Assessing the Effect of Deceptive Data in the Web of Trust

Yi Hu, Brajendra Panda, and Yanjun Zuo

Computer Science and Computer Engineering Department

University of Arkansas

Fayetteville, AR

Outline

- Open Rating Systems
- Objective of this Research
- Model
  - Indirect Trust Computation
  - Trust on Objects
  - Social Circles and their Effects
- Conclusion

Open Rating Systems

- No central authority
- Available to virtually everyone
- Lack of full knowledge of subjects and objects
- Trust plays a vital role
- Information Flow Policy may exist
  - Lattice Vs. Non-Lattice based

Problems

- Lack of mechanisms to prevent deceptive data from spreading from one subject to another.
- Lack of capability to evaluate the impacts of any deceptive data in an effective way.

Objective of this Research

- Evaluation of the effects of deceptive data transmitted by a malicious user
  - Which subjects in the trusted network may be affected by the deceptive data?

Our Model

- Utilizes both the web of trust and the information flow policy.

- Information Flow

  $< S, \rightarrow >$ where S is a set of subjects and $\rightarrow$ is defined on pairs of subjects.

  $A \rightarrow B$ indicates information from subject A is allowed to flow to subject B.

Our Model (continued)

- Web of Trust

  Set of Objects: O

  Set of Subjects: A

  Set of possible ratings of objects: D $(0 \leq D \leq 1)$

  Set of possible ratings of subjects: T $(0 \leq T \leq 1)$

  Partial function R: $A \times O = D$

  Partial function W: $A \times A = T$

  Web of trust is a directed graph represented by W

Our Model (continued)

- Information Flow Network and Web of Trust
  - Usually web of trust and information flow network are independent of each other.
  - However, trust management plays a critical role in discretionary based information flow policy.

Calculation of Indirect Trust Ratings

$$T_{ij} = Max(\forall P_k \in P: (1-d)^{|P_k|-1} * \prod_{T_{mn} \in P_k} T_{mn})$$

where

T_{ij} : indirect rating of user j by user i

P: all possible paths from j to i

P_k: an element of P

$|P_k|$: number of edges on kth path from j to i

T_{mn}: trust ratings between any pair of neighboring nodes m and n on a particular path represented by P_k from j to i

d: decay factor

Trust Rating Based on Information Flow Path

$$D_{io}' = D_{jo} * (1-d)^{|Q|-1} * \prod_{t_{mn} \in Q} T_{mn}$$

where
D_{io}' : rating of object o by subject i based on a particular information flow path from j to i

D_{jo}: originator j's rating of o

Q: set of trust ratings between all pairs of neighboring nodes on a particular path from j to i

The Basic Model

Steps to calculate effects of deceptive data:

1. Find all possible nodes where the information may reach.

2. For each of possible destination nodes, find all possible paths from the originating node to it.

3. For each of possible paths, calculate the rating of the deceptive data to the destination node. If the rating is below a trust threshold, this deceptive data will be discarded and, thus, would not spread to other nodes continuing on that path.

An Example

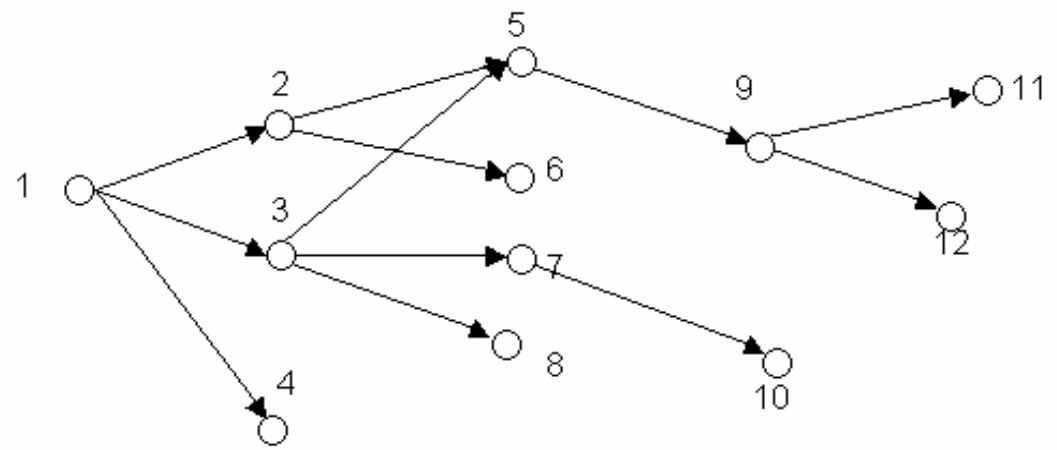

Figure 1. Information Flow Policy

An Example (Continued)

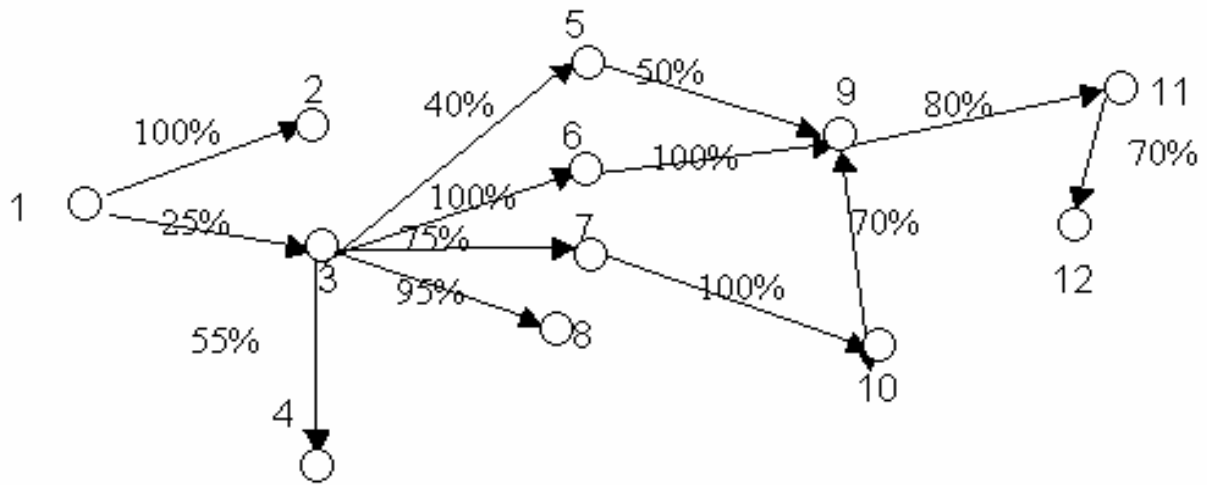

Figure 2. Web of Trust

Discussion of the Example

- Suppose subject 3 spreads a deceptive data *a*

- Suppose the trust decay factor d = 5%, and the trust threshold equal to 30%

  Subject 9 will not trust this deceptive data (D_{9a}'= 40% * 50% * 95% * 100% = 19%); thus (s)he will not send it to other subjects.

  So subjects 11 and 12 will not receive the data.

Augmenting the Basic Model with Social Circle Factor

- In the basic model no consideration was given to the property of social circle of web of trust.
- In general, information is selectively sent to individuals who the host thinks would be interested in it.
- Trust among subjects often developed based on the common interests, this is especially true with online communities.

A Social Circle

- In the web of trust in Figure 3, the circle indicates the social circle of subject *A*.
- In this figure, subjects inside the circle are considered to have common interest as that of subject *A*, whereas the people outside the circle have very little common interest as that of subject A.

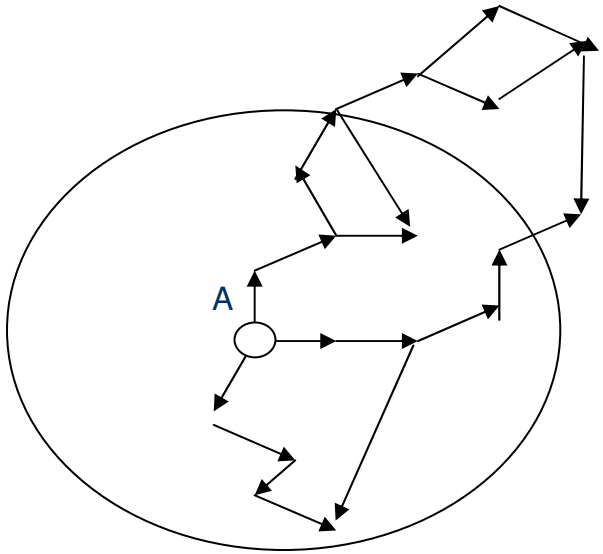

Figure 3. Social circle in a web of trust

Deceptive Data in a Social Circle

- The size of the social circle is calculated based on interest decay factor.
- Taking a social circle into account, there are four cases of how a deceptive data originating from subject *A* can affect other users.

Deceptive Data in a Social Circle (continued)

(Suppose D_{BO} represents the trust rating of object o by subject B and R_{trust} represents the trust threshold)

- Case 1: B is outside the social circle and $D_{BO} > R_{trust}$
  - No harm
- Case 2: B is outside the social circle and $D_{BO} < R_{trust}$
  - No harm
- Case 3: B is inside the social circle and $D_{BO} > R_{trust}$
  - B would be affected
- Case 4: B is inside the social circle and $D_{BO} < R_{trust}$
  - No harm

Conclusions

- Deceptive data transmitted by a malicious user in a web of trust affects other subjects in this network.
- The presented model utilizes both web of trust and information flow network to assess the effect of any such data.
- Future work would include a recovery mechanism to undo the damage.