Modeling security of power communication systems using defense graphs and influence diagrams

Teodor Sommestad
Mathias Ekstedt
Lars Nordström

Royal Institute of Technology,
Osquldas väg 12,
100 44 Stockholm,
Sweden

The purpose of this paper is to present a framework for assessing the security of wide area networks used to operate electrical power systems. The framework is based on the formalism influence diagrams and the concept of defense graphs and facilitates so called consequence based analysis of the security problem. The framework is also capable of managing uncertainties, both related to the efficacy of countermeasures and the actual posture of the SCADA system. A model over wide area network attacks and countermeasures and experiences from applying the framework are described.

1 Introduction

The importance of IT security is increasing in enterprises today. This is especially the case for organizations using IT to operate power systems since power production and delivery is a cornerstone of society's critical infrastructure. The cyber security of SCADA systems used in electric power distribution is thus an important issue that needs careful management. Securing SCADA systems used in power transmission and distribution is however difficult. SCADA systems often, for instance, comprise of a great number of heterogeneous components with varying age and criticality. They are today also significantly interconnected to a great number of other information systems that all need to be understood and perhaps managed to ensure the security of the SCADA system. Another characteristic property of SCADA systems for the power systems is that they are dispersed over large geographical areas [1]. This fact introduces a number of vulnerabilities in the SCADA systems design that needs to be carefully considered and specifically managed.

The wide-area networks (WAN) used by SCADA systems are large geographically widespread systems that connect the control center with substations and mediate messages between these. In this context decision-makers in the power industry are faced with difficult decisions where the benefits of investments, in security measures have to be compared to their costs. This tradeoff analysis is even more important when it comes to investments in large and complex infrastructures such as WANs used by SCADA systems.

For the decision maker there is however uncertainty involved when the cyber security of WANs in SCADA systems is assessed. Firstly, there is an uncertainty regarding how to achieve security and what solutions that is effective in mitigating threats. Recommendations and standards, such as ISO/IEC 17799 [2], describe how to achieve security, but these do not explain the level of cyber security achieved when there are deviations from the standard. Nor do they specify the level of assurance that threats are mitigated with the suggested technologies. Secondly, decision makers often face uncertainty regarding the details of technologies and configurations of employed communication architectures. WANs are large and complex and there might for instance be an uncertainty regarding the existing physical protection of communication or if security functionalities of the protocol are applied or not.

1.1 Scope of the paper

The paper presents a generic method to determine a level, or value, of cyber security that support decision makers striving to improve cyber security levels for SCADA WANs. The applied method is based on [3] and utilizes the formalism influence diagrams to set up the security problem and to infer a value of security. Influence diagrams are based on Bayesian mathematics and are capable of probabilistically deal with the uncertainty present in the security assessments.

In short, the method decomposes plausible attacks against SCADA WANs and models these together with the countermeasures mitigating them. This structure is called a defense graph. Based on probabilistic relationships between the modeled factors, and the indicators collected during an assessment, the probability that an attack will succeed can be inferred. In addition, it is shown how consequences can be incorporated into the model and how this can be used to perform consequence based analysis. The method has been tested and empirically refined in collaboration with a power distribution system operator.

A method based for coping with the uncertainty related to data collected during cyber security assessments using Dempster-Shafer theory has previously been presented in [4]. This paper is a continuation of that previous work.

1.2 Outline of the paper

The outline of this paper is as follows. In chapter two related work within attack and defense graphs together with the formalism influence diagrams are described. Chapter three describes how defense graphs can be modeled using influence diagrams and in the fourth chapter the defense graph over a typical SCADA WANs is presented. Chapter five presents how the proposed framework can be used for security analysis and experiences from a security assessment where the framework has been applied is described. Finally, in chapter six, conclusions are drawn.

2 RELATED WORK

Within the field of security, a large number of initiatives have resulted in practical guides for how to achieve security, examples of these are NIST SP 800-82 [1] and ISO 17799 [2]. Within the field of WAN security, IEC TC 57 has published a technical report [5] describing how security can be managed within the domain of power system control and associated communications. This report promotes a methodology where the negative consequences of successful attacks are taken into consideration when security is managed. Together with analysis of the threats, activities and events that lead to consequences, a suitable way to distribute security efforts can thereby be derived.

Attack trees [6][7][8][9] (sometimes called threat trees) is an approach used to decompose the steps and obstacles an attacker has to perform to breach a system and to reason about this in a structured manner. Attack trees are similar to fault trees. The attacker's main goal is depicted as the root of the tree and the steps to reach this goal are broken down into sub-goals of the attack through "AND" and "OR" relationships.

Several approaches to analyze security using attack trees and attack graphs have been proposed, see for example [10][11][12][13][14] and [15]. Methods using attack trees also include the work Liu and Hong [16], who have used Bayesian networks to calculate the probability of an attack against computer networks being successful based on vulnerabilities within it. Liu and Hong's approach can be used to assess the security posture and compare it to previous postures. The approach does however not include controllable concepts or describe how a security posture can be improved.

Decision makers can typically influence the difficulty to perform attacks through implementation of countermeasures. Consequently, a natural extension of attack graphs is to include these controllable countermeasures in the graph. In both [17][8] countermeasures are modeled together with trees depicting threats and attacks. The idea of including countermeasures in the tree structure has also been embraced in [18], and are there called defense trees. Techniques has been presented which use defense trees for strategic evaluation of security investments [18], modeling strategic games in security [19], as well as modeling of conditional preference of defense techniques using conditional preference nets [20].

However, even if the possible ways an attack can be accomplished is identified, it is difficult to answer if an attack will be successful or not given a set of countermeasures. As stated in [21], there is no algebra for perimeter security. Moreover, the time and effort required for a thorough survey identifying and assuring the status of all the factors influencing the difficulty of attacks is rarely available and security analyzes will often have to be based on incomplete and unverified data. Especially this is the case when systems are large and complex, such as distributed control systems for the power process.

Bayesian networks are a formalism well equipped for combining disparate concepts and managing the uncertainty present in security assessments. In [3] the Bayesian network variation extended influence diagrams are suggested to be used for expressing defense graphs. This paper has applied that approach using influence diagrams to the domain of SCADA WANs.

3 EXPRESSING DEFENSE GRAPHS WITH INFLUENCE DIAGRAMS

In the field of security there is, as discussed above, an uncertainty regarding both if some particular countermeasure mitigates an attack, and the exact properties and configurations of the employed system architecture. Influence diagrams [22][23] are graphic representations of decision problems coupled with a probabilistic inference engine, and is therefore well equipped for expressing uncertainties. These diagrams are an enhancement of Bayesian networks and have been applied in a wide range of domains, including the security domain (see for example [24]).

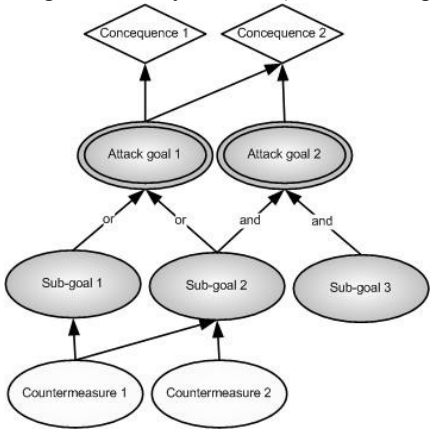

Figure 1 – Defense expressed through influence diagrams notation.

Influence diagrams can be used to express defense graphs [3]. The goal and sub-goals of an attack can be illustrated by chance nodes with the states "success" and "failure". Where "success" means that the goal is possible for the adversary to reach and "failure" mean that the adversary cannot reach this goal. The AND-relationships and OR-relationships in the attack graph can be expressed using deterministic nodes and specified through conditional probability tables. Moreover, the consequences of a successful attack can be taken into consideration and expressed through utility nodes (cf. Figure 1).

In the utility nodes, each configuration of states in the parent nodes is associated with a utility, representing the loss of a successful attack. In the example described in Figure 1, the utility of "Consequence 1" would have a loss associated with the state "success" and "failure" of "Attack Goal 1". Correspondingly, "Consequence 2" would have a negative utility associated with all combinations of "success" and "failure" of "Attack Goal 1" and "Attack Goal 2". Given the utilities of successful attacks, the expected consequence from an attack can be calculated as a

weighted average from the probabilities that attack goals will be reached.

The probability that an attack goal, *A,* can be reached through an OR-relationship of sub-goal S_1 to S_n can be defined as: $P(A=Success \mid S_i=Success) = 1$, where S_i is any of S_1 to S_n. Otherwise $P(A=Success) = 0$.

The conditional probability for the AND-relationship for an attack goal *A,* with sub-goals S_1 to S_n can be defined as: $P(A=success \mid S_i=Failure) = 0$, where S_i is any of S_1 to S_n. Otherwise $P(A=Success) = 1$

The probability that a particular type of adversary, with certain capability and resources, succeed in reaching the goals in the attack graph is dependent on the countermeasures that are in place. To include countermeasures into the model, arcs are drawn between the countermeasures and the sub-goals they influence the difficulty of. In addition to this graphical description (cf. Figure 1), the impact of different states of countermeasures of the difficulty of achieving influenced sub-goals is also described through conditional probability tables.

If *S* is a sub-goal of an attack and C_1 to C_n is countermeasures which influence the difficulty of reaching the sub-goal. Then the conditional probability $P(S=Success| C_1, .., C_n)$ expresses the probability that S will succeed given the state of C_1 to C_n.

4 A DEFENSE TREE FOR A SCADA WAN

In a joint project with one of Sweden's larger distribution system operators defense graphs over WAN security has been specified, applied and validated. The defense graph is depicted in Appendix A. Its components are described below.

4.1 Attacker goals

Attacks on SCADA WAN may be motivated with financial gain, terrorism, vandalism or more. The means an adversary can use to reach these goals are to exploit or destroy services provided by the SCADA WAN. Based on literature and interviews with system suppliers and system operators the following attacker goals have been identified as relevant for substation communication:

- Eavesdropping messages
- Traffic analysis
- Manipulate control messages
- Manipulate status messages
- Reconfigure field devices
- Disrupt messaging

These attack goals are further described below.

Eavesdropping of messages sent from and to substations is one possible goal of attackers [1][25][26]. Since the confidentiality of this kind of data is not typically an issue, the direct consequence of such an attack is limited. It can however be an important part of other goals, for instance if messages are later replayed in the networks or if they contain device passwords.

Traffic analysis does as eavesdropping involve listening to messages sent within the WAN [26]. The difference is that traffic analysis is only concerned with finding information about traffic patterns with the network [27]. It might for instance be enough to investigate the headers of messages.

By *manipulating control messages* and send these to controllers or actuators within the substation attackers can take control of the power grid [26] [28][29]. In a similar manner, an attacker may *manipulate status messages* sent from the process with status indications or measurements [26] [28][29]. To accomplish this attackers can either [25]: intercept and replay previously sent messages; intercept messages and modify them; or inject new messages in the network. Since a successful attack of this kind would enable the attacker to force the equipment into an insecure state the consequences can be severe.

Manipulation of messages can also be used to compromise equipment configurations [26] [28][29]. The behavior of field devices is decided by its configuration and has an impact on the SCADA system functionality. An adversary who manages to *reconfigure field devi*ces might for example change set points, alter alarm levels or even disable control and protection functionality.

A perhaps easier way to hide events and status of the power system than to manipulate status messages is to *disrupt messages* from reaching its intended destination through a denial of service attack [26] [28] [29]. A simple way of accomplishing this is to physically disconnecting systems. Three other ways are to [1]: exploit a software vulnerability which makes it crash; overload a device with messages to stall it; or pollute the network with messages. This kind of attack can also be used to hinder automated controllers and operators to control the power process.

4.2 Countermeasures

A defense graph describing the relationship between the attack goals, their sub-goals, and countermeasures is depicted in Appendix A. Typically, a number of steps have to be successfully completed for the adversaries to reach their goals. For example, to be able to repeat messages sent within the network the adversary have to first achieve network connectivity; then a message needs to be successfully intercepted; and finally the message must not lose validity before it is replayed, otherwise it will most certainly be disregarded. Countermeasures that can be used against this replay attack include physical protection and static addresses within the network to prevent connectivity to be gained; a communication medium with good protection and a network topology that makes message interception difficult; and timestamps or message sequence numbers to keep track of outdated messages.

A similar way to produce manipulated messages would be to not only intercept and replay them, but also change the content of them. This would require the adversary to understand the structure of the message and reconstruct a possible checksum, but it would on the other hand make it possible to modify timestamps and sequence numbers. Countermeasures against modification of messages include encryption to make them difficult to understand and reproduce, and message signatures for detection of unauthorized modifications.

The injection of completely new messages is just as modification of messages made more difficult when messdafe signatures are used. Injection of messages does however differ from modification since eavesdropping is not prerequisite. However, if plaintext passwords are used to validate messages eavesdropping to these can be a step on the way.

System designers can chose among many countermeasures to make attacks more difficult. A list of preventive countermeasures identified as relevant to the abovementioned attacks is shown in TABLE 1.

TABLE 1 – Countermeasure mitigating attacks through communication links

Physical protection	The physical protection of RTUs and communication links is an important component for substation security [25]. To gain some degree of physical connection is a prerequisite for any attack.
Medium type	The type of medium used is related to the physical security and also of relevance. A ranking of risks associated with different mediums can be found in [25].
Address locking	By locking the addresses on network, such as MAC-addresses in ARP tables, a barrier against unauthorized access is enforced. This adds another level of security to but is not in itself attacker proof [1].
Message sequence numbering	By keeping track of received messages numbering replayed messages can then be disregarded based on their sequence number.[25] [26][29]
Message timestamps	Timestamps can, as sequence numbers, be used to mitigate replay attacks. Provided that a maximum time a message takes to reach its destination is known, all messages older than this time can be disregarded. [25][29]
Message signatures	An effective countermeasure against message modification and injection is signatures. A key is used to encrypt the message checksum and based on this the recipient can validate the creator of the message. [1][26][29]
Clear-text passwords	By authenticating access to devices with passwords some protection is provided. This would force attackers to identify the password before they can gain access, something which can be done by eavesdropping messages containing passwords [1].
Message encryption	To protect messages from being eavesdropped the entire message may be obfuscated for unauthorized users through encryption [1][26]
Random message delays	Some obscurity can be added to the traffic flow in a network if random message delays are employed as it makes response times more difficult to analyze [27].
Link padding	Another mechanism that makes traffic analysis more difficult is to pad the payload traffic with dummy messages [32].
Redundant communication links	Redundant communication links is a measure that increases resilience against disconnected communication links or overloaded network segments [1].

4.3 Validation and quantification

The creation of an influence diagram does, like the creation of a Bayesian network comprise two parts: one qualitative part where the structure of the diagram is determined and one quantitative part where the relationships are specified through conditional probability tables. The influence diagram depicted in Appendix A has been developed together with two system suppliers and one system owner.

The conditional probability tables have been specified for the relationship among variables. For the defined "AND" and "OR" relationships this has been done deterministically as illustrated in Figure 1 and described in section III. Non-deterministic relationships are on the other hand to be specified probabilistically. An example is shown in TABLE 2.

This table describe the probability that an adversary can construct a new valid message and how this depend on whether clear-text passwords are used, cryptographic signatures are used, and if messages can be eavesdropped. This table does for example express that the combination of clear-text passwords and communication that can be eavesdropped will not hinder successful attacks. Nor will communication that lack both cryptographic signatures and clear-text passwords.

Notable here is the uncertainty regarding the efficacy of cryptographic signatures and passwords, and that their existence is not believed to provide absolute security. Possible weaknesses in key management, software implementations or the algorithms as such introduce some uncertainty leave some room for successful attacks although these technologies are uses.

TABLE 2 – CONDITIONAL PROBABILITY TABLE FOR CREATING NEW VALID MESSAGE

Use of clear-text passwords	T				F			
Use of cryptographic signatures	T		F		T		F	
Eavesdrop messages	T	F	T	F	T	F	T	F
Success	0.01	0.005	1	0.005	0.01	0.005	1	1
Failure	0.99	0.995	0	0.995	0.99	0.995	0	0

Another example is given in TABLE 3 which describes the probability that message content can be understood by the attacker. A protection mechanism that makes this difficult for adversaries is message encryption. TABLE 3 specifies that without encryption message content will surely be understood, but with encryption this is most unlikely.

TABLE 3 – CONDITIONAL PROBABILITY TABLE FOR INTERPRETING MESSAGE CONTENT

Encryption used	True	False
Success	0.01	1.00
Failure	0.99	0.00

In the same format, conditional probabilities were specified for ten variables that are targeted through causal arcs. Furthermore, beliefs on the prior state of countermeasures have been specified.

4.4 Accounting for empirical uncertainty

Empirical uncertainty, i.e. uncertainty regarding related to data collected in an assessment, is present in most types of assessments. Firstly, security assessments usually cannot cover all the variables of importance, but must instead focus on those of highest relevance. Additionally, there is typically uncertainty arising from lack of accuracy and credibility in the collected data. As an example, information about the systems security posture could be collected by asking people or consulting system documentation. Both these sources provide indications on the state of attributes that are related to security. However, just as any test these indicators can be wrong. There can for example be an uncertainty regarding the accuracy of a one year old design specification, or uncertainty regarding the credibility of answers from a system engineer. Indicators provided by different sources can also be conflicting.

Influence diagrams offer support for expressing the uncertainty and credibility associated with different indicators at to account for this in the result of the security assessment. For a more extensive elaboration on heuristics for credibility of gathered data see [31].

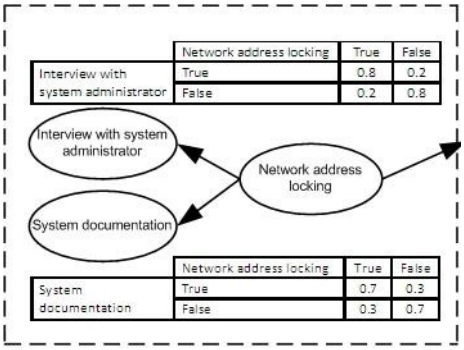

Figure 2 - Indications on the state in network address locking and the conditional probability tables expressing each test's significance.

Figure 2 depicts the two pieces of indicators on the use of static network addresses: a) an interview with the system administrator and b) the systems documentation. These two indicators will both provide information on how likely the network is to be configured to have static network addresses. What the answer of a network administrator will be, is influenced by whether static addresses are actually used or not; and the descriptions of documentation is likewise believed to be influenced by the system's actual network configuration. Associated with these two indicators are probability distributions describing the outcome of the indicator provided a state of the assessed attribute. In Figure 2, conditional probability tables describing this probability distribution are depicted.

The table related to the system administrator's answer states that given that network address locking is being used, the system administrator will answer that it does with 80 percents probability representing potential ignorance or misconfiguration. With 20 percents probability the system administrator will answer true also if network address locking is not used. Hence, there is some uncertainty regarding the accuracy of the system administrator's answer. Similarly there is an uncertainty regarding the accuracy of documentation. This is however believed to have a credibility of only 0.7. Indicators may also have an unsymmetrical probability distribution. For example, if an internet search is performed to identify if a protocol specification is publically available a hit will provide complete evidence on this. However, if nothing is found this is not a guarantee for that specifications are kept confidential. This type of asymmetry can also be expressed using the method described here.

Generally described the states of indicative attributes can be used to infer a belief on the state of an assessed attribute. Consider the indicators on Network address locking depicted in Figure 2. This figure describes how a probability on the use network address locking (*Nal*) can be attained from an interview with the system administrator (*Adm*) and from the system's documentation (*Doc*). Given the prior probability *P(Nal)* of the use of network address locking and the observations Doc_o and Adm_o, the likelihood $L(Nal| Doc_o , Adm_o)$ can be obtained using the formula: $L(Nal| Doc_o , Adm_o) = P(Doc_o| Nal) P(Adm_o| Nal)$. Given this, and the prior probability *P(Nal)*, the posterior probability, $P(Nal| Doc_o , Adm_o)$, can be calculated as: $k*P(Nal)* L(Nal| Doc_o , Adm_o)$, where *k* is a normalizing constant.

In a similar way results from intrusion attempts, such as penetration tests, can be used to assess the likelihood that certain attack goals are reachable. For example, a successful eavesdropping attempt will provide a strong indicator of the possibility to succeed with eavesdropping attacks. This in turn would be an indirect indication that would provide information about likely state of security attributes. It would for instance make it more likely that no encryption is used in the protocol.

5 Consequence based analysis under uncertainty

For confidentiality reasons the actual results from the study cannot be published. Instead, we here present a fictive example to demonstrate how the framework can be applied for security assessments using consequence based analysis.

5.1 Describing the assessed communication links

In our example assessment, two communication links (A and B) are assessed. Both of these are links within the control network and between substations and the control center. Link A uses an implementation of the IEC 60870-5-104 protocol and link B uses a proprietary developed, but openly available, protocol.

According to the indicators gathered, it is not clear whether link A uses a leased line or power line carrier as its medium since two conflicting pieces of indicators exists (cf. TABLE 4). The indicator on Link A says that it neither uses cryptographic signatures nor network address locking. Timestamps is however used and regardless of medium, the asset management system tells us that the link is physically protected. It is too close to the power lines to be tampered with. Furthermore, given that the system specification is correct about the use of IEC 60870-5-104, we know that message sequence numbers is used since this is a part of the standard specification [33].

TABLE 4 – Countermeasure Indicators for communication links A and B in the assessment (Indicators are provided by Different Sources: A – Administrator, D –Documentation, I – Internet search, G – Geographical Information System)

Variable	Link A	Link B
Message encryption	A=False	A=False
Medium type	A=Leased line D=PLC	A=Private line D= Private line
Protocol description publically available	I =True	I =True
Cryptographic signatures	D=False	D=F
Device password	-	D=T
Message sequence numbers	D=True	D=T
Address locking	A=False D=False	A=True D=True
Physical protection	G=True	G=True

Communication link B has corroborative indicators on the use of a private communication line as both the administrator and system documentation state so. In our example, an internet search identified the protocol specification and from documentation information on the use of cryptographic signatures and clear-text passwords was collected. For this link, both the administrator and the system's documentation described that network address locking was used. From the system protocol specification, an indication on the use of message sequence numbers was obtained, and based on data from the geographical information system it seems as the communication wires are protected physically.

Also assessed was the consequence of successful attacks for the system owner. This was done on a scale from zero to four, inspired by the severity rating in [34]. Since the two links was used for different purposes, and was used to control a different amount of substations, the consequences of successful attacks on them differed somewhat. The rating of consequences for the two links can be found in

TABLE 5

TABLE 5 – ATTACK CONSEQUENCES FOR LINK A AND B

Attack	Link A	Link B
Eavesdrop	**1**	**1**
Manipulate status messages	**3**	**2**
Manipulate control messages	**3**	**2**
Reconfigure field devices	**3**	**2**
Perform traffic analysis	**0**	**0**
Disrupt messaging	**1**	**1**

5.2 Results

The assessment of the two links include uncertainty related to data collected during the assessment and the defense tree holds some uncertainties regarding what attacks that are possible to accomplish. However, albeit this uncertainty, probabilities for attacks succeeding can be inferred and consequence based reasoning can be applied. Figure 3 describes the assessment result from Link A and Link B.

The ellipses in Figure 3 state the probability that attacks will succeed against the communication links; and rhombs state the expected consequences of attack attempts. From these numbers, and by tracing the numbers back to countermeasures, decisions makers can make informed decisions regarding the security of the WANs.

Given the collected indicators and the theory captured in the influence diagram it does for example seem as link A is the weaker one. For this link both traffic analysis and disrupting messaging can be accomplished with high probability. Although disrupted messaging is not regarded as severe, the high probability of an attack succeeding yields the highest expected attack consequence of all plausible attacks. It would thus seem reasonable to spend resources on security improvements on this link. A closer examination of the influence diagram will show that the most efficient countermeasure is to introduce redundancy in the WAN to better withstand attacks that attempt to disrupt messaging.

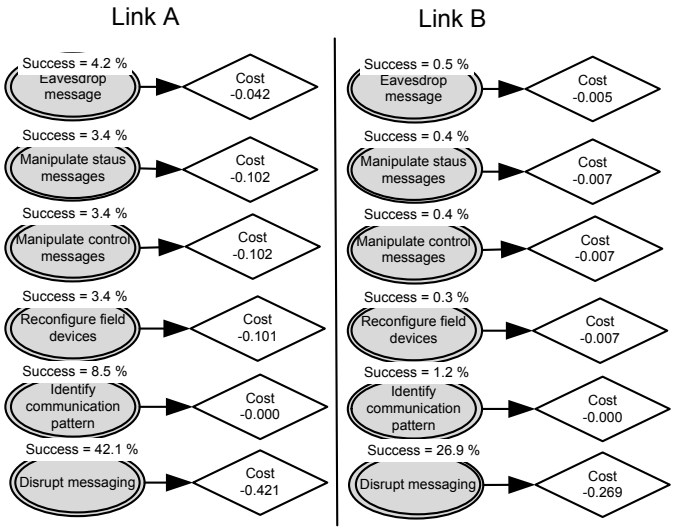

Figure 3 – Results from the security assessment of link A and B. Ellipses show the attack goals and the probability that they can be reached; rhomb shaped utility nodes display the expected losses associated with each attack attempt.

6 CONCLUSIONS

When evaluating the security of today's SCADA communication solutions, decision makers are faced with a great deal of uncertainty. The experience from applying the framework to assess the security of a power distributors WAN is that the consequence based methodology highlighted several areas in which improvements were critical. The possibility to take both empirical and theoretical uncertainty into account when assessing security in the assessment was also experienced as a convenient feature. This made it possible to quantitatively assess the security without a complete and thorough survey of the system architecture, or exact knowledge of what countermeasures that mitigate attacks.

7 REFERENCES

[1] Stouffer, K., J. Falco, and K. Scarfone, *Guide to Industrial Control Systems (ICS) security.* Technical Report Special Publication 800-82, NIST, 2007.

[2] ISO/IEC 17799, 2000 ISO/IEC 17799, Information technology – code of practice for information security management, International Organization for Standardization (ISO), Switzerland (2000)

[3] T. Sommestad, M. Ekstedt, P. Johnson, Combining defense graphs and enterprise architecture models for security analysis, Proceedings of the 12th IEEE International Enterprise Computing Conference, September 2008

[4] L. Nordström, Assessment of Information Security Levels in Power Communication Systems Using Evidential Reasoning, Volume: 23, Issue: 3, pp 1384-1391, 2008.

[5] IEC 62210, Power control and associated communications – Data and communications security, 2003

[6] S. E. Schechter. Computer Security Strength & Risk: A Quantitative Approach. PhD thesis, Harvard University, 2004.

[7] B. Schneier. Attack trees: Modeling security threats. Dr. Dobb's Journal, 1999.

[8] N. L. Foster. The application of software and safety engineering techniques to security protocol development. PhD thesis, Univ. of York, Dep. Of Computer Science, 2002.

[9] W.J. Caelli, D. Longley, and A.B. Tickle. A methodology for describing information and physical security architectures. Proceedings of the IFIP TC11, Eigth International Conference on Information Security, IFIP/Sec '92, volume A-15 of IFIP Transactions, pages 277–296. Elsevier, May 27–29, 1992.

[10] P. Ammann, J. Pamula, R. Ritchey, and J. Street. A host-based approach to network attack chaining analysis. In Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC '05), pages 72–84, Tucson, AZ, December 2005.

[11] P. Ammann, D. Wijesekera, and S. Kaushik. Scalable graph-based vulnerability analysis. In Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02), pages 217–224, Washington, DC, November 2002.
[12] S. Jha, O. Sheyner, and J. Wing. Two formal analyses of attack graphs. In Proc. of the 15th Computer Security Foundation Workshop, June 2002.
[13] O. Sheyner "Scenario Graphs and Attack Graphs," Carnegie Mellon University, April 2004. PhD Thesis.
[14] O. Sheyner and J.M. Wing, "Tools for Generating and Analyzing Attack Graphs," Proceedings of Workshop on Formal Methods for Components and Objects, 2004, pp. 344-371.
[15] Philips, C., Swiler, L.P, Graph-Based System for Network-Vulnerability Analysis, Proceedings of the 1998 workshop on New security paradigms, 1998.
[16] Y. Liu and M. Hong, Network vulnerability assessment using Bayesian networks, Proceedings of Data Mining, Intrusion detection, Information assurance and Data networks security, Orlando, Florida, USA, 2005, pp
[17] M. Howard and D. C. LeBlanc. Writing Secure Code, Microsoft Press, Redmond, WA, USA, 2002.
[18] S. Bistarelli, F. Fioravanti, P. Peretti, Defense trees for economic evaluation of security investments, Proceedings of Availability, Reliability and Security (ARES), Vienna, Austria, 2006, pp. 8.
[19] S. Bistarelli, M. Dall'Aglio, P. Peretti, "Strategic games on defense trees", Formal Aspects in Security and Trust, Springer Berlin / Heidelberg, 2007, pp. 1-15.
[20] S. Bistarelli, F. Fioravanti, P. Peretti, Using CP-nets as a Guide for Countermeasure Selection, Proceedings of the 2007 ACM symposium on Applied computing, Seoul, Korea, 2007, pp. 300-304.
[21] R. Vaughn, R. Henning, and A. Siraj, Information assurance Measures and Metrics: State of Practice and Proposed Taxonomy. Proceedings of 36th Hawaiian International Conference on System Sciences, 2003, pp. 331-334.
[22] R. Shachter, Evaluating influence diagrams. Operations Research, 34(6), Institute for Operations Research and the Management Sciences, Hanover Maryland, 1986, pp. 871-882.
[23] R.A Howard, J.E. Matheson, influence diagrams. Decision Analysis, 2(3), Institute for Operations Research and the Management Sciences, Hanover Maryland, 2005, pp. 127–143.
[24] K. J. S. Hoo. How much is enough: a risk management approach to computer security. In Workshop on Economic and Information Security, 2002.
[25] Igure, V., Laughter, S., Williams, R., "*Security Issues in SCADA networks"*, Computers and Security, Volume 25, Issue 7, 2006, pp 498-506.
[26] Melton, R., Fletcher, T., Earley, M., "System Protection Profile – Industrial Control Systems", Version 1.0, National Institute of Standards and Technology, Gaithersburg, Maryland, April, 2004
[27] Fu, X., Graham, B., Bettati, R., Zhao, W.,*"Active Traffic Analysis Attacks and Countermeasures",* Proceedings of the International Conference on Computer Networks and Mobile Computing, 2003, pp. 31- 39.
[28] Krutz, R.,"*Securing SCADA Systems*", Wiley Publishing, Indianapolis, Indiana, 2006.
[29] Dzung, D., Naedele, M., Von Hoff, T., Crevatin, M.,"Security for Industrial Communication Systems", Proceedings of the IEEE, Volume 93, Issue 6, 2005, pp. 1152-1177
[30] Naedele, M., Dzung, D., Stanimirov, M.,*"Network Security for Substation Automation System",* Computer Safety, Reliability and Security, Springer Berlin / Heidelberg, 2001.
[31] E. Johansson, Assessment of Enterprise Information Security – How to make it credible and efficient, PhD thesis, Royal Institute of Technology (KTH), 2005.
[32] Bettati, R., Fu, X., Graham, B., Zhao, W.,"*On effectiveness of link padding for statistical traffic analysis attacks."* Proceedings of the 23rd International Conference on Distributed Computing Systems, 2003.
[33] IEC 60870-5-104, Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles, CEI/IEC 60870-5-104:2000.
[34] R.K. Fink, D.F. Spencer, R.A. Wells, INL Lessons learned from cyber security assessments of SCADA energy and energy management systems, INL/CON-06-11655, September 2006,

8 APPENDIX A

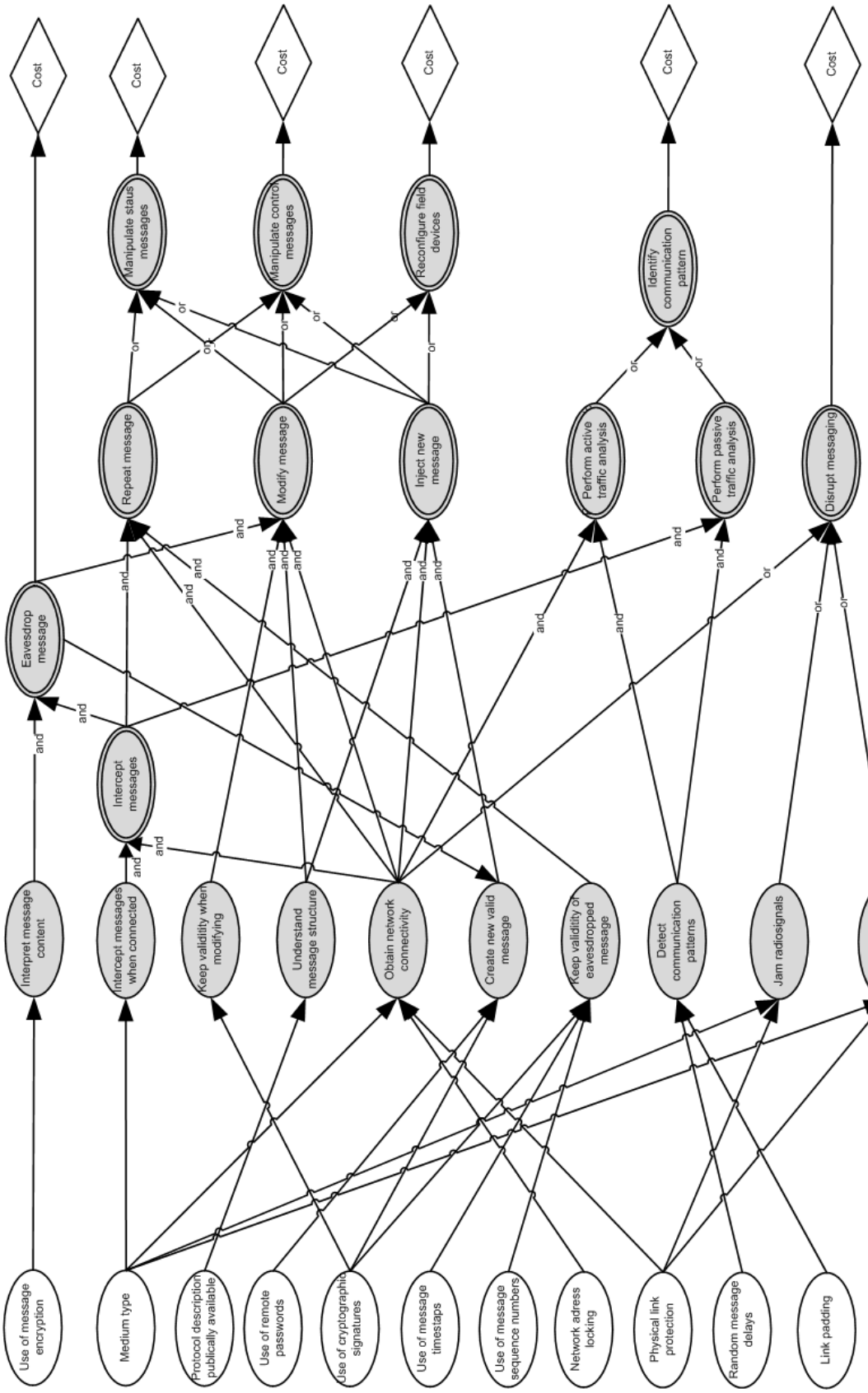

Figure 4 - Defense graph over substation communication. Diamond shaped nodes denote utility nodes associated with negative values of attacks. Grey elliptic nodes depict the attack graph and the goals and sub-goals of attackers. White elliptic nodes depict the countermeasures influencing the difficulty of attacks