Application System Security Compliance to FISMA Standard

Elaine Hulitt

April 23, 2009

Outline

- Information system security
- Federal Information Security Management Act (FISMA)
- Pathfinder Networks (PFNETs)
- FISMA Compliance measurement using PFNETs – an example

Information System Security

- The Problem
- Security Standards
- FISMA

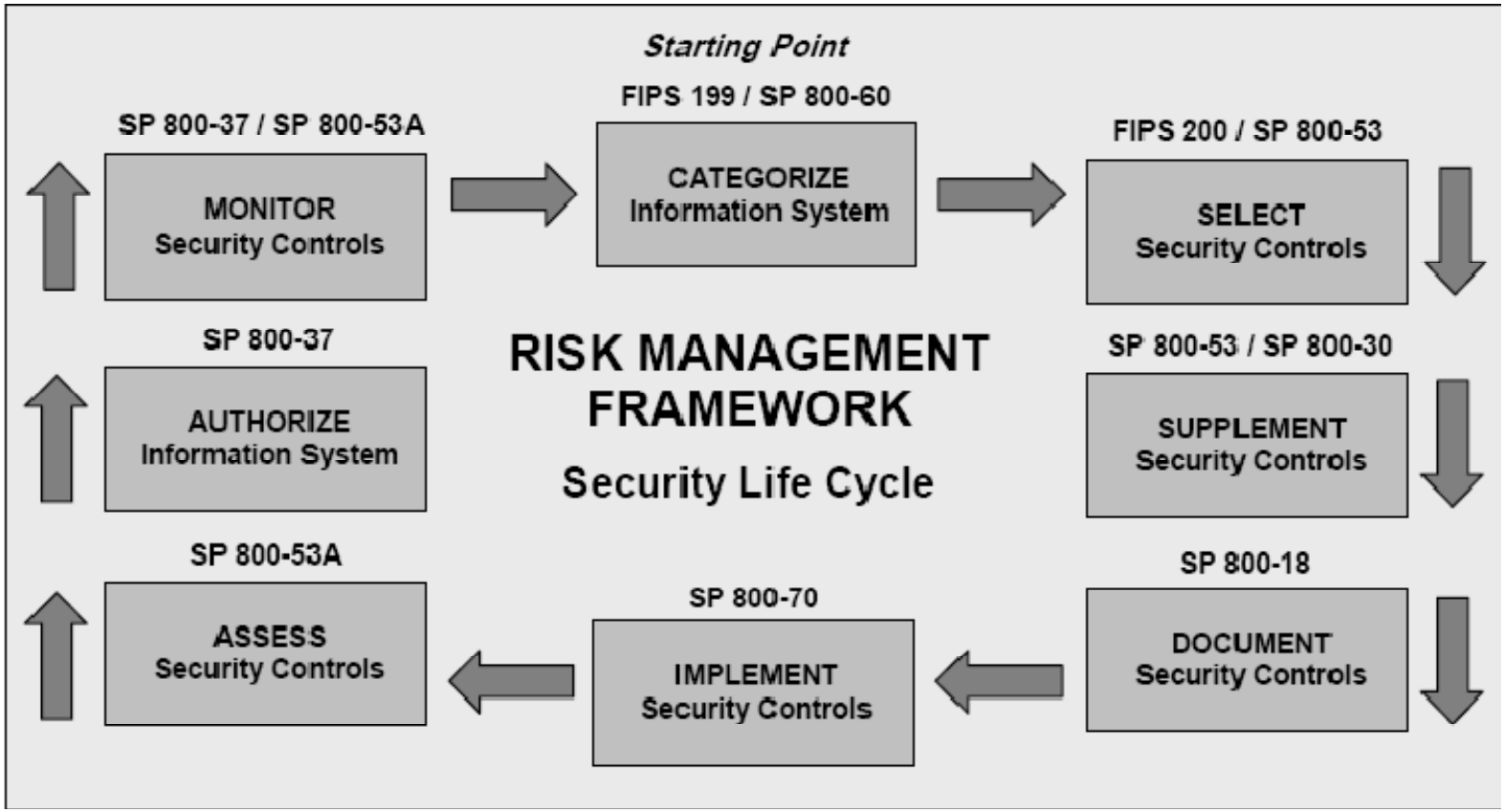
Outline

- Information system security
- Federal Information Security Management Act (FISMA)
- Pathfinder Networks (PFNETs)
- FISMA compliance measurement using Pathfinder – an example

Federal Information Security Management Act (FISMA)

- Enacted into law December 17, 2002
- Requires definition of:
  - Information system categories
  - Guidelines for types of systems to be included in each category
  - Minimum security requirement (controls) for each category
- Tasked NIST to implement requirements

NIST Risk Management Framework (RMF)



FIPS 200/SP 800-53
Minimum Security Control Required

Identifier	Family	Class
AC	Access Control	Technical
CA	Certification Accreditation and Security Assessments	Management
:	:	:
:	:	:
SI	System and Information Integrity	Operational

CNTL No.	Control Name	Control Baselines		
		Low	Mod	High
Access Control				
AC-1	Access Control Policy and Procedure	AC-1	AC-1	AC-1
AC-2	**Account Management**	AC-2	AC-2(1)(2)(3)(4)	AC-2(1)(2)(3)(4)
:	:	:	:	:
:	:	:	:	:
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20(1)

AC-2 Account Management

Control: The organization manages information system accounts, including establishing, activating, modifying, retrieving, disabling, and removing accounts. The organization reviews information system accounts …

Supplemental Guidance: *description…*

Control Enhancements: *description…*

(1) *description…*
(2) *description…*
(3) *description…*
(4) *description…*

Outline

- Information system security
- Federal Information Security Management Act (FISMA)
- Pathfinder Networks (PFNETs)
- FISMA compliance measurement using Pathfinder – an example

What Is Pathfinder

- Set of algorithms – Dearholt and Schvaneveldt (1981)
- Network models of proximity data – asymmetric or symmetric
- Structure determined by entity relationships, the *r*-metric and *q*
- Mathematical model of subjective data

Pathfinder Network (PFNET) Generation

- Correlate Entities
- Build Similarity Matrix
- Build Dissimilarity Matrix
- Build Pathfinder Network
- Build Minimum Distance Matrix
- Compare Stakeholder Perceptions

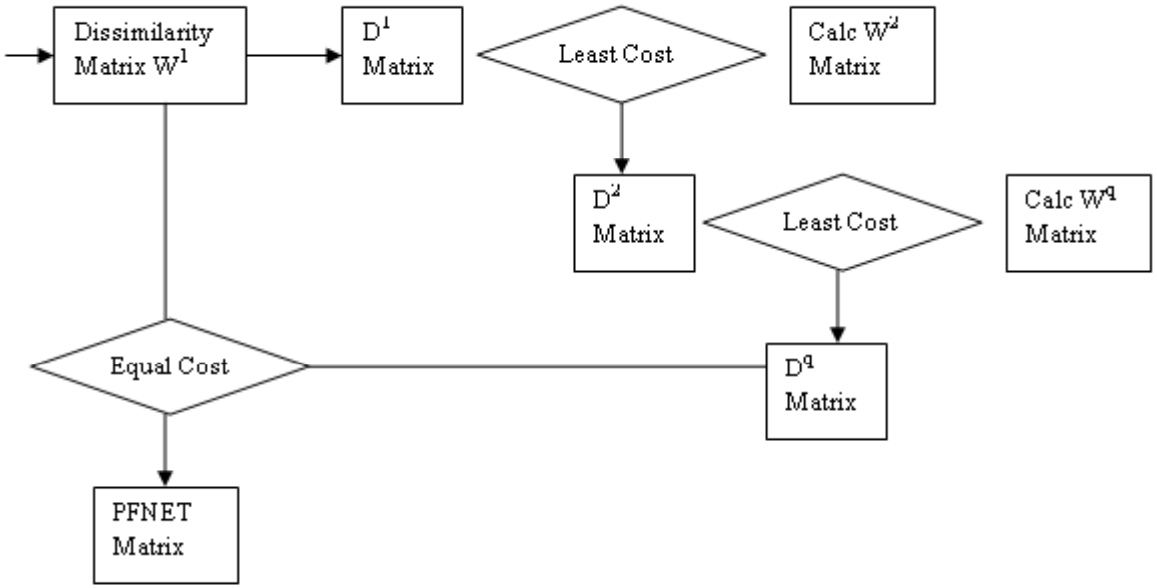
PFNET(*r, q)* – Minkowski *r*-metric

$$w(P) = \left[\sum_{i=1}^{k} w_i^r \right]^{1/r} \quad \text{where } r \geq 1,\ w_i \geq 0 \text{ for all } i$$

When r = 1, Minkowski distance is the sum of the path weights.

When r = ∞, Minkowski distance is the max weight of any link along the path.

Build Pathfinder Algorithm



Procedure PATHFINDER PFNET(*r*, *q*)

1. Compare W^2 , D^2, W^3, D^3,…, W^q, D^q;
2. Comparing elements of D^q and W^1, wherever $d_{ij} = w_{ij}$, then mark e_{ij} as a link in PFNET(r, q).

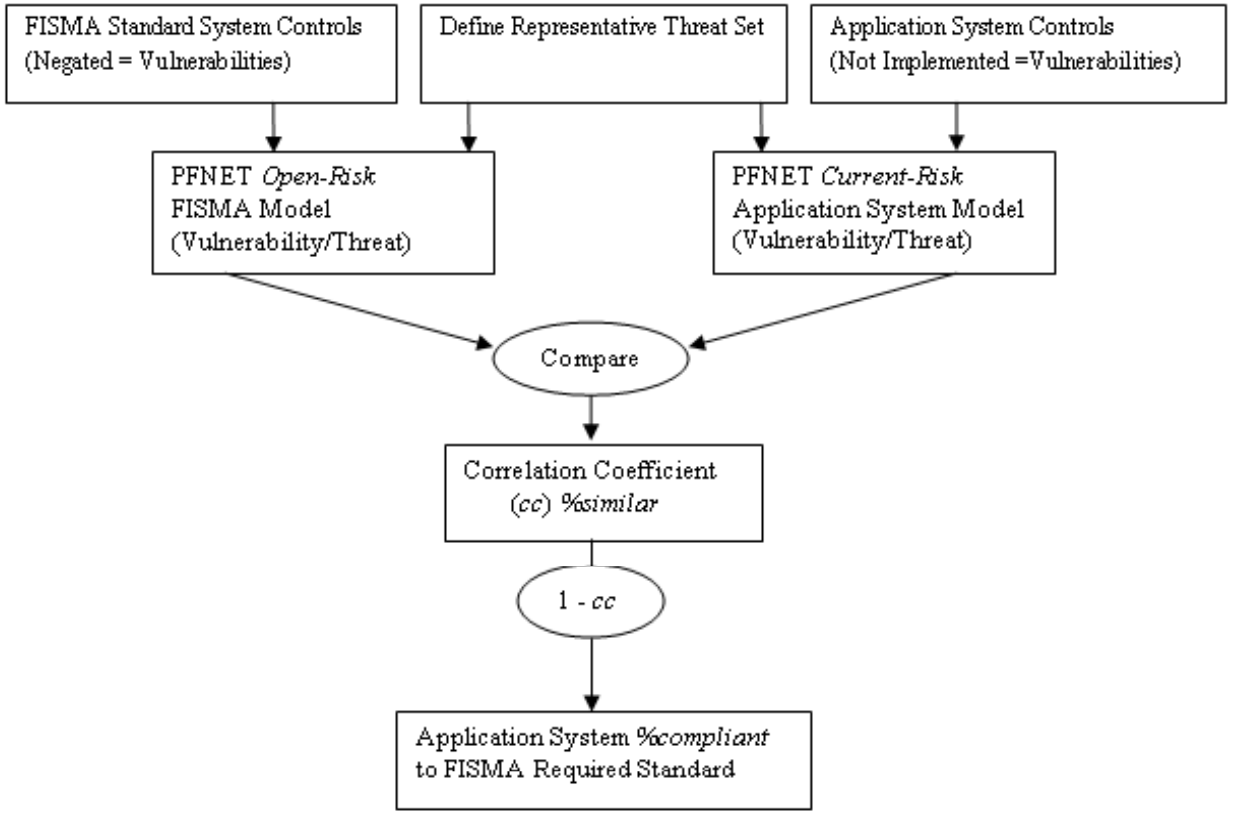
PFNET(*r, q)* Algorithm Properties

- Network guaranteed to be connected
- When $r = \infty$ and $q = n - 1$
  - Shortest paths having n-1 or fewer links retained
  - Triangle inequality not violated
  - Minimum number of edges
  - A unique network generated

Outline

- Information system security
- Federal Information Security Management Act (FISMA)
- Pathfinder Networks (PFNETs)
- FISMA compliance measurement using Pathfinder – an example

Compliance Measurement Using PFNETs



Risk Analysis Entity Set

ID	Threat Category Name	Control ID		Vulnerability Category Name
T1	Unapproved Software	CM-1	V1	Inadequate Configuration Management Policy and Procedures
T2	Software Version Errors	CM-5	V2	Inadequate Access Restrictions for Change
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-
T9	Accountability Data Loss	SI-9	V20	Inadequate Information Input Restrictions

Define Standard Correlation

T1: Introduction of Unapproved Software

V1: Inadequate Configuration Management Policy and Procedures

T2: Software Version Implementation Errors

V1: Inadequate Configuration Management Policy and Procedures

.

.

.

T9: Accountability Data Loss

V4: Inadequate User Identification and Authentication

V5: Inadequate Account Management

V6: No System Use Notification

V7: No Termination After Maximum Unsuccessful Login Attempts

V8: Inadequate Access Control Policy and Procedures

V9: Inadequate Supervision and Review – Access Control

V11: Inadequate Access Monitoring

V16: Inadequate Audit Monitoring, Analysis, and Reporting

FMS System Correlation

Assume Financial Management System (FMS) where these vulnerabilities exist:
V4,V6,V7,V8,V9,V10,V11,V12,V13,V14,V15,V16,V17,V18,V19

Open-risk Standard Co-occurrence Groups	**FMS System** Co-occurrence Groups
(T1,V1)	
(T2,V1)	
(T3,V2)	
(T4,V2)	
(T5,V18,V17,V10,V8,V4,V3,V1)	(T5,V18,V17,V10,V8,V4)
(T6,V18,V10,V8,V4,V3,V1)	(T6,V18,V10,V8,V4)
(T7,V20,V19,V10,V8,V4,V3,V1)	(T7,V20,V19,V10,V8,V4)
(T8,V15,V14,V13,V12,V3,V1)	(T8,V15,V14,V13,V12)
(T9,V16,V11,V9,V8,V7,V6,V5,V4)	(T9,V16,V11,V9,V8,V7,V6,V4)

Build Similarity Matrices

n x *n* matrix of categorized entities
Higher count implies greater similarity

Open-risk Standard Co-occurrence Groups	**FMS System** Co-occurrence Groups
(T1,V1)	
(T2,V1)	
(T3,V2)	
(T4,V2)	
(T5,V18,V17,V10,V8,V4,V3,V1)	(T5,V18,V17,V10,V8,V4)
(T6,V18,V10,V8,V4,V3,V1)	(T6,V18,V10,V8,V4)
(T7,V20,V19,V10,V8,V4,V3,V1)	(T7,V20,V19,V10,V8,V4)
(T8,V15,V14,V13,V12,V3,V1)	(T8,V15,V14,V13,V12)
(T9,V16,V11,V9,V8,V7,V6,V5,V4)	(T9,V16,V11,V9,V8,V7,V6,V4)

Build Dissimilarity Matrices

- Input Similarity Matrix
- Dissimilarity Matrix Entries =

  (max co-occurrence count + 1) – similarity matrix entry

  - Open Risk Standard max co-occurrence count = 4
  - FMS System max co-occurrence count = 4
- Lower count implies greater similarity

Build Pathfinder Networks

- Input Dissimilarity Matrix
- Apply Pathfinder Algorithm
- Output PFNET *(r, q)* = (∞, 28*)*
- Standard model – 189 edges/edge-weights
- FMS System model – 344 edges/edge-weights

Build Minimum Distance Matrices

- Input PFNET
- Apply Shortest Path Algorithm
- Output Minimum Distance Matrix
- Standard Open Risk Model & FMS System Model

Compare Stakeholder Perceptions

- Compare FMS System model with Standard Open Risk model

$$cc = \frac{\sum (a - \bar{a})(b - \bar{b})}{\sqrt{\sum (a - \bar{a})^2 \sum (b - \bar{b})^2}}$$

- Output **overall** and **detail** similarity percentages
- 1 – overall % similar = *%compliant*

Risk Model Co-occurrence Groups

Open Risk:	(T1,V1)	(T2, V1)
	(T3,V2)	(T4,V2)
	(T5,V18,V17,V10,V8,V4,V3,V1)	(T6,V18,V10,V8,V4,V3,V1)
	(T7,V20,V19,V10,V8,V4,V3,V1)	(T8,V15,V14,V13,V12,V3,V1)
	(T9,V16,V11,V9,V8,V7,V6,V5,V4)	
FMS Model 1	(T5,V18,V17,V10,V8,V4)	(T6,V18,V10,V8,V4)
	(T7,V20,V19,V10,V8,V4)	(T8,V15,V14,V13,V12)
	(T9,V16,V11,V9,V8,V7,V6,V4)	
FMS Model 2	(T5,V18,V10,V8)	(T6,V18,V10,V8)
	(T7,V20,V19,V10,V8)	(T8,V15,V14,V13,V12)
	(T9,V16,V11,V9,V8,V7,V6)	
FMS Model 3	(T5,V10,V8)	(T6,V10,V8)
	(T7,V10,V8)	(T8,V15,V14,V13,V12)
	(T9,V16,V11,V9,V8,V7,V6)	
FMS Model 4	(T5,V8)	(T6,V8)
	(T7,V8)	(T8,V15,V14,V13,V12)
	(T9,V16,V11,V9,V8,V7,V6)	
FMS Model 5	(T5,V8)	(T6,V8)
	(T7,V8)	(T8,V15,V14,V13,V12)
	(T9,V9,V8,V6)	
FMS Model 6	(T5,V8)	(T6,V8)
	(T7,V8)	(T8,V15,V14,V13)
	(T9,V8,V6)	
FMS Model 7	(T5,V8)	(T6,V8)
	(T7,V8)	(T9,V8,V6)
FMS Model 8	(T9,V6)	
Closed Risk	(No Category Groupings)	
Note: Highlighted vulnerabilities corrected in following model.		

Compare Risk Models

	Open Risk	FMS 1	FMS 2	FMS 3	FMS 4	FMS 5	FMS 6	FMS 7	FMS 8	Closed Risk
%compliant	0.0	0.55	0.59	0.66	0.69	0.77	0.82	0.87	0.95	1.0
Overall Path Distance *cc*	1.0	0.45	0.41	0.34	0.31	0.23	0.18	0.13	0.05	0.0
Node Path Distance *cc*										
V1	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V2	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V3	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V4	1.0	0.70	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V5	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V6	1.0	0.43	0.46	0.45	0.62	0.41	0.33	0.33	0.23	0.0
V7	1.0	0.43	0.46	0.45	0.62	0.0	0.0	0.0	0.0	0.0
V8	1.0	0.70	0.43	0.35	0.13	0.10	0.09	0.09	0.0	0.0
V9	1.0	0.43	0.46	0.45	0.63	0.41	0.0	0.0	0.0	0.0
V10	1.0	0.75	0.54	0.43	0.0	0.0	0.0	0.0	0.0	0.0
V11	1.0	0.43	0.46	0.45	0.63	0.0	0.0	0.0	0.0	0.0
V12	1.0	0.56	0.56	0.56	0.56	0.56	0.0	0.0	0.0	0.0
V13	1.0	0.56	0.56	0.56	0.56	0.56	0.48	0.0	0.0	0.0
V14	1.0	0.56	0.56	0.56	0.56	0.56	0.48	0.0	0.0	0.0
V15	1.0	0.56	0.56	0.56	0.56	0.56	0.48	0.0	0.0	0.0
V16	1.0	0.43	0.46	0.45	0.62	0.0	0.0	0.0	0.0	0.0
V17	1.0	0.66	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V18	1.0	0.74	0.69	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V19	1.0	0.65	0.62	0.0	0.0	0.0	0.0	0.0	0.0	0.0
V20	1.0	0.65	0.62	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T1	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T2	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T3	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T4	1.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
T5	1.0	0.66	0.64	0.54	0.29	0.29	0.29	0.29	0.0	0.0
T6	1.0	0.64	0.61	0.51	0.31	0.31	0.31	0.31	0.0	0.0
T7	1.0	0.64	0.62	0.55	0.29	0.29	0.29	0.29	0.0	0.0
T8	1.0	0.56	0.56	0.56	0.56	0.56	0.48	0.0	0.0	0.0
T9	1.0	0.43	0.46	0.45	0.62	0.41	0.33	0.33	0.23	0.0

Live Data Experiments

- Overall *%compliant* vs. system certification rating
- Detailed *cc* vs. certification recommended mitigation path
- Overall *%compliant* vs. certification ratings between years

The Challenge

- Clearly describe FISMA compliance status
- Track progress toward compliance
- Justify resource allocation
- Simplify report preparation

Note: This approach may be used with any standard where controls may be negated to form vulnerabilities.

Acronyms

- *cc*: Correlation Coefficient
- FIPS: Federal Information Processing Standard
- FISMA: Federal Information Security Management Act
- FMS: Financial Management System
- NIST: National Institute of Standards and Technology
- PFNETs: Pathfinder Networks
- RMF: Risk Management Framework
- SP: Special Publication

QUESTIONS

Additional Material

The slides that follow present a general example of the procedure for building Pathfinder models from subjective data.

Pathfinder Network Generation

- Correlate Entities
- Build Similarity Matrix
- Build Dissimilarity Matrix
- Build Pathfinder Network
- Build Minimum Distance Matrix
- Compare Stakeholder Perceptions

Correlate Entities

Stakeholder A Entity Correlation

(E1, E2, E3), (E2, E3, E4), (E3, E4)

	E1	E2	E3	E4
E1	-	X	X	
E2	X	-	X	X
E3	X	X	-	X
E4		X	X	-

Stakeholder B Entity Correlation

(E1, E3, E4), (E2, E3, E4), (E3, E4)

	E1	E2	E3	E4
E1	-		X	X
E2		-	X	X
E3	X	X	-	X
E4	X	X	X	-

Build Similarity Matrices

Stakeholder A Co-occurrance Groups
(E1, E2, E3), (E2, E3, E4), (E3, E4)

	E1	E2	E3	E4
E1	-	1	1	0
E2	1	-	2	1
E3	1	2	-	2
E4	0	1	2	-

Stakeholder B Co-occurrance Groups
(E1, E3, E4), (E2, E3, E4), (E3, E4)

	E1	E2	E3	E4
E1	-	0	1	1
E2	0	-	1	1
E3	1	1	-	3
E4	1	1	3	-

Build Dissimilarity Matrices

Stakeholder A DissimilarityMatrix

	E1	E2	E3	E4
E1	-	2	2	3
E2	2	-	1	2
E3	2	1	-	1
E4	3	2	1	-

Stakeholder B Dissimilarity Matrix

	E1	E2	E3	E4
E1	-	4	3	3
E2	4	-	3	3
E3	3	3	-	1
E4	3	3	1	-

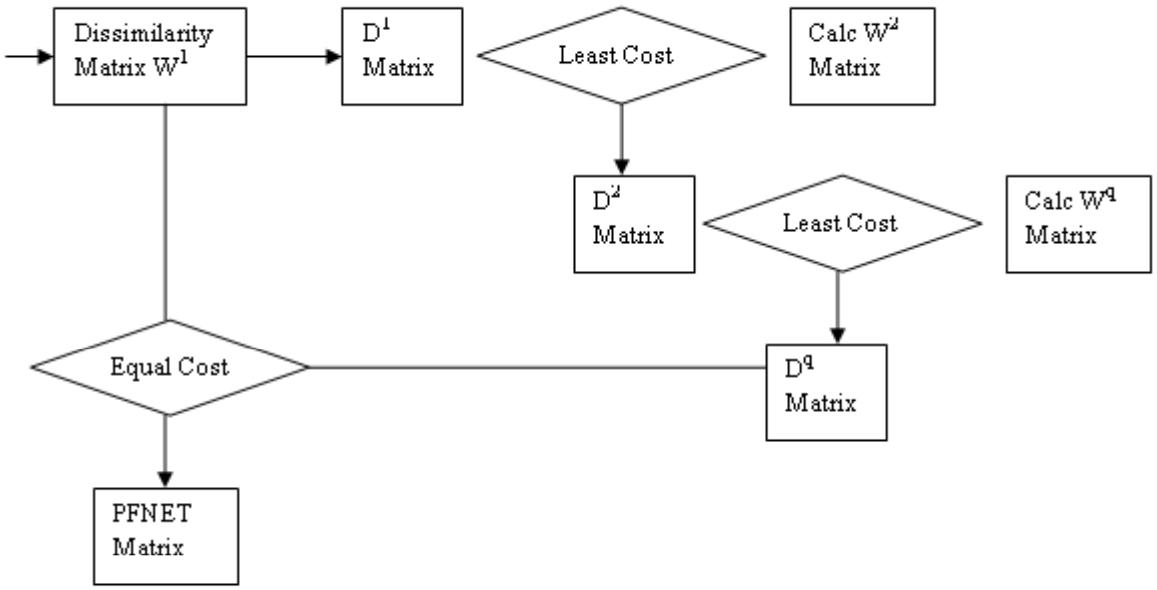
PFNET(*r, q)* – Minkowski *r*-metric

$$w(P) = \left(\sum_{i=1}^{k} w_i^r \right)^{1/r} \quad \text{where } r \geq 1,\ w_i \geq 0 \text{ for all } i$$

When r = 1, Minkowski distance is the sum of the path weights.

When r = ∞, Minkowski distance is the max weight of any link along the path.

Build Pathfinder Algorithm

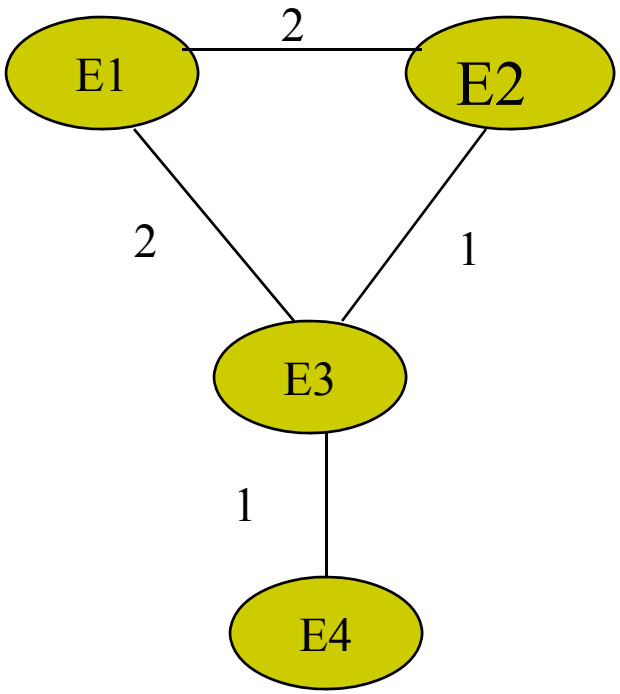


Procedure PATHFINDER PFNET(*r*, *q*) [2]

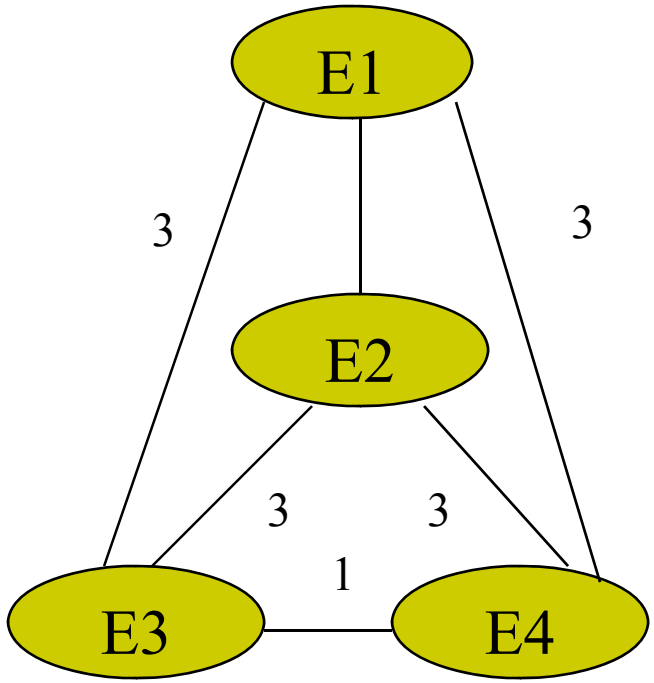
1. Compare W^2 , D^2, W^3, D^3,…, W^q, D^q;
2. Comparing elements of D^q and W^1, wherever $d_{ij} = w_{ij}$, then mark e_{ij} as a link in PFNET(r, q).

Pathfinder Networks

Stakeholder A PFNET(∞, 3)



Stakeholder B PFNET (∞, 3)



Build Minimum Distance Matrices

Stakeholder A

Minimum Distance Matrix

Distance Vector = (2 2 3 1 2 1)

	E1	E2	E3	E4
E1	-	2	2	3
E2	2	-	1	2
E3	2	1	-	1
E4	3	2	1	-

Stakeholder B Minimum

Minimum Distance Matrix

Distance Vector = (6 3 3 3 3 1)

	E1	E2	E3	E4
E1	-	6	3	3
E2	6	-	3	3
E3	3	3	-	1
E4	3	3	1	-

Compare Stakeholder Perceptions [3, 4]

$$cc = \frac{\sum (a - \bar{a})(b - \bar{b})}{\sqrt{\sum (a - \bar{a})^2 \sum (b - \bar{b})^2}}$$

Correlation Coefficient (cc) Formula

Stakeholder-A distance vector (2 2 3 1 2 1).

Stakeholder-B distance vector(6 3 3 3 3 1).

Comparison Results

Overall *cc* = 0.36

Stakeholder A Distance Vectors	Entity	Detail *cc*	Stakeholder B Distance Vectors
2 2 3	E1	-0.50	6 3 3
2 1 2	E2	0.50	6 3 3
2 1 1	E3	0.50	3 3 1
3 2 1	E4	0.87	3 3 1