. It allows our research to graphically identify, analyze, and rate the strength of relationships between sets of information in vulnerabilities. Elements of a decision matrix represent decisions based upon calculations and Bayesian network (BN) on certain vulnerabilities decision criteria. The matrix development is especially useful and critical for looking at large sample numbers of decision factors and assessing each factor's relative importance. Decision matrix employed in the research is used to describe a multi-criteria decision analysis (MCDA) for the tactical RF wireless network. When given a MCDA problem, where there are M alternative options and each need to be assessed on N criteria, can be described by the decision matrix which has M rows and N columns, or $M \times N$ elements. Each element, such as X_{ij} , is either a single numerical value or a single grade, representing the performance of alternative i on criterion j . For example, if alternative i is "Wireless Node i ", criterion j is "Background Noise" assessed by five grades {Excellent, Good, Average, Below Average, Poor}, and "Wireless Node i " is assessed to be "Good" on "Background Noise", then $X_{ij} = \text{"Good"}$. The matrix table 1 is shown below:

	Criterion 1	Criterion 2	...	Criterion N
Alternative 1	x_{11}	x_{12}	...	x_{1N}
Alternative 2	x_{21}	x_{22}	...	x_{2N}
...	$X_{ij} = \text{Good}$...
Alternative M	x_{M1}	x_{M2}	...	x_{MN}

Table 1.

5.1 Multiple criteria decision

Using a modified belief decision matrix, the research is now more refined and the matrix can describe a multiple criteria decision analysis (MCDA) problem in the Evidential Reasoning Approach. In decision theory, the evidential reasoning approach is a generic evidence-based multi-criteria decision analysis (MCDA) approach for dealing with problems having both quantitative and qualitative criteria under various uncertainties. This matrix may be used to support various decision analysis, assessment and evaluation activities such as wireless RF networks environmental impact assessment and wireless RF networks internal nodes (transceiver) assessment based on a range of quality models that are developed. For a given MCDA, there are M alternative options and each need to be assessed on N criteria, then the belief decision matrix for the problem has M rows and N columns or $M \times N$ elements. Instead of being a single numerical value or a single grade as in a decision matrix, each element in a belief decision matrix is a belief structure. For example, suppose Alternative i is "Wireless Node i ", Criterion j is "Background Noise" assessed by five grades {Excellent, Good, Average, Below Average, Poor}, and "Wireless Node i " is assessed to be "Excellent" on "Message Completion Rate" with a high degree of belief (i.g. 0.6) due to its low Transmission Delay, low Propagation Delay, good Signal-to-Noise Ratio and low Bit Error

Rate. At the same time, the quality is also assessed to be only "Good" with a lower degree of confidence (i.g. 0.4 or less) because its fidelity and "Message Completion Rate (MCR) can still be improved. If this is the case, then we have $X_{ij} = \{ (Excellent, 0.6), (Good, 0.4) \}$, or $X_{ij} = \{ (Excellent, 0.6), (Good, 0.4), (Average, 0), (Below Average, 0), (Poor, 0) \}$. A conventional decision matrix is a special case of belief decision matrix when only one belief degree in a belief structure is 1 and the others are 0. The modified matrix table 2 is shown below:

	Criterion 1	Criterion 2	...	Criterion N
Alternative 1	x_{11}	x_{12}	...	x_{1N}
Alternative 2	x_{21}	x_{22}	...	x_{2N}
...	$X_{ij} = \{ (Excellent, 0.6), (Good, 0.4) \}$...
Alternative M	x_{M1}	x_{M2}	...	x_{MN}

Table 2.

5.2 Probability distributions

The research may help to develop a more systematic and automated approach for building "Bayesian network vulnerabilities graph" with weights assignment for vulnerability study in tactical wireless RF networks [11]. Bayesian network [17] is designed in vulnerabilities graph and models all potential attack steps in a given network. As describe by T. Leonard and J. Hsu [17], using Bayesian's rule as a special case involving continuous prior and posterior probability distributions and discrete probability distributions of data, but in its simplest setting involving only discrete distributions, the theorem relates the conditional and marginal probabilities of events A and B, where B has a certain (non-zero) probability as in (1):

$$P(A | B) = (P(B | A)P(A))/P(B) \quad (1)$$

Each term in the theorem has a conventional name: $P(A)$ is the prior probability or marginal probability of A. It is "prior" in the sense that it does not take into account any information about B. $P(A | B)$ is the conditional probability of A, given B. It is also called the posterior probability because it is derived from or depends upon the specified value of B. $P(B | A)$ is the conditional probability of B given A. $P(B)$ is the prior or marginal probability of B, and acts as a normalizing constant. The theorem in this form gives a mathematical representation of how the conditional probability of even A given even B is related to the converse conditional probability of even B when given even A. In our research, each wireless network node represents a single security and vulnerability point and contains property violation mode; each link edge corresponds to an exploitation of one or more possible vulnerabilities and each network path represents a series of exploits that can signify a potential vulnerability for attack within the RF wireless network. The communication model takes on characteristics of a tactical wireless RF network, and we consider an integrated posterior probability of Bayesian networks (BN) [17] with well-defined security metric represents a more comprehensive quantitative vulnerability assessment of a given

tactical RF networks which contain different communication stages. Posterior probability is a revised probability that takes into account new available information. For example, let there be two stages within a given wireless transceiver. Wireless stage A having vulnerability or 0.35 accuracy due to noise factor and 0.85 accuracy due to jamming factor and wireless stage B having vulnerability or 0.75 accuracy due to noise factor and 0.45 accuracy due to jamming. Now if wireless stage is selected at random, the probability that wireless stage A is chosen is 0.5 (50% chance, one out of two stage). This is the a priori probability for the vulnerability of wireless communication stage. If we are given an additional piece of information that a wireless stage was chosen at random from the wireless network, and that the factor is noise, what is the probability that the chosen wireless stage is A? Posterior probability takes into account this additional information and revises the probability downward from 0.5 to 0.35 according to Bayesian's theorem. Also, the noise factor effect is more probable from stage B (0.75) than stage A (0.35). When the factor is jamming instead, the probability that the chosen wireless stage is A will be revised upward from 0.5 to 0.85 instead. Then, the vulnerability related jamming factor now is definitely less probable from stage B (0.45) than stage A (0.85). With conditional independence relationship encoded in a Bayesian network (BN) can be stated as follows: a wireless node is independent of its ancestors given its parents, where the ancestor/parent relationship is with respect to some fixed topological ordering of the wireless nodes. Using figure 1 below to demonstrate the outcomes, by the chain rule of probability with stages C, S, R & W, the joint probability of all the nodes in the vulnerabilities graph is now become: $P(C, S, R, W) = P(C) * P(S|C) * P(R|C,S) * P(W|C,S,R)$. By using conditional independence relationships, we can rewrite this as: $P(C, S, R, W) = P(C) * P(S|C) * P(R|C) * P(W|S,R)$ where we are allowed to simplify the third term because R is independent of S given its parent C, and the last term because W is independent of C given its parents S and R. We can see that the conditional independence relationships allow us to represent the joint more compactly. Here the savings are minimal, but in general, if we had n binary nodes, the full joint would require $O(2^n N)$ space to represent, but the factored form would require $O(n \sum k)$ space to represent, where k is the maximum fan-in of a node with fewer overall parameters.

5.3 Wireless communication models

In the model, we concern about the vulnerability of the wireless network caused by the failure of various communication stages in the wireless RF communication network. Figure 2 clearly presents the logical communication block diagram of our RF model. Each stage in a RF network is profiled with network and system configurations with exhibited vulnerabilities. They are identified through the breaking down of a given transceiver into transmitter and receiver with different stages. The purpose of our modeling and simulation goals is to make use the DISA JCSS Transceiver Pipeline stages [12]. All vulnerabilities data may be collected and the following information may be collected at run-time: (1) Effect of the transmission on nodes in the vicinity. (2) Set of nodes will attempt to receive the packet. (3) Determine a node attempting to receive a packet successfully. (4) Time it take for a packet to be transferred to the receiver. To start with the transmitter, we break down the transceiver into different radio pipeline stages. On the transmitter side, the transmitter has a

Bit Error Rate, Error Allocation and Error Correction. In JCSS [12] and OPNET Modeler, there are altogether 14 Pipeline Stages (PS) that have implemented vulnerabilities graph for Bayesian networks (BN) [17] analysis. These are customized collections sequence of 'C' or 'C++' procedures (code & routines) with external Java subroutines and portable applications written for research purposes. In figure 2, each 14 different stages that comprised in a transceiver network perform a different calculation. For example in (1) Line-of-sight, (2) Signal strength & (3) Bit errors rates, Pipeline Stages (PS) code & routines are written in C, C++ and with external subroutine interfaces written in Java. Each procedure has a defined interface (prototype) with arguments typically a packet. Unlike most available vulnerability bulletins on public domains, we classify tactical wireless networks with vulnerabilities inside the 14 different stages of a given tactical wireless RF communication transceiver. So the vulnerabilities graph for a given tactical transceiver may be classified as vulnerabilities in Radio Transmitter are: (Vt1) Receiver Group, (Vt2) Transmission Delay, (Vt3) Link Closure, (Vt4) Channel Match, (Vt5) Transmitter Antenna Gain and (Vt6) Propagation Delay. On the hand the vulnerabilities for the Radio Receiver are: (Vr1) Rx Antenna Gain, (Vr2) Received Power, (Vr3) Interference Noise, (Vr4) Background Noise, (Vr5) Signal-to-Noise Ratio, (Vr6) Bit Error Rate, (Vr7) Error Allocation and (Vr8) Error Correction.

Vulnerabilities	Vulnerabilities
precond:	precond:
Radio Transmitter:	Radio Receiver:
(Vt1) Receiver Group	(Vr1) Rx Antenna Gain
(Vt2) Transmission Delay	(Vr2) Received Power
(Vt3) Link Closure	(Vr3) Interference Noise
(Vt4) Channel Match	(Vr4) Background Noise
(Vt5) Transmitter Antenna Gain	(Vr5) Signal-to-Noise Ratio
(Vt6) Propagation Delay	(Vr6) Bit Error Rate
postcond:	postcond:
(Vt1) Receiver Group = 0.99	(Vr1) Rx Antenna Gain = 0.75
(Vt2) Transmission Delay = 0.55	(Vr2) Received Power = 0.65
(Vt3) Link Closure = 0.65	(Vr3) Interference Noise = 0.85
(Vt4) Channel Match = 0.85	(Vr4) Background Noise = 0.10
(Vt5) Transmitter Antenna Gain = 0.15	(Vr5) Signal-to-Noise Ratio = 0.90
(Vt6) Propagation Delay = 0.25	(Vr6) Bit Error Rate = 0.25
	(Vr7) Error Allocation = 0.35
	(Vr8) Error Correction = 0.40

Fig. 3. An example of vulnerabilities template for JCSS (transmitter / receiver pair) and related simulations.

Using the existing JCSS tactical RF hosts configuration and profile editors with wireless networking analysis tools [13] [14], we can construct generic, vulnerabilities graph and templates to describe possible exploitations conditions with certain vulnerabilities in a given transceiver and then on to a larger scale, a given tactical communication network's overall situation. Each template contains some pre-conditions and post-conditions of an atomic event related to the communication stage along with some security metric(s) information. A successful JCSS simulation will lead to better understanding for a more secure tactical RF communication model. Since we build vulnerability graphs using Bayesian networks (BN), we also assign probability of success after a failure in a pipeline stage's link-edge weight.

5.4 Algorithm within vulnerabilities graph

Specifying valid probability of communication in different stages requires domain expert knowledge. Most existing vulnerabilities scanning tools report those vulnerabilities with a standard set of categorical security measurements, such as severity level and vulnerability consequences. Therefore, considering the nature of a wireless network, one can define a more than one dimension security or vulnerabilities matrix using these categorical information and quantify levels of each category into numerical values for computation and comparison basis. Our approach is to make each matrix entry value related to each stage in a given transceiver. The result can then be computed and derived by a mathematical function that receives contributions from various dimensions like a normal linear additive function $f(x + y) = f(x) + f(y)$ or multiplicative function $f(ab) = f(a) f(b)$. Then, it can be converted to a value within range [0,1] by applying a special scalar function. A function of one or more variables whose range is one-dimensional, this scalar function can be applied to the matrix. Such value may be represented the probability of a given vulnerability with respect to the transceiver. For example, One can define a two dimension $m \times n$ security matrix $W = (w_{ij})$, with one dimension w_i to denote severity levels and another dimension w_j to denote ranges of exploits. A 3-scale severity level may be specified as {high = 0.95, medium = 0.65, low = 0.35}, and 2-scale exploit ranges may be specified as {remote = 0.55, local = 0.95}. If applying a multiplicative function to the matrix, then each entry value is given by $w_{ij} = w_i \times w_j$. Our research constructs Bayesian vulnerabilities graphs with our graph generation and mapping routine by matching a list of stages in a given transceiver on a wireless network with profile information against a library of computed vulnerabilities specified node characteristic templates. For any vulnerability, if all pre-conditions are met, values of post-condition attributes are updated with an edge that is assigned with weight. It is then added to the vulnerability graph. The most common task we wish to solve using Bayesian networks (BN) is probabilistic inference. For example, consider the network G with a current vulnerability status W , and suppose we observe the fact that G with a status of W . There are two possible causes for this: either it is due to factor R , or the due to factor S is on. Which is more likely? We can use Bayesian's rule to compute the posterior probability of each explanation (where 0=false and 1=true).

$$\Pr(S = 1 | W = 1) = \frac{\Pr(S = 1, W = 1)}{\Pr(W = 1)} = \frac{\sum_{c,r} \Pr(C = c, S = 1, R = r, W = 1)}{\Pr(W = 1)} = 0.2781 / 0.6471 = 0.430$$

$$\Pr(R = 1 | W = 1) = \frac{\Pr(R = 1, W = 1)}{\Pr(W = 1)} = \frac{\sum_{c,s} \Pr(C = c, S = s, R = 1, W = 1)}{\Pr(W = 1)} = 0.4581 / 0.6471 = 0.708$$

where

$$\Pr(W = 1) = \sum_{c,r,s} \Pr(C = c, S = s, R = r, W = 1) = 0.6471$$

$\Pr(W = 1)$ is a normalizing constant, equal to the probability (likelihood) of the data. So we see that it is more likely that the network G will have a status of W, because of the weight in factor R is more than factor S: i.e. the likelihood ratio is $0.7079/0.4298 = 1.647$. With variable elimination techniques illustrated below and using vulnerabilities graph in figure 4, we use Bayesian networks (BN) with Bucket Elimination Algorithm implementation in the models with belief updating in our scenarios, to the most probable explanation. We need to provide vulnerability values in each communication stage within each transceiver plus the network scores on the entire tactical network. Finding a maximum probability assignment to each and the rest of variables is a challenge. We may really need to maximizing a posteriori hypothesis with given evidence values, finding an assignment to a subset of hypothesis variables that maximize their probability. On the other hand we may need to maximize the expected utility of the problem with given evidence and utility function, finding a subset of decision variables that maximize the expected utility. Any other consideration is Bucket Elimination Algorithm. It may be used as a framework for various probabilistic inferences on Bayesian Networks (BN) in the experiment. Finally, a RF Vulnerability Scoring System (RF-VSS) analysis is in development. It is based upon the Common Vulnerability Scoring System [22] and associates with additional features of Bayesian networks [17] (also known as belief network) that in turn yields a more refined belief decision matrix and the matrix can then describes a multiple criteria decision analysis (MCDA) with evidential reasoning approach for vulnerabilities analysis of a given tactical wireless RF network.

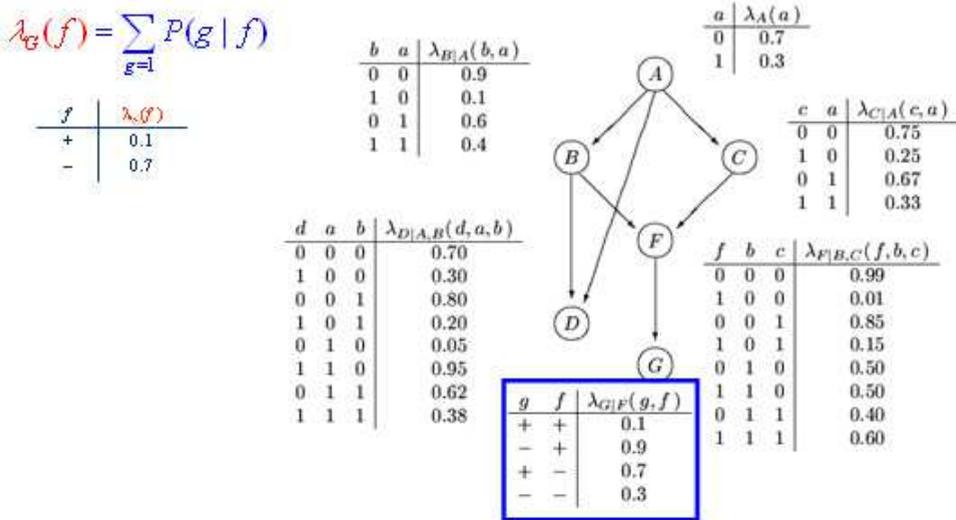


Fig. 4. Use of Bucket Elimination Algorithm within vulnerabilities graph

6. Result generated from sample experiments

For simplicity in terms of network radio analysis, we provide here a rather simple two (2) nodes wireless RF network scenarios that are communicating with each other via UDP protocol. A more complex one is illustrated in figure 5b. Using some of the available wireless networking analysis toolkits [13] [14] as in figure 5a, a set of JCSS EPLRS Scenarios with a link being jammed. Packets were being captured and exported into Microsoft EXCEL spreadsheet. Jamming occurs between 2 wireless links for this network: EPLRS_6004 and EPLRS_6013. EPLRS_6013 transceiver model was changed to a special EPLRS EW network vulnerability model as in figure 5c. The receiver link was intentionally jammed (by increase the noise level to an extremely high value, i.e. the vulnerabilities within one of the wireless stage are increased by many fold) so that no more simulated packet will be “successful” in getting through from EPLRS_6004 to EPLRS_6013 and the results are listed and illustrated in figure 5d with some sample data.

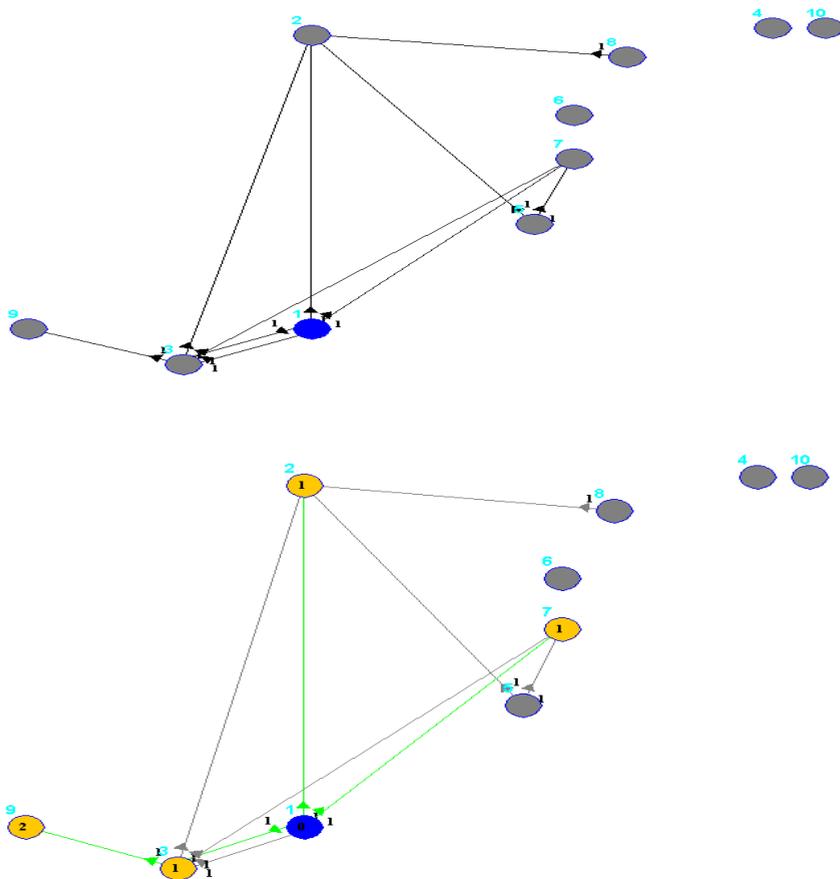


Fig. 5a. Before and after scenarios using wireless networking analysis toolkits in Java

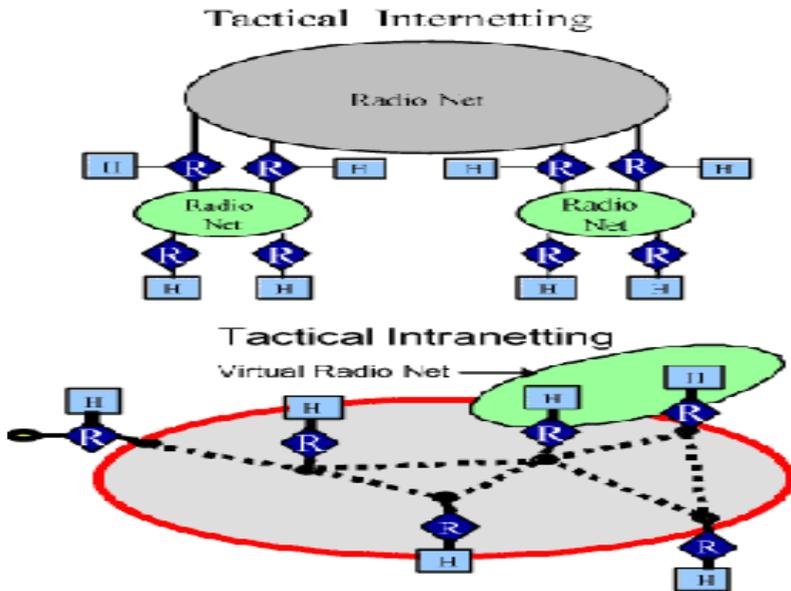


Fig. 5b. Wireless RF Networks

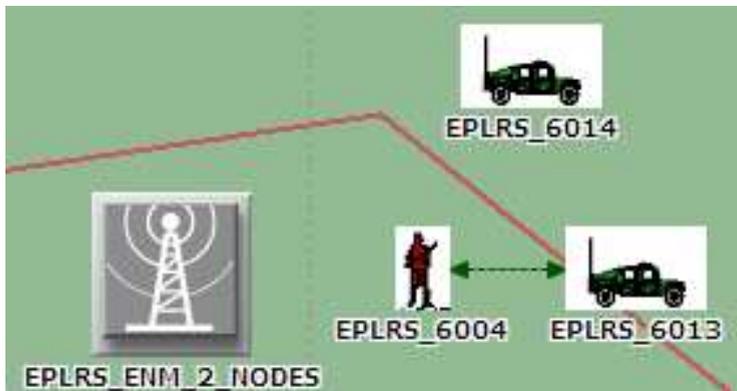


Fig. 5c. Two wireless nodes network

7. Future possibilities

Bayesian Analysis [17] – the Bayesian’s Theorem looks at probability as a measure of a state of knowledge, whereas traditional probability theory looks at the frequency of an event happening. In other words, Bayesian probability looks at past events and prior knowledge and tests the likelihood that an observed outcome came from a specific probability distribution. With some sample field data the Bayesian’s Theorem can be applied including wireless RF communications & computer networking science in tactical military applications. The research presented here is for building a set of “Bayesian network

vulnerabilities graph” for vulnerability study in tactical wireless RF networks. Bayesian network is designed in vulnerabilities graph and model all potential attack steps in a given network. Each wireless network node represents a single security property violation mode; each link edge corresponds to an exploitation of one or more possible vulnerabilities and each network path represents a series of exploits that can signify a potential vulnerability for attack within a tactical RF wireless communication network. Inference is played a major part in our vulnerability calculations. Future research work will involve looking into different kinds of Bayesian’s network (BN) with advanced topological arrangements as in figure 6 below with multiple experts and multiple factors analysis for our more advanced JCSS wireless RF vulnerabilities analysis.

BEFORE:	AFTER:
Scenario IER Summary	Scenario IER Summary
Total IER Sent: 1999	Total IER Sent: 1999
Total IER Received: 1999	Total IER Received: 1121
Total IER Failed: 0	Total IER Failed: 878
Total IER Undelivered: 0	Total IER Undelivered: 0
Total IER Perished: 0	Total IER Perished: 0

Fig. 5d. Sample results generated by JCSS scenarios

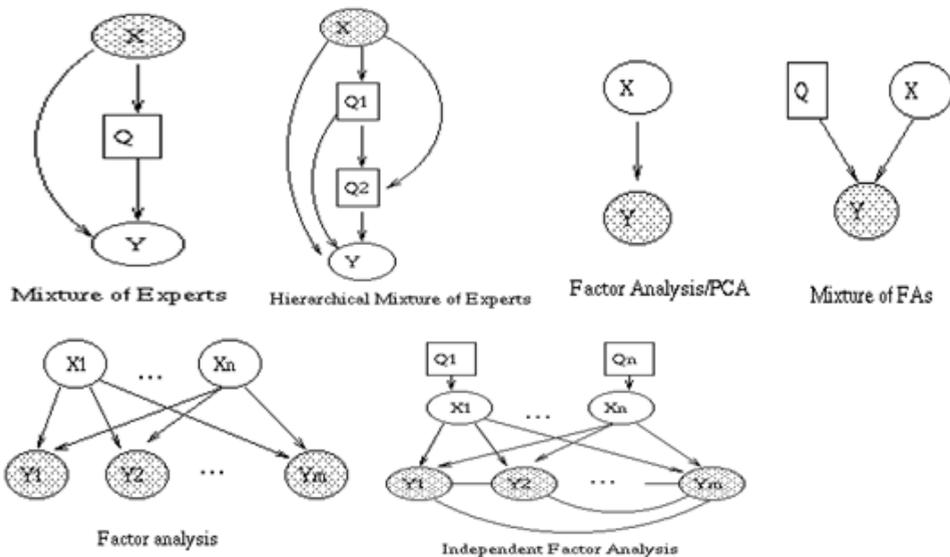


Fig. 6. Multiple experts and multiple factors analysis

7.1 Adaptive Bayesian network and scoring system

Finally, we may consider an adapted Bayesian network (BN) of wireless tactical network analysis with a RF Vulnerability Scoring System (RF-VSS) that can generate weighted scores in the research. The Common Vulnerability Scoring System (CVSS), a NIAC research project from U.S. Department of Homeland Security. This rating system is designed to provide open and universally standard severity ratings of vulnerabilities in certain specific systems. It creates a global framework for disclosing information about security vulnerabilities. The CVSS may be recognized and generally accepted by the public in support, international coordination and communication to ensure successful implementation, education and on-going development of the scoring system. It serves a critical need to help organizations appropriately prioritize security vulnerabilities across different domains. A common scoring system has the advantages of solving the similar problems with better coordination. Based upon the Common Vulnerability Scoring System develops by Peter Mell et al. [22], we think this is a very valuable, useful tool and scoring system for quickly assessing wireless RF security and vulnerabilities. RF-VSS scores are derived from three scores: a "base network" score, an "adversaries impact" score, and an "environmental impact" score. These can better be described as "fixed" score, "external variable" score, and "wireless RF network experts" assigned score. The base network system score is fixed at the time the vulnerability is found and its properties do not change. The base assigned score includes numerous scoring metrics. Each of these metrics will then be chosen from a pre-determined list of options. Each option has a value. The values are then fed into a formula to produce the base network score. Next comes the temporal or adversaries impact score. The adversaries impact score changes and revises the base network score up or down. The temporal or adversaries impact score can also change over time (thus it is "time sensitive"). For example, one of the component metrics of the adversaries impact score is System Remediation Level (SRL). This means, there exists a possible common defense fixes out there, maybe from a contractor or vendor or an emergency research workaround. If, when the detected vulnerability is first encountered, there may be no possible fix, then the temporal or adversaries impact score will be much higher. But when a solution or fix is possible, then the score will go down dramatically. Again, it was temporary and a changing factor. There are three possible vulnerabilities metrics that make up the temporal or adversaries impact score. This score is then multiplied by the base network score to produce a new score. This first computed new score will be produced based upon the current operating wireless RF network scenarios set up via background expert diagnostic. The final part is the environmental impact score. This is how the final vulnerability will affect the wireless RF network. The researchers get to determine how the combined vulnerabilities might affect the overall wireless RF network in field deployment. If the vulnerability has very little risk or to do with all the listed factors then this computed score will be very, very low (like zero). There are five metrics that affect the environmental impact score. This portion is combined with the base network and temporal adversaries impact score to produce a final score. The score will be on a scale of 1-10. If it is a low 2, then don't be too worried. However, a rather higher score like 6 or above might indicate major security issues in terms of security. We will provide a vulnerabilities smart index by constructing a novel calculator with a set of RF Vulnerability Scoring System (RF-VSS) for final system vulnerability analysis. For an example: For a given wireless RF radio network, according to expert released analysis and advisory, there are a set of "RF wireless

network vulnerabilities" being assigned. The example metrics for the given wireless RF network scenarios with vulnerabilities are: (1) base network impact, (2) temporal or adversaries' impact and (3) Environmental impact.

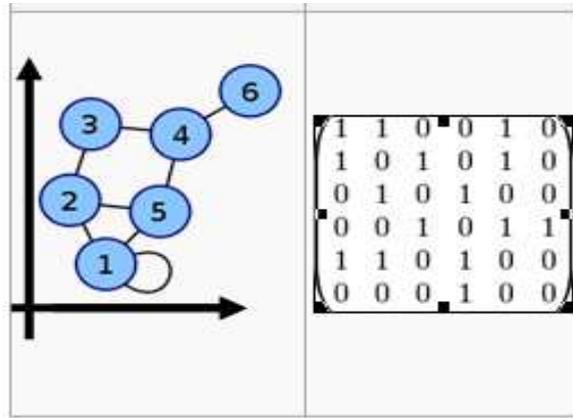


Fig. 7. Transposing the vulnerabilities graph into a matrix for analysis

So, overall a base RF wireless network vulnerability score of 8.8 (very bad) that is slightly mitigated to 7.9 by the temporal or adversaries metrics. Still, 7.9 is not a great score and still has considerable amount of risk. Now, this is where the final environmental impact score comes in to alter the landscape. The negative impact may be bad for the overall wireless RF network when we look at the environmental impact metrics calculated before for certain wireless network scenarios as illustrated above. We gather all those factors into the RF Vulnerability Scoring System (RF-VSS) calculator and it produces an environmental score of 6.5 which translates into high vulnerabilities. This is a relatively good approach to determine what the overall risk is for a give wireless RF network and the RF Vulnerability Scoring System (RF-VSS) analysis is based upon the Common Vulnerability Scoring System develops by Peter Mell [22] and associates with additional features of Bayesian networks [17] (also known as belief network). Using adjacency-matrix as a starting point, a more quantitative wireless RF network vulnerability assessment may be achieved. An adjacent edge counts as 1 unit in the matrix for an undirected graph as illustrated in figure 7. (For example a given X, Y coordinates that are numbered below from #1 to #6 may be transposed into a 6x6 matrix.)

8. Conclusion

A possible framework with systems engineering approach [7] [8] is utilized. The ultimate goal is now partially achieved by providing a comprehensive network assessment methodology. Our study illustrates using system engineering thinking, Bayesian networks [17] can be applied during the analysis as a powerful tool for calculating security metrics regarding information system networks. The use of our modified Bayesian network model with the mechanisms from CVSS is in our opinion an effective and sound methodology contributing towards improving the research into the development of security metrics by constructing a novel calculator with a set of RF Vulnerability Scoring System (RF-VSS) for

final system vulnerability analysis. We will continue to refine our approach using more dynamic Bayesian Networks to encompass the temporal domain measurements established in the CVSS. This short paper demonstrated an approach to model all potential vulnerabilities in a given tactical RF network with Bayesian graphical model. In addition, using a modified belief decision matrix, the research can describe a multiple criteria decision analysis (MCDA) using Evidential Reasoning Approach [3] [4] [5] [6]. It was used to support various decision analysis, assessment and evaluation activities such as impact and self assessments [1] [2] based on a range of quality models. In decision theory, evidential reasoning approach (ER) is generally a evidence-based multi-criteria decision analysis (MCDA) for dealing with some problems having both quantitative and qualitative criteria with various uncertainties including ignorance and randomness. With evidential reasoning approach, a generic evidence-based multi-criteria decision analysis (MCDA) approach is chosen for dealing with problems having both quantitative and qualitative criteria with variables. This matrix may be used to support various decision analysis, assessment and evaluation activities such as wireless RF networks environmental impact assessment and wireless RF networks internal nodes (transceiver) assessment based on a range of quality models that are developed. Bayesian vulnerabilities graphs provide comprehensive graphical representations with conventional spanning tree structures. The Bayesian vulnerabilities graph model is implemented in Java, and it is deployed along with JCSS software. JCSS is the Joint Net-Centric Modeling & Simulation Tool used to assess end-to-end communication network capabilities and performance. It is the Joint Chiefs of Staff standard for modeling military communications systems. JCSS is a desktop software application that provides modeling and simulation capabilities for measuring and assessing the information flow through the strategic, operational, and tactical military communications networks. Our new tool can generate implement vulnerabilities network graph with link edges and weights. All these may be transposed into an adjacency-matrix as illustrated before for a more quantitative wireless RF network vulnerability assessment. The convention followed here is that an adjacent edge counts as one in a matrix for an undirected graph as illustrated before in figure 7. For a given X, Y coordinates, for instant; they can be numbered from one to six and may also be transposed into a 6x6 matrix. The vulnerabilities analysis with the help of system engineering approach [25] [26] [29] of a wireless RF network is then achieved by assigning corresponding measurement metrics with posterior conditional probabilities of Bayesian network [17]. The Bucket Elimination algorithm is adapted and modified for probabilistic inference in our approach. The most common approximate inference algorithms are stochastic MCMC simulation, bucket algorithm and related elimination steps which generalizes looping and aggregated belief propagation, and variation methods. A better approximate inference mechanism may be deployed in the near future for more complex vulnerabilities graph. Our method is very applicable to tactical wireless RF networks by picking, implementing each model's communication stages and states. The result when using with OPNET JCSS [12] simulation and modeling will provide both graphical quantitative and real assessment of RF network vulnerabilities at a network topology state and during time of actual deployment.

9. Acknowledgment

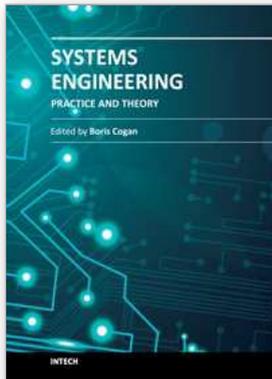
The authors thank Dr. John V. Farr, Dr. Ali Mostashari, Dr. Jose E. Ramirez-Marquez of the Department of Systems Engineering, Stevens Institute of Technology for many fruitful

discussions in the early stages, the referees for helpful comments, for providing outstanding intellectual environments and significant guidance. We appreciate the assistance of Dr. Jessie J. Zhao who proof read some of the technical materials. Finally, we also thank the countless effort and insight contributed to this research by Dr. Mung Chiang, Professor of Electrical Engineering Department from Princeton University for his excellent technical skills, strategies and valuable advice in applying conventional and distributed convex optimization in the area of wireless communication network.

10. References

- [1] Wang Y.M., Yang J.B. and Xu D.L. (2006). "Environmental Impact Assessment Using the Evidential Reasoning Approach". *European Journal of Operational Research*, 174 (3): 1885–1913.
- [2] Siow C.H.R., Yang J.B. and Dale B.G. (2001). "A new modeling framework for organizational self-assessment: development and application". *Quality Management Journal* 8 (4): 34–47.
- [3] Keeney, R. & Raiffa, H. (1976). *Decisions with Multiple Objectives*. Cambridge University Press. ISBN 0521438837.
- [4] Shafer, G.A. (1976). *Mathematical Theory of Evidence*. Princeton University Press. ISBN 0691081751.
- [5] Yang J.B. & Xu D.L. (2002). "On the evidential reasoning algorithm for multiple attribute decision analysis under uncertainty". *IEEE Transactions on Systems, Man and Cybernetics Part A: Systems and Humans* 32 (3): 289–304.
- [6] Xu D.L., Yang J.B. and Wang Y.M. (2006). "The ER approach for multi-attribute decision analysis under interval uncertainties". *European Journal of Operational Research* 174 (3): 1914–43.
- [7] Popper, S., Bankes, S., Callaway, R., and DeLaurentis, D., *System-of-Systems Symposium: Report on a Summer Conversation, July 21-22, 2004*, Potomac Institute for Policy Studies, Arlington, VA.
- [8] Manthorpe Jr., W.H., "The Emerging Joint System-of-Systems: A Systems Engineering Challenge and Opportunity for APL," *Johns Hopkins APL Technical Digest*, Vol. 17, No. 3 (1996), pp. 305–310.
- [9] Li, B.; Xu, Y. & Choi, J. (1996). *Applying Machine Learning Techniques, Proceedings of ASME 2010 4th International Conference on Energy Sustainability*, pp. 14-17, ISBN 842-6508-23-3, Phoenix, Arizona, USA, May 17-22, 2010
- [10] Kotov, V. "Systems-of-Systems as Communicating Structures," *Hewlett Packard Computer Systems Laboratory Paper HPL-97-124*, (1997), pp. 1-15.
- [11] Luskasik, S. J. "Systems, Systems-of-Systems, and the Education of Engineers," *Artificial Intelligence for Engineering Design, Analysis, and Manufacturing*, Vol. 12, No. 1 (1998), pp. 55-60
- [12] Adamy, D. L. "EW103: Tactical Battlefield Communications Electronic Warfare", Artech House, ISBN-13: 978-1-59693-387-3, 2009.
- [13] JCSS. *The Joint Net-Centric Modeling & Simulation Tool*. JCSS Project Manager, JCSS@disa.mil Commercial: (703) 681-2558.
- [14] Chan P., U.S. Army, ARL patent (pending) - ARL Docket No. ARL 06-37. "Network Security and Vulnerability Modeling & Simulation Libraries".

- [15] Chan P., U.S. Army, ARL patent (pending) - ARL Docket No. ARL 10-09. "Wireless RF Network Security and Vulnerability Modeling & Simulation Toolkit - Electronic Warfare Simulation & Modeling of RF Link Analysis with Modified Dijkstra Algorithm".
- [16] Swiler, Phillips, Ellis and Chakerian, "Computer-attack graph generation tool," in Proceedings of the DARPA Information Survivability Conference & Exposition II (DISCEX'01), vol. 2.
- [17] Liu Yu & Man Hong, "Network vulnerability assessment using Bayesian networks," Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005. Proceedings of the SPIE, Volume 5812, pp. 61-71 (2005).
- [18] Leonard T. & Hsu J., "Bayesian Methods: An Analysis for Statisticians and Interdisciplinary Researchers," Cambridge University Press, ISBN 0-521-00414-4, 1997.
- [19] Sheyner, Lippmann and J. Wing, "Automated generation and analysis of attack graphs," in Proceedings of the 2002 IEEE Symposium on Security and Privacy (Oakland 2002), pp. 254-265, May 2002.
- [20] Dijkstra E., Dijkstra's algorithm. Dutch scientist Dr. Edsger Dijkstra network algorithm. http://en.wikipedia.org/wiki/Dijkstra's_algorithm
- [21] Phillips & Swiler, "A graph-based system for network-vulnerability analysis," in Proceedings of the 1998 workshop on New security paradigms, pp. 71-79, January 1999.
- [22] Ammann, Wijesekera and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in Proceedings of 9th ACM conference on Computer and communications security, pp. 217-224, November 2002.
- [23] Mell & Scarfone, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0", National Institute of Standards and Technology. <http://www.first.org/cvss/cvss-guide.html#n3>.
- [24] Systems Engineering Fundamentals. Defense Acquisition University Press, 2001.
- [25] Chan P., Mansouri M. and Hong M., "Applying Systems Engineering in Tactical Wireless Network Analysis with Bayesian Networks", Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference, Publication Year: 2010 , Page(s): 208 - 215.
- [26] Defense Acquisition Guidebook (2004). Chapter 4: Systems Engineering.
- [27] Bahill, T. & Briggs, C. (2001). "The Systems Engineering Started in the Middle Process: A Consensus of Systems Engineers and Project Managers". in: Systems Engineering, Vol. 4, No. 2 (2001)
- [28] Bahill, T. & Dean, F. (2005). What Is Systems Engineering?
- [29] Boehm, B. (2005). "Some Future Trends and Implications for Systems and Software Engineering Processes". In: Systems Engineering, Vol. 9, No. 1 (2006)
- [30] Vasquez, J. (2003). Guide to the Systems Engineering Body of Knowledge - G2SEBoK, International Council on Systems Engineering.
- [31] Lima, P.; Bonarini, A. & Mataric, M. (2004). *Application of Machine Learning*, InTech, ISBN 978-953-7619-34-3, Vienna, Austria



Systems Engineering - Practice and Theory

Edited by Prof. Boris Cogan

ISBN 978-953-51-0322-6

Hard cover, 354 pages

Publisher InTech

Published online 16, March, 2012

Published in print edition March, 2012

The book "Systems Engineering: Practice and Theory" is a collection of articles written by developers and researchers from all around the globe. Mostly they present methodologies for separate Systems Engineering processes; others consider issues of adjacent knowledge areas and sub-areas that significantly contribute to systems development, operation, and maintenance. Case studies include aircraft, spacecrafts, and space systems development, post-analysis of data collected during operation of large systems etc. Important issues related to "bottlenecks" of Systems Engineering, such as complexity, reliability, and safety of different kinds of systems, creation, operation and maintenance of services, system-human communication, and management tasks done during system projects are addressed in the collection. This book is for people who are interested in the modern state of the Systems Engineering knowledge area and for systems engineers involved in different activities of the area. Some articles may be a valuable source for university lecturers and students; most of case studies can be directly used in Systems Engineering courses as illustrative materials.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Philip Chan, Hong Man, David Nowicki and Mo Mansouri (2012). System Engineering Approach in Tactical Wireless RF Network Analysis, Systems Engineering - Practice and Theory, Prof. Boris Cogan (Ed.), ISBN: 978-953-51-0322-6, InTech, Available from: <http://www.intechopen.com/books/systems-engineering-practice-and-theory/system-engineering-approach-in-tactical-wireless-rf-network-analysis>

INTECH

open science | open minds

InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2012 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the [Creative Commons Attribution 3.0 License](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.