INTECH
open science | open minds

OPEN ACCESS
ARTICLE

International Journal of Engineering Business Management

Managing Vulnerabilities of Tactical Wireless RF Network Systems: A Case Study

Regular Paper

Philip Chan[1,3], David Nowicki[1], Hong Man[2] and Mo Mansouri[1]

1 Department of Systems Engineering, Stevens Institute of Technology, USA
2 Department of Electrical and Computer Engineering, Stevens Institute of Technology, USA
3 Department of CMIS/CMSC, University of Maryland University College, USA
* Corresponding author E-mail: PWChan@faculty.umuc.edu

Received 03 Jan 2012; Accepted 20 Jan 2012

Abstract Organisations and individuals benefit when wireless networks are protected. After assessing the risks associated with wireless technologies, organisations can reduce the risks by applying countermeasures to address specific threats and vulnerabilities. These countermeasures include management, operational and technical controls. While these countermeasures will not prevent all penetrations and adverse events, they can be effective in reducing many of the common risks associated with wireless RF networks. Among engineers dealing with different scaled and interconnected engineering systems, such as tactical wireless RF communication systems, there is a growing need for a means of analysing complex adaptive systems. We propose a methodology based on the systematic resolution of complex issues to manage the vulnerabilities of tactical wireless RF systems. There are is a need to assemble and balance the results of any successful measure, showing how well each solution meets the system's objectives. The uncertain arguments used and other test results are combined using a form of mathematical theory for their analysis. Systems engineering thinking supports design decisions and enables decision-makers to manage and assess the support for each solution. In these circumstances, complexity management 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 resolutions which this system helps to facilitate. Smart and innovative performance matrixes are introduced using a mathematical Bayesian network to manage, model, calculate and analyse all the potential vulnerability paths in wireless RF networks.

Keywords Engineering Management, Network Vulnerabilities, Systems Engineering, Bayesian Analysis, Risk Control

1. Introduction

Department of defence organisations recognise that tactical wireless communications networks are critical, flexible and efficient to use. Wireless network systems have been deployed among agencies and remote offices while maintaining connectivity with the local wireless

network. Wireless tactical networks allow the sharing of data and applications with other network systems with compatible RF communication devices, without being tied to other local connections. Tactical portable and commercially available Off-The-Shelf (COTS) devices, such as wearable military mini-computers, iPad-like gadgets and third- or fourth-generation modified secure smart phones that can synchronise military signals between classified tactical networks' servers, are being considered. These tactical wireless RF network systems carry various classified and unclassified network services, such as wireless email, user applications, browsing and Internet access. Wireless networks are exposed to many of the same risks as wired networks. In addition, they are also vulnerable to additional risks. Tactical wireless networks transmit data through radio frequencies and are open to unauthorised intruders unless they are fully protected. External and internal intruders can exploit this open weakness in order to access the RF systems, destroy or expose critical data, and launch undesirable attacks that hold up the network bandwidth and initiate numerous denials of service assaults to numerous authorised users. Checklists are needed that defence departments and related organisations will find it useful to assess the cyber security of their wireless networks systems. Information on how to manage wireless frequencies and their applications are very useful in terms of wireless spectrum communication standards, such as the IEEE 802.11 wireless local area network (WLAN), and research information about the effectiveness of wireless networking tools. Tactical wireless network vulnerabilities are continually reported and are critically studied by many U.S. government organisations. The need for a comprehensive framework for network vulnerability assessment using a systems engineering management approach [24] [26] [27] [28] [30] [31] has posed an increasing challenge for many research analysts. Researchers have proposed a more systematic means of managing wireless network nodes and trees using possible chains of events and then performing normal post-graph vulnerability assessments with a system of systems methodology. The most recent system engineering approaches build attack trees by attempting to number all of the potential attack paths with the identification of vulnerabilities, node probability calculations, inference analysis, and weight assignments by system experts. These constitute a form of expert-driven vulnerability analysis. Assessment and identification provide some of the main key issues in ensuring the proper security of a given deployed tactical RF communication network. The vulnerability assessment process involves many uncertain factors which reside within both the networks and the network nodes.

Threat assessment (or injecting threats) constitutes one of the major factors in evaluating a situation for its suitability for supporting decision-making and giving an indication of the security of a given tactical RF communication network system. One approach uses an experienced decision-makers database. This type of expert-driven database records most of their decisions on vulnerability identification. The decision-makers use past experience for their decisions, which 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 network configurations. Any similar situations and actions that have worked well in past cases will be considered in the assessment due to the present situation 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]. Bayesian networks (BN) and various related methods [17] provide an effective tool for modelling situations of uncertainty and knowledge.

This paper discusses the Bayesians' Theory [17], Bayesian networks and their ability to function in a given tactical RF communication network [11] for vulnerability analysis and identification. This paper presents an approach for using a Bayesian network to model all potential vulnerabilities or attack paths in a given tactical RF wireless network. We will call such graph a "Bayesian network vulnerabilities graph" for a given tactical RF wireless network. It provides a more compact representation of attack paths than is offered by conventional methods. Methods of Bayesian inference can be used for probabilistic analysis. It is necessary to use algorithms for updating and computing optimal subsets of attack paths relative to any current knowledge of attackers. The tactical RF wireless models were tested on a small sample JCSS [12] network. The simulated test results demonstrate the effectiveness of approach.

2. Environmental Risk Factors

Sensitive classified data and critical information that is broadcast between two wireless nodes and devices can be intercepted and disclosed if not shielded and protected by strong encryption technology. Handheld devices, which are easily pried open and stolen, can reveal sensitive personal information. Up until the early 2000s, Wireless Encryption Protocol/Wired Equivalent Privacy (WEP) was the primary security mechanism used to safeguard wireless computer networks. In recent years, Wi-Fi Protected Access (WPA and WPA2) has replaced the WEP method as the standard for all wireless network security. Wireless networks and handheld devices are vulnerable to many of the same threats as conventional wired networks. Intruders may gain access to critical systems via wireless communications and can bypass any monitoring and penetrate the firewall protection. Once

they receive the right of entry, intruders can easily launch multiple levels of denial of service (DOS) attacks, embezzle and use unauthorised identities, violate the privacy of the legitimate users of classified information, insert viruses or malicious code, and even destroy or disable operations. Before establishing tactical wireless networks, organisations should use sound risk management processes to assess the risks involved, to take steps to reduce potential risks to an acceptable level, and to maintain that acceptable level of risk. Using risk management processes, project leaders can protect systems and information in a cost-effective manner by balancing the operational and economic costs of the required protective measures with the gains in mission capability through the adoption of new technology.

3. Methodology

Systems engineering [7] [8] [27] [28] methodology is applied here to assist with the rapid design and development of complex systems, such as tactical wireless communication systems. Systems engineering [29] uses the techniques of the engineering sciences with operations research. Operations research also tackles the design of complex systems. Our goal is to utilise the concurrent engineering principles in systems engineering analysis which cover our design goals and testing requirements in the development of the RF communication system. The systems approach to solving complex problems is critical since the integrating of complex analyses and the building of RF communication models requires a synthesis of different methods. The systems approach is widely used and successful in the field of engineering, for example systems engineering. It is most effective in treating the complex phenomena present in tactical wireless RF communication networks. 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. Further knowledge may be gained about the parts in order to better understand the whole nature of a given tactical RF communications system. The system and its details at many levels may then be decomposed into several subsystems and into sub-subsystems - and so on - to the last details. At the same time, we can change focus in order to view different levels so that users are not overwhelmed by complexity. From time to time, abstract levels of information may be hidden in order to assist focus on a certain task for more detailed analysis. We may simplify the system by treating some of its parts as black boxes apart from their interfaces. Hiding information for more certain RF tactical analysis is not the same as discarding it. The same black box can be opened at a 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 improve system-level performance. The systems approach is effective not only for understanding and designing tactical RF wireless communication systems but also for abstract constructions in mathematical theories. Instead of an actual RF communication physical module, a RF wireless network “subsystem” can form a concept within a conceptual scheme, and its “interfaces” can be formed by relations to others in the scheme. Initially, the analyses and concepts will sometimes be approximated. We can then refine approximations, step-by-step, towards a better answer with our method of analysis. The systems approach is not merely a system-level approach but rather it delves into lower-level subsystems. The system-level is powerful and appropriate in some cases, but it also misses out on most of the structures and the dynamics of the system. It is not employed in our systems approach, since modularity is studied here. A systems approach is an integral part of systems engineering. Our analysis may also call reduction and "lessening" so as to acquire yet finer information and this also underlines the importance of detailed analysis.

4. Vulnerabilities

Vulnerability is characterised in terms of the susceptibility (uncountable) to attack or damage from adversaries; it is defined as the state or condition of being weak or poorly defended. For example, from military or DoD point of view, it is defined for a given tactical wireless RF communication systems which have a defence vulnerability after experiencing an external EW high power electronic blasting attack on a specific bandwidth. Another definition of vulnerability looks to a specific list of weaknesses (countable) in the defences surrounding a given tactical wireless RF communication system. In general, vulnerability means the state of being vulnerable in terms of a susceptibility to attack from external and internal forces. In this instance, these are the vulnerabilities of tactical wireless RF communication systems when dealing with external and internal factors. In order to better manage the vulnerabilities in a system of systems [9] [10], a compilation of task-oriented or dedicated systems that bundle their resources and capabilities together in order to obtain a newer, more complex system that offers more functionality and better performance than is provided with a simple summation of basic systems. Currently, system of systems stands as a critical research discipline that supplements engineering processes, quantitative analysis, tools and design methods. The methodology for defining, abstracting, modelling and analysing 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 to our study of tactical wireless

communications systems. The goal will be to link systems into a joint system of systems which allows for the interoperability and integration of Command, Control, Computers, Communications, and Information (C4I) and Intelligence, Surveillance and Reconnaissance (ISR) systems as a description in the field of information management control in modern armed forces. The integration of a system of systems is a method for pursuing better development, integration, interoperability, and the optimisation of systems so as to enhance performance in future combat zone scenarios that are related to the area of the integration of intensive information. One can predict that the modern systems which comprise system of systems problems are not merely massive and that they have certain common characteristics: operational independence among the individual systems and the 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 behaviours that would not be apparent if the systems and their interactions were modelled separately. Taken together, all of these background requirements suggest that a complete system of systems engineering framework is 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 is desired to help decision-makers to determine whether related infrastructure, policy and technological 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 technological challenges, but also because such problems require large resource commitments and investment with costs over many years. The birds-eye view provided by using a system of systems approach will allow an individual system constituting a system of systems that will be different and which will operate independently. The interactions reveal certain important, emergent properties. These emergent patterns have an evolving nature which the RF communication systems' stakeholders must recognise, analyze and understand. The system of systems way of thinking promotes a new approach to solving grand challenges where the interaction of current technology, organisational policy and resources are the primary drivers. A system of systems study is also integrated with the study of designing, complexity and systems engineering. A system of systems typically exposes the behaviours of complex systems. However, not all complex problems fall into the area of a system of systems. Systems of systems have, by their nature, several combinations of qualities, not all of which are exhibited in the operation of heterogeneous networks of systems. Current research into effective approaches to system of systems problems includes consideration of proper frames of reference and design architecture. Our study of RF communication network modelling, simulation and techniques of analysis will include network theory, agent-based modelling, probabilistic (Bayesian) robust design (including uncertainty modelling/management), software simulation and programming with multi-objective optimisation. We have also studied and developed various numerical and visual tools for capturing the interaction of RF communication systems' requirements, concepts and technologies. A system of systems approach continues to be employed predominantly in the defence sector and space exploration. The system of Systems engineering methodology is used heavily by the U.S. Department of Defence, but it is increasingly being applied to many non-defence 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 involve slightly different fields of study. Systems engineering addresses the development and operation of one particular product, like RF communication networks. System of systems engineering addresses the development and operation of evolving programs. Traditional systems engineering seeks to optimise an individual system (i.e., the target product), while system of systems engineering seeks to optimise a network of various interacting old and new systems that brought together to satisfy multiple objectives of the program. It enables decision-makers to understand the implications of various choices for technical performance, cost, extensibility and flexibility over time, and the effectiveness of the methodology. It may prepare decision-makers for designing informed architectural solutions for system of systems context problems. The objective in our research is to focus on tactical wireless network within the context of the system of systems research area. The ultimate goal is to provide a comprehensive network assessment and sound management methodology and possible framework.

5. Engineering Approach

Systems engineering management [7] [8] [9] is employed here in order to look into the vulnerabilities of wireless networks through simulation and the modelling of work-processes. A set of useful tools is developed to handle the vulnerability analysis aspect of the RF wireless network. In the research, we have summarised a variety of methods for building network trees with chains of possible exploits, and we then performed the normal post-graph vulnerability assessment and analysis. Recent approaches recommend building more advanced attack trees by trying to number all of the potential attack paths with the identification of vulnerabilities, nodes'

probability calculations, inference analysis, and weight assignments by system experts. Vulnerabilities' analysis, assessment and identification are one of the key issues in making sure of 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 involved in evaluating a situation for its suitability to support decision-making and the indication of the security of a given tactical RF communication network system. The methodology of systems engineering in the research plays a critical role in helping develop a distinctive set of concepts and a methodology for the assessment of the vulnerability of tactical RF communications networks. Systems engineering approaches have been developed in order to meet the challenges of engineering the functional physical systems of tactical RF communications networks with complexity. The system engineering process employed here is a brand of the holistic concept of system engineering processes. With this holistic view in mind, systems engineering focuses on analysing and understanding the U.S. government's needs as a potential customer. Re-useable RF connectivity models with requirements and functionality are implemented early in the development cycle of these RF communications network models. We then proceed with design synthesis and system validation while considering the complete problem, namely the system lifecycle. Based upon the concept by Oliver et al. [23], systems engineering technical processes are adopted during the course of the research. Within Oliver's model [23], the technical process includes assessing the available information and defining effectiveness measures in order to create a Bayesian vulnerabilities model of behaviour, create a structure model, perform trade-off analysis, and create a sequential build-and-test plan. At the same time, a RF communication system can become ever more complex due to an increase in network size as well as an increase in the amount of data on vulnerabilities, engineering variables, and the number of fields that are involved in the analysis. The development of smarter matrices with better algorithms constitutes 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 modelling and simulation methodologies, optimisation calculations and vulnerability analysis. Taking an interdisciplinary systems engineering approach to perform a vulnerability analysis using a Bayesian graph with a weights calculation is inherently complex. The behaviour of - and interaction among - RF wireless network systems' components can be well-defined, at least in some cases. Defining and characterising such RF communication systems and subsystems and the interactions among in a manner that supports vulnerability analysis is one of the goals of the research.

6. Research Insights

Decision matrixes are used for vulnerability analysis in the research. A decision matrix is an arrangement of related qualitative or quantitative values in the form of rows and columns. It allows our research to graphically identify, analyse and rate the strength of relationships between sets of information on vulnerabilities. The elements of a decision matrix represent decisions based upon calculations. Bayesian network (BN) plays a role on certain vulnerabilities decision criteria. Matrix development is especially useful and critical for looking at large samples of decision-factors and assessing each factor's relative importance. The decision matrix employed in the research is used to describe a multi-criteria decision analysis (MCDA) for a tactical RF wireless network. When given a MCDA problem, where there are M alternative options and each needs to be assessed according to N criteria, this can be described by a decision matrix which has M rows and N columns, or M × N elements. Each element, such as Xij, 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 Xij = "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} = Good	...
Alternative *M*	x_{M1}	x_{M2}	...	x_{MN}

Table 1. Multi-criteria decision analysis (MCDA) matrix

Using a modified belief decision matrix, the research is now more refined and the matrix can describe a multiple criteria decision analysis (MCDA) problem within 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 which have both quantitative and qualitative criteria under various uncertainties. This matrix may be used to support various decision analyses and the assessment and evaluation of 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 have been developed. For a given MCDA, there are M alternative options each of which needs to be assessed according to N criteria and the belief decision matrix for the problem has M rows and N columns, or M X 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 (e.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 (e.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 a 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. Modified multi-criteria decision (MCDA) matrix

The research may help to develop a more systematic and automated approach for building a "Bayesian network vulnerabilities graph" with weight assignments for the study of vulnerability in tactical wireless RF networks [11]. A Bayesian network [17] is designed in terms of vulnerabilities graphs and models all of the potential attack steps in a given network. As described by Leonard and Hsu [17], using the 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:

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}.$$

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 it acts as a normalising constant. In this form, the theorem provides a mathematical representation of how the conditional probability of an event A given event B is related to the converse conditional probability of event B given event A. In our research, each wireless network node represents a single security and vulnerability point and contains a property violation mode; each link's 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 to attack within the RF wireless network. The communication model takes on the characteristics of a tactical wireless RF network, and we consider an integrated posterior probability of Bayesian networks (BN) [17] with a well-defined security metric representing a more comprehensive quantitative vulnerability assessment of a given tactical RF network which contains different communication stages. The 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, with wireless stage A having a vulnerability of 0.35 accuracy due to a noise factor and a 0.85 accuracy due to a jamming factor, and with wireless stage B having a vulnerability of 0.75 accuracy due to a noise factor and a 0.45 accuracy due to jamming. Now, if a wireless stage is selected at random, the probability that wireless stage A is chosen is 0.5 (50% chance, one out of two stages). This is the *a priori* probability for the vulnerability of the wireless communication stage. If we are given an additional piece of information, namely 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? The posterior probability takes into account this additional information and revises the probability downward from 0.5 to 0.35 according to Bayesian's theorem. Moreover, the noise factor's effect is more probable at stage B (0.75) than at stage A (0.35). When the factor is instead jamming, the probability that the chosen wireless stage is A will be revised upward from 0.5 to 0.85. Here, the vulnerability related jamming factor is now definitely less probable at stage B (0.45) than at stage A (0.85). The conditional independence relationship encoded into 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 dependent with respect to some fixed topological ordering of the wireless nodes. Using Fig. 1, below, to demonstrate the outcomes, through the chain rule of probability with stages C, S, R and W, the joint probability of all the nodes in the vulnerabilities graph is now: 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 these 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 it, but the factored form would require **O(n** $_2 k$ **)** space to represent it, where k is the maximum fan-in of a node with fewer overall parameters.

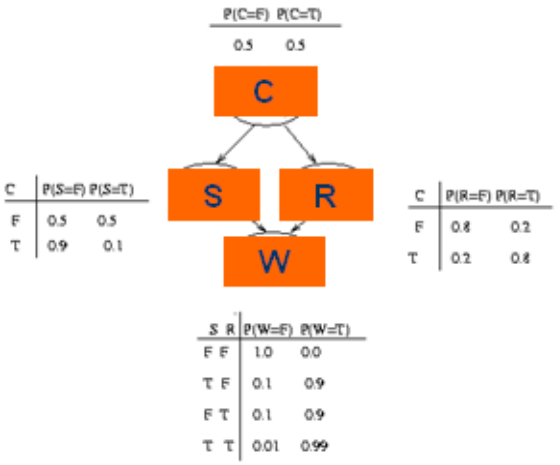

Figure 1. Vulnerabilities graph (simple stage within a wireless node)

In the model, we are concerned with the vulnerability of the wireless network caused by the failure of various communication stages in the wireless RF communication network. Fig. 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 a transmitter and receiver with different stages. The purpose of our modelling and simulation is to make use of the DISA JCSS Transceiver Pipeline stages [12]. All of the vulnerability data may be collected and the following information may be collected at run-time: (1) the effect of the transmission on nodes in the vicinity, (2) the set of nodes will attempt to receive the packet, (3) the determination of whether a node attempting to receive a packet did so successfully, (4) the time it takes 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 "Group Receiver" start with the index "Group 0". The transmitter is executed once at the start of simulation for each pair of transmitter and receiver channels or else dynamically by OPNET JCSS's [12] Kernel Procedure (KP) calls. Inside the radio pipeline stages of the receiver side, for every receiver channel which "passed" the transmission checks, the simulated RF packet will "flow" through the pipe. Using JCSS [12] and OPNET Modeller, it is crucial to make sure that the JCSS Radio Pipeline Model's [12] attributes are being configured correctly. This is particular important for military RF radios like EPLRS [12] during a lay-down of network nodes in different scenarios. In all cases, the configuration should be retained and saved in the node model. In summary, for a radio transmitter, there are six (6) different stages (stage 0 through to stage 5) associated with each radio transmitter. The following are the six stages of a given radio transmitter (RT): Receiver Group, Transmission Delay, Link Closure, Channel Match, Transmitter (Tx) Antenna Gain and Propagation Delay. As for the Radio Receiver, there are eight (8) stages (stage 6 through to stage 13) that are associated with a Radio Receiver (RR): Rx Antenna Gain, Received Power, Interference Noise, Background Noise, Signal-to-Noise Ratio, Bit Error Rate, Error Allocation and Error Correction. In JCSS [12] and the OPNET Modeller, there are, altogether, 14 Pipeline Stages (PS) that implement the vulnerabilities graphs for the analysis of Bayesian networks' (BN) [17]. These are customised collections of sequences of 'C' or 'C++' procedures (code & routines) with external Java subroutines and portable applications written for research purpose. In Fig. 2, each of the 14 different stages that are comprised by a transceiver network performs a different calculation. For example, in (1) Line-of-sight, (2) Signal strength and (3) Bit error rates, Pipeline Stages (PS) code and routines are written in C, C++ and with external subroutine interfaces written in Java. Each procedure has a defined interface (prototype) with arguments typically as a packet. Unlike most available vulnerability bulletins on public domains, we classify tactical wireless networks with vulnerabilities within the 14 different stages of a given tactical wireless RF communications transceiver. So, the vulnerabilities graph of a given tactical transceiver which may be classified as vulnerabilities in a 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 other 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.

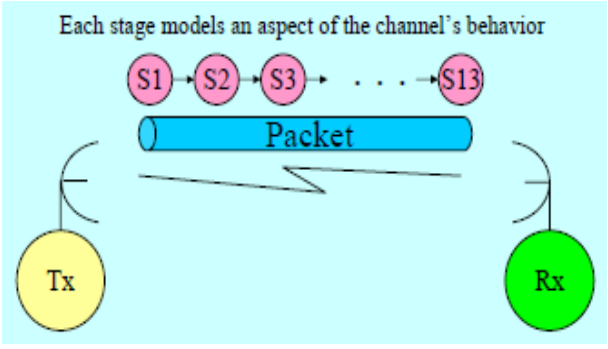

Figure 2. JCCS pipeline stages are defined for a wireless communication model

Using the existing JCSS tactical RF host's configuration and profile editors with wireless networking analysis tools [13] [14], we can construct generic vulnerabilities graphs and vulnerabilities templates, as in Fig. 3, to describe the possible exploitation of 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 information of the security metric(s). A successful JCSS simulation will lead to a better understanding for a more secure tactical RF communication model. Since we build vulnerabilities graphs using Bayesian networks (BN), we also assign the probability of success after a failure in a pipeline stage's link-edge weight.

Vulnerabilities
precond:
Radio Receiver:
(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
(Vr8) Error Correction
postcond:
(Vr1) Rx Antenna Gain = 0.75
(Vr2) Received Power = 0.65
(Vr3) Interference Noise = 0.85
(Vr4) Background Noise = 0.10
(Vr5) Signal-to-Noise Ratio = 0.90
(Vr6) Bit Error Rate = 0.25
(Vr7) Error Allocation = 0.35
(Vr8) Error Correction = 0.40

Figure 3. An example of a vulnerabilities template for JCSS (part of the transmitter / receiver pair) and related simulations.

Specifying the valid probability of communication in different stages requires expert knowledge of the domain. Most existing vulnerability scanning tools report 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 in more than one dimension a security or vulnerabilities matrix using this categorical information and quantify the levels of each category into numerical values for computation and comparison. Our approach is to make each matrix's 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 function $f(x + y) = f(x) + f(y)$ or a multiplicative function $f(ab) = f(a)\ f(b)$. Then, it can be converted to a value within the 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 a value may be represented as the probability of a given vulnerability with respect to the transceiver. For example, one can define a two dimensional m × n security matrix W = (wij), with one dimension wi to denote the severity levels, and another dimension wj to denote the 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 wij = wi × wj. 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 of the pre-conditions are met, the values of post-condition attributes are updated with an edge that is assigned with a weight. It is then added to the vulnerabilities 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 that we observe the fact that G has a status of W. There are two possible causes for this: either it is due to factor R or it is due to the fact that factor S is on. Which is more likely? We can use the Bayes' rule to compute the posterior probability of each explanation (where 0==false and 1==true).

Pr(W = 1) as a normalising 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 the variable elimination techniques illustrated below, and using the vulnerabilities graph in Fig. 4, we use Bayesian networks (BN) with Bucket Elimination Algorithm implementation in the models with belief-updating in our scenarios. We need to provide vulnerability values in each communication stage within each transceiver as well as the network scores on the entire tactical network. Finding a maximum probability assignment for each and the rest of the variables is a challenge. We may really need to find a maximising *a posteriori* hypothesis with given evidence values, finding an assignment to a subset of hypothesis variables that maximises their probability. On the other hand, we may need to maximise the expected utility of the problem with some evidence and utility function, finding a subset of decision variables that maximises the expected utility.

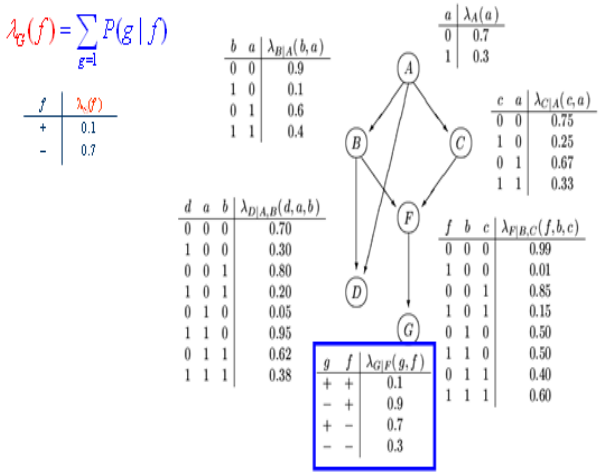

Figure 4. Use of Bucket Elimination Algorithm within a vulnerabilities graph

Another consideration is a Bucket Elimination Algorithm. This 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. This is based upon the Common Vulnerability Scoring System [22] and associates with additional features of Bayesian networks [17] (also known as belief networks) which in turn yields a more refined belief decision matrix. The matrix can then describe a multiple criteria decision analysis (MCDA) with an evidential reasoning approach for the vulnerability analysis of a given tactical wireless RF network.

7. Results from the Experiments

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

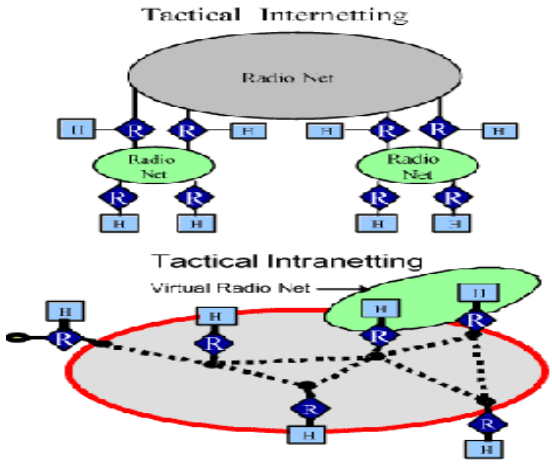

Figure 5a Wireless RF Networks

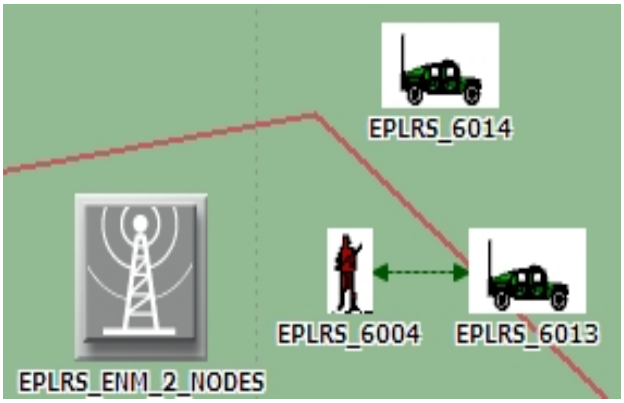

Figure 5b Two wireless nodes network

BEFORE:
Scenario IER Summary

Total IER Sent: 1999
Total IER Received: 1999
Total IER Failed: 0
Total IER Undelivered: 0
Total IER Perished: 0

AFTER:
Scenario IER Summary

Total IER Sent: 1999
Total IER Received: 1121
Total IER Failed: 878
Total IER Undelivered: 0
Total IER Perished: 0

Figure 5c Sample results generated by JCSS scenarios

8. Future

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 to wireless RF communications and computer networking science in tactical military applications. The research presented here is for the building of a set of "Bayesian network vulnerabilities graphs" for the study of vulnerabilities in tactical wireless RF networks. The

Bayesian network is designed as a vulnerabilities graph and models all of the 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 to attack within a tactical RF wireless communications network. Inference plays a major part in our vulnerability calculations. Future research work will involve looking at different kinds of Bayesian networks (BNs) with advanced topological arrangements that support multiple experts and multiple factors for the analysis of more advanced JCSS wireless RF vulnerabilities. We may consider an adapted Bayesian network of wireless tactical network analysis with a RF Vulnerability Scoring System (RF-VSS) that can generate weighted scores in the research. Based upon the Common Vulnerability Scoring System developed by Peter Mell et al. [22], we think that this is a very valuable, useful tool and a good 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 a "fixed" score, an "external variable" score and a "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 either 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 the System Remediation Level (SRL). This means that there exists a possible common defence fix out there, maybe from a contractor or a vendor or an emergency research workaround. If, when the detected vulnerability is first encountered, there is no possible fix, then the temporal or adversaries impact score will be much higher. However, when a solution or fix is possible, then the score will go down dramatically. Again, it was temporary and had a changing factor. There are three possible vulnerabilities metrics that make up the temporal or adversaries impact score. The base network score to produce a new score then multiplies this score. This first computed new score will be produced based upon the current operating wireless RF network scenarios set up via a 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 when deployed in the field. If the vulnerability has very little risk or else little to do with all the listed factors, then this computed score will be very, very low (such as zero). There are five metrics that affect the environmental impact score. This portion is combined with the base network and the 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, there will be little reason to worry. However, a higher score such as 6 or above might indicate major security issues. We will provide a vulnerabilities smart index by constructing a novel calculator with a set of RF Vulnerability Scoring System (RF-VSS) for the final system vulnerability analysis. For example, for a given wireless RF radio network, according to expert analysis and advice, there is a set of "RF wireless network vulnerabilities" assigned. The example metrics for the given wireless RF network scenarios with vulnerabilities are: (1) the base network impact, (2) the temporal or adversaries impact, and (3) the environmental impact. So, overall a base RF wireless networks vulnerability score of 8.8 (very bad) is slightly mitigated to 7.9 by the temporal or adversaries metrics. Still, 7.9 is not a great score and it suggests a considerable amount of risk. Now, this is where the final environmental impact score comes in to play so as 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 earlier for certain wireless network scenarios, as illustrated above. We gather all of those factors into the RF Vulnerability Scoring System (RF-VSS) calculator and it produces an environmental score of 6.5, which translates into a high vulnerability. This is a relatively good approach for determining what the overall risk is for a given wireless RF network, and the RF Vulnerability Scoring System (RF-VSS) analysis is based upon the Common Vulnerability Scoring System developed by Peter Mell [22] and associates, with additional features of Bayesian networks [17]. Using an adjacency-matrix as a starting point, a more manageable quantitative wireless RF network vulnerability assessment may be achieved.

9. Conclusions

A manageable framework is now partially achieved by providing a comprehensive network management and assessment methodology. Our study illustrates the use of a systems engineering approach; where Bayesian networks [17] can be applied during the analysis as a powerful tool for calculating security metrics with regard to 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 research into the development of security metrics by constructing

a novel calculator with a set of RF Vulnerability Scoring System for final system vulnerability analysis. We will continue to refine our approach using more dynamic Bayesian Networks in order to encompass the temporal domain measurements established in the CVSS. This paper demonstrates a management approach to modelling all of the 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 an Evidential Reasoning Approach [3] [4] [5] [6]. It was used to support various decision analyses and assessment and evaluation activities, such as impact and self-assessments [1] [2] based on a range of quality models. In decision theory, the evidential reasoning approach (ER) is generally an 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 an 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 analyses, 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 being 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 Modelling & Simulation Tool used to assess end-to-end communication network capabilities and performance. It is the Joint Chiefs of Staff's standard for modelling military communications systems. JCSS is a desktop software application that provides modelling and simulation capabilities for measuring and assessing the information flow through the strategic, operational, and tactical military communications networks. Our new tool can generate and implement vulnerabilities network graphs with linked edges and weights. All of these may be transposed into an adjacency-matrix, as illustrated earlier, 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. For given X, Y coordinates, for instance, they can be numbered from one to six and they may also be transposed into a 6x6 matrix. The vulnerabilities analysis with the help of system engineering approach [25] [26] [29] to a wireless RF network is then achieved by assigning corresponding measurement metrics with the 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, the bucket algorithm and related elimination steps which generalise looping and aggregated belief propagation and variation methods. A better approximate inference mechanism may be deployed in the near future for more complex vulnerabilities graphs. Our method is highly applicable to tactical wireless RF networks in picking and implementing each model's communication stages and states. The result, when used with OPNET JCSS [12] simulation and modelling, will provide both manageable graphical quantitative and real assessments of an RF network's vulnerabilities at a network topology state and during the time of actual deployment.

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] Kotov, V. "Systems-of-Systems as Communicating Structures," Hewlett Packard Computer Systems Laboratory Paper HPL-97-124, (1997), pp. 1–15.

[10] 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.

[11] Adamy, D. L. "EW103: Tactical Battlefield Communications Electronic Warfare", Artech House, ISBN-13: 978-1-59693-387-3, 2009.
[12] JCSS. The Joint Net-Centric Modeling & Simulation Tool. JCSS Project Manager, JCSS@disa.mil Commercial: (703) 681-2558..
[13] Chan P., U.S. Army, ARL patent (pending) - ARL Docket No. ARL 06-37. "Network Security and Vulnerability Modeling & Simulation Libraries".
[14] 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 Dijstrka Algorithm".
[15] Swiler, Phillips, Ellis and Chakerian, "Computer-attack graph generation tool," in Proceedings of the DARPA Information Survivability Conference & Exposition II (DISCEX'01), vol. 2.
[16] Yu, L. & Hong, M., "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).
[17] Leonard T. & Hsu J., "Bayesian Methods: An Analysis for Statisticians and Interdisciplinary Researchers," Cambridge University Press, ISBN 0-521-00414-4, 1997.
[18] Sheyner, Lippmann & Wing J., "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.
[19] Dijkstra E., Dijkstra's algorithm. Dutch scientist Dr. Edsger Dijkstra network algorithm. http://en.wikipedia.org/wiki/Dijkstra's_algorithm
[20] 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.
[21] 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.
[22] 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.
[23] Systems Engineering Fundamentals. Defense Acquisition University Press, 2001.
[24] Chan P., Mansouri M. & 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.
[25] Defense Acquisition Guidebook (2004). Chapter 4: Systems Engineering.
[26] 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)
[27] Bahill, T. & Dean, F. (2005). What Is Systems Engineering?
[28] Boehm, B. (2005). "Some Future Trends and Implications for Systems and Software Engineering Processes". In: Systems Engineering, Vol. 9, No. 1 (2006).
[29] Vasquez, J. (2003). Guide to the Systems Engineering Body of Knowledge – G2SEBoK, International Council on Systems Engineering.
[30] Chan P., Mansouri M. and Hong M., "System Engineering Approach Tactical Wireless RF Network Analysis with Vulnerability Assessment using Bayesian Networks", International Journal of Simulation Systems, Science & Technology, Vol 11, No.6 (2010), Page 67-75
[31] Cogan B., Chan P, et al. Journal of "Systems Engineering – Practice and Theory", InTech Press, ISBN-13: 979-953-307-410-7, 2011.