Received September 27, 2019, accepted November 7, 2019, date of publication November 18, 2019,
date of current version December 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2953996

Sensitivity Analysis of Multi-State Social Network System Based on MDD Method

XUEYING SONG, XUJIE JIA, AND NANNAN CHEN
College of Science, Minzu University of China, Beijing 100081, China

Corresponding author: Xujie Jia (jiaxujie@126.com)

This work was supported by the National Natural Science Foundation of China Grant 71571198.

ABSTRACT With the advancement of computer and network technologies, Internet-based social networks called social networking services have become popular. Trust is a crucial basis for interactions among parties in social networks. Based on trust scores of direct links between parties, a trust sensitivity analysis can help identify which direct link(s) in a social network contributes the most to a trust relationship between parties who are not directly connected in the network. This paper generalizes the research object from two-state social networks to multistate social networks since the trust grade for people in a real social connection may have multiple levels. We model asymmetric multitrust level and multiparty social network systems and propose a probabilistic method based on multivalued decision diagrams (MDDs) to perform trust sensitivity analysis of social networks. Numerical examples are provided to demonstrate the application of the proposed methodology.

INDEX TERMS Multistate system, multivalued decision diagrams, sensitivity analysis, social network, trust evaluation.

I. INTRODUCTION

A social network is traditionally a conception of social science that uses actors (individuals, groups, or organizations) and relations to indicate the social relationships or interactions between actors [1]. With the advancement of computer and network technologies, Internet-based social networks called social networking services have become popular. Almost all Internet services that help people maintain their connections with others, such as Facebook, Google+, Twitter, and MySpace, can be regarded as a part of social networks [2].

Trust is a crucial basis for interactions among parties in social networks. A definition of trust was first developed by Deutsch [3]. A trusting behavior is defined as a person perceiving an ambiguous path, and the outcome of following the path can be good or bad, contingent on the action of another person. Jøsang *et al.* [4] proposed that trust networks consist of transitive trust relationships between people, organizations and software agents connected through a medium for communication and interaction.

A trust relationship between parties is typically characterized by a trust score or rating, which indicates how much a party trusts the others. Evaluating trust scores has been a challenging problem for social networks. Golbeck [5] proposed that a computational problem of trust is to determine how much one person in the network should trust another person to whom they are not connected. Avesani *et al.* [6] claimed that trustworthiness is a user-centered notion that requires the computation of personalized metrics. Different ways are available to express a trust relationship. Guha *et al.* [7] incorporated distrust in a computational trust propagation setting and developed a framework of trust propagation schemes, each of which may be appropriate in certain circumstances. Jøsang *et al.* [4] described a method for trust network analysis using subjective logic (TNA-SL). It provided a simple notation for expressing transitive trust relationships and defined a method for simplifying complex trust networks so that they can be expressed in a concise form and be computationally analyzed. Based on their research, Jiang *et al.* [8] proposed a modified flow-based trust evaluation scheme, GFTrust, in which they addressed path dependence using network flow and modeled trust decay by the leakage associated with each node. Then, Wang *et al.* [9] analyzed fine-grained feature-based social influence evaluation in online social networks and designed a social influence adjustment model based on the PageRank algorithm by identifying the influence contributions of friends.

The associate editor coordinating the review of this manuscript and approving it for publication was Zhaojun Li.

Trust evaluation algorithms are a hot topic in trust analysis research. Several trust evaluation algorithms have been developed to quantify trust. Kamvar *et al.* [10] proposed an Eigen Trust algorithm for peer-to-peer systems based on peers' historical performance. Katz and Golbeck [11] introduced the Tidal Trust algorithm to infer trust relationships. Tidal Trust utilizes a weighted-average approach based on the assumption that the propagation of trust along a path is multiplicative. Kuter and Golbeck [12] proposed a trust inference model and provided a confidence measurement based on probabilistic sampling. Golbeck [5] presented two sets of algorithms for calculating these trust inferences: one for networks with binary trust ratings and one for continuous ratings. For each rating scheme, the algorithms are built upon defined notions of trust. Each is then analyzed theoretically and with respect to simulated and actual trust networks. Liu *et al.* [13] proposed the OpinionWalk algorithm that models trust by the Dirichlet distribution and uses a matrix to represent the direct trust relations among users. There have also been many studies on social network trust; examples can be seen in Richardson *et al.* [14], Ziegler and Lausen [15], Quercia *et al.* [16], and Hang *et al.* [17].

Among the rich works on social network systems, considerable research efforts have been devoted to sensitivity and importance analysis. It is common that multiple communication paths exist between two parties for sharing information, interests or activities in a social network. As introduced in reference [2], some link(s) can be critical and thus become potential hazards for delivering reliable and secure information flow between two parties that are not directly connected in social networks. It is important to identify which direct link contributes the most to a trust relationship. Based on the trust scores of direct links between parties, trust sensitivity analysis can help identify which direct link(s) in a social network contributes the most to a trust relationship between different parties who are not directly connected in the network. Sensitivity analysis has been well studied in the context of fault tree reliability analysis [18]–[20]. Xing and Dugan [18] developed a methodology to analyze the sensitivity of the unreliability of generalized PMS to changes in the failure probability of a component. Zeng *et al.* [21] proposed a TAPE (Trust-Aware Privacy Evaluation) framework for quantitatively evaluating users' privacy levels in social networks. Xing and Amari [22] analyzed two-party trust sensitivity in social networks and presented a binary decision diagram (BDD)-based algorithm for trust sensitivity analysis in social networks. Three different sensitivity measures, including Birnbaum's measure, criticality importance factor, and structural importance measure, were investigated and adapted for a two-party trust sensitivity analysis.

Sensitivity analysis studies of social networks have mainly focused on two parties and binary systems. In practice, however, social networks are usually very complex and may consist of multiple parties. Additionally, trust always has properties of being diversified and asymmetric. There are not only two states of trust and distrust but also high trust, comparative trust, less trust, distrust, high distrust and so on. In social networks, a trust score between two parties has the characteristic of asymmetry. That is, the two parties usually trust each other differently [23]. Binary and symmetrical system models are inadequate for modeling and analyzing some social networks exhibiting multiple states [24], [25].

To the best of our knowledge, no studies have been performed on sensitivity and importance analysis of multiparty and multistate social network systems. In this paper, our efforts are focused on modeling asymmetric multitrust level and multiparty social network systems and proposing a probabilistic method based on multivalued decision diagrams (MDDs) to perform trust sensitivity and importance analysis of social networks.

The remainder of this paper is organized as follows: Section II describes the basics of MDDs. Section III presents the proposed MDD-based method for sensitivity analysis of a two-party multistate social network. The sensitivity of a multiparty multistate social network system is analyzed in Section IV. Section V presents illustrative example analysis results. Finally, Section VI gives conclusions and directions for future work.

II. MDD MODEL

A binary decision diagram (BDD) is a state-of-the-art data structure for the representation and efficient symbolic manipulation of logical functions [26], [27]. Based on a BDD method, an MDD consists of a set of decision (nonsink) nodes and two sink nodes labeled 0 and 1, representing the system not being or being in a particular state, [28], [29], respectively.

Assume two MDD logical expressions G and H:

$$\begin{aligned} G &= case\left(x, G_0, G_1, \ldots, G_{k-1}\right), \\ H &= case\left(x, H_0, H_1, \ldots, H_{k-1}\right). \end{aligned}$$

The operating rule for combining them into one MDD model is [30]:

$$\begin{aligned} &G\Diamond H \\ &= case\left(x, G_0, G_1, \ldots, G_{k-1}\right) \Diamond\, case\left(x, H_0, H_1, \ldots, H_{k-1}\right) \\ &= \left\{ \begin{array}{c} case\left(x, G_0\Diamond H_0, \ldots, G_{k-1}\Diamond H_{k-1}\right), \\ index\left(x\right) = index(y) \\ case\left(x, G_0\Diamond H, \ldots, G_{k-1}\Diamond H\right), \\ index\left(x\right) < index(y) \\ case\left(y, G\Diamond H_0, \ldots, G\Diamond H_{k-1}\right) \\ index\left(x\right) > index(y) \end{array} \right\} \end{aligned} \tag{1}$$

Based on the manipulation rules, the MDD model is generated with regard to a specific system performance metric. In computer implementation, the MDD can be evaluated using the recursive evaluation in equation (2) [27].

$$P_m(F) = p_{A,0}(t)P_m(F_0) + \cdots + p_{A,k-1}(t)P_m(F_{k-1}) \tag{2}$$

where $P_m(F)$ represents the system state probability associated with node F in state S_m.

An MDD is more suitable for describing systems with multiple state characteristics and multiterminal features.

Compared with the traditional precise method of reliability modeling, an MDD based on Shannon decomposition theory can describe the implicit state space of a system and ease the state space explosion problem. An MDD is an effective method for dealing with complex systems, especially for in-depth analysis of system design mechanisms and dynamic mastery of system performance. It is an increasingly powerful research tool with powerful and flexible characteristics in the field of reliability research.

III. SENSITIVITY OF A TWO-PARTY MULTISTATE SOCIAL NETWORK

As a conception in social science, a social network uses actors and relations in the form of a graph model to indicate relationships or interactions between different actors [1]. An actor (also referred to as a party) in the social network may represent an individual, a social group, or an organization and is represented by a node in the graph model. The direct interaction relationship between two actors is represented by a link connecting the nodes modeling the two actors in the graph. Any two actors within the same social network can be related through either a direct link (if applicable) or multiple hops along one or multiple paths.

In this work, a social network is represented using a probabilistic directed graph $G(V, E)$. It contains a set V of nodes and a set E of direct links between parties with a direct trust relationship. A two-party social network describes a social network with only one source node and sink node. The links are directed since trust in social networks is usually asymmetrical.

Assume that there are P links in a social network system represented by $e_1, e_2, \ldots, e_p$. Each link can assume multiple trust levels ranging from the lowest level 0 (total distrust) to the highest trust level n. $p(e_i^j)$ represents the probability that link e_i is in the state j $(i = 0, \ldots, p, j = 1, \ldots, n)$. Social networking systems also have multiple states, expressed as numbers $1, 2, \ldots, m$, of which 1 indicates that the entire social network is in the worst trust state and m indicates the optimal trust state for the entire social network system. There are two steps to analyze the sensitivity of a social network. The first is a path search, and the second is generating the MDD model and evaluating the sensitivity.

A. PATH SEARCH

The process of solving the sensitivity depends on the path in each system state. Order the social network links using a variable ordering heuristic as follows:

$$e_{\pi_1} < e_{\pi_2} < \cdots < e_{\pi_p},$$

where $\pi_1, \pi_2, \ldots, \pi_p$ are the rankings for integers $1, 2, \ldots, p$.

Then, look for all paths in state $k (k \in \{1, 2, \ldots, m\})$ of the social network system according to the search method shown in Fig. 1. There is a total number of paths N_k that meet state k of the system: $Path_1^k, Path_2^k, \ldots, Path_{N_k}^k$; then, the l-th path $Path_l^k$ can be represented by the following formula:

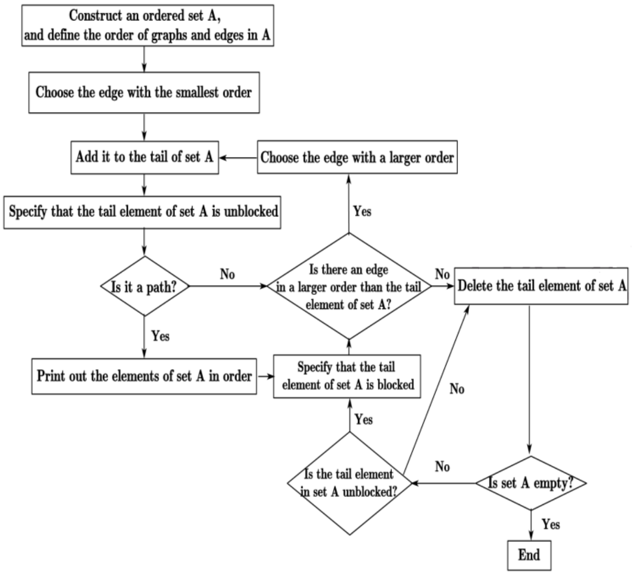
Construct an ordered set A, and define the order of graphs and edges in A
Choose the edge with the smallest order
Add it to the tail of set A
Choose the edge with a larger order
Specify that the tail element of set A is unblocked
Yes
Is it a path?
No
Is there an edge in a larger order than the tail element of set A?
No
Delete the tail element of set A
Yes
Print out the elements of set A in order
Specify that the tail element of set A is blocked
No
Yes
No
Is the tail element in set A unblocked?
Is set A empty?
Yes
End

FIGURE 1. Heuristic search flow of all paths in a social network from source nodes to sink nodes.

$$Path_l^k = \bigcap_{i=1}^{p} I(e_{\pi_i}^j,\ k,\ l)$$

where $e_{\pi_i}^j$ denotes link π_i in state j and $I(\cdot)$ is an indicative function as follows:

$$I(e_{\pi_i}^j, k, l) = \begin{cases} e_{\pi_i}^j, & e_{\pi_i}^j \text{ is in the l-th link which cause the system in state k} \\ 1, & e_{\pi_i}^j \text{ is not in the l-th link which cause the system in state k} \end{cases} \tag{3}$$

B. SENSITIVITY ANALYSIS

By Birnbaum's measure (Zhao *et al.* [20]; Akers [26]), the importance or sensitivity of a direct link e_i in the social network is defined as the partial derivative of the two-party trust probability between source S and sink T, denoted by $Trust(S, T)$, with respect to the link trust score $p(e_i)$, that is [2],

$$I_{BM}(i) = \frac{dTrust(S, T)}{dp(e_i)} \tag{4}$$

Then, the sensitivity index in a multistate social network system can be expressed as equation (5):

$$I_{BM}(i, j, k) = \frac{\partial Trust(S, T, k)}{\partial p(e_i^j)} \tag{5}$$

where $Trust(S, T, k)$ represents the trust value in the k-th state of the social network between S and T and e_i^j denotes link i in state j. For trust sensitivity analyses of two-party multistate social networks, we propose an algorithm based on Birnbaum's measure as follows.

Theorem 1: In a two-party multistate social network system, the state of the links e_i is $0, \ 1, \ \ldots, \ n$, respectively, and the sensitivity $S(i, k)$ of edge e_i to state k of the social network system is:

$$S(i,k) = \sqrt{1 - \frac{1}{1 + \sum_{j=0}^{n-1} (I_{BM}(i,j,k) - I_{BM}(i,n,k))^2}} \tag{6}$$

where

$$I_{BM}(i,j,k) = \frac{\partial Trust(S,T,k)}{\partial p(e_i^j)}.$$

The indicator $I_{BM}(i,j, \ k)$ indicates the influence degree of the small change of trust value in the specific state j of edge e_i on the change of trust value in the k-th state of social network, while $S(i,k)$ measures the influence of whole edge e_i on k-th state of network.

1) TWO-STATE SOCIAL NETWORK

For a two-state social network, the system and edges have two states, 0 and 1. Then, for edge e_i, $Trust(S, T)$ and $p(e_i^1)$ can be expressed as:

$$\begin{aligned} Trust(S,T) &= P(Path_1 + Path_2 + \cdots + Path_{N_1}) \\ &= P(Path_1) + P(Path_2) + \cdots + P(Path_{N_1}). \end{aligned}$$

$$\begin{cases} Trust(S,T) = f_{i0}(p(e_i^0)) + f_{i1}(p(e_i^1)) + F \\ p(e_i^0) + p(e_i^1) = 1 \end{cases} \tag{7}$$

where f_{i0} and f_{i1} represent the functions of $Trust(S, T)$ associated with edges e_i^0 and e_i^1, respectively and F represents the function that is not related to e_i^0 and e_i^1 for $Trust(S, T)$. Two state sensitivities can be analyzed in different ways, and equation (2) can be calculated. The full differential in equation (5) is as follows:

$$\begin{cases} dTrust(S,T) = \dfrac{\partial f_{i0}(p(e_i^0))}{\partial p(e_i^0)} dp(e_i^0) + \dfrac{\partial f_{i1}(p(e_i^1))}{\partial p(e_i^1)} dp(e_i^1), \\ dp(e_i^0) + dp(e_i^1) = 0. \end{cases} \tag{8}$$

For equation (6), from the analytical geometry aspect: let $y = dTrust(S,T)$, $A = \frac{\partial f_{i0}(p(e_i^0))}{\partial p(e_i^0)}$, $B = \frac{\partial f_{i1}(p(e_i^1))}{\partial p(e_i^1)}$, $x_0 = dp(e_i^0)$, and $x_1 = dp(e_i^1)$; then, equation (6) becomes

$$\begin{cases} y = Ax_0 + Bx_1 \\ x_0 + x_1 = 0, \end{cases}$$

which yields $y = (B - A)x_1$. Then,

$$\frac{dTrust(S,T)}{dp(e_i^1)} = \frac{y}{x_1} = B - A.$$

For the line $y = (B - A)x_1$, if the angle between the line and the horizontal plane is θ, then $y/x_1 = \tan\theta$. Therefore, for θ or the expression of θ equivalent to the role of the Birnbaum importance index, the closer θ is to 90°, the greater the sensitivity index value is. The Birnbaum importance index can be replaced by the angle between the normal vector $(B - A, -1)$ and the negative axis of y. The normal vector of the line $y = (B - A)x_1$ is $(B - A, -1)$, and the angle between $(B-A, -1)$ and the negative axis of y is equal to θ. Therefore, the Birnbaum importance index can be expressed by the angle between the normal vector and the negative axis.

2) MULTISTATE SOCIAL NETWORK

For the k-th state of a multistate social network,

$$\begin{cases} Trust(S,T,k) = f_{i0}(p(e_i^0)) + f_{i1}(p(e_i^1)) + \cdots + f_{in}(p(e_i^n)) + F, \\ p(e_i^0) + p(e_i^1) + \cdots + p(e_i^n) = 1, \end{cases} \tag{9}$$

Then, the full differential on both sides of (9) is:

$$\begin{cases} dTrust(S,T,k) = \dfrac{\partial f_{i0}(p(e_i^0))}{\partial p(e_i^0)} dp(e_i^0) + \cdots + \dfrac{\partial f_{in}(p(e_i^n))}{\partial p(e_i^n)} dp(e_i^n) \\ dp(e_i^0) + dp(e_i^1) + \cdots + dp(e_i^n) = 0 \end{cases}$$

$$y = dTrust(S,T,k), \quad A_j = \frac{\partial f_{ij}(p(e_i^j))}{\partial p(e_i^j)}, \ x_j = dp(e_i^j).$$

Then, equation (9) can be expressed as:

$$\begin{cases} y = A_0x_0 + A_1x_1 + \cdots + A_nx_n \\ x_0 + x_1 + \cdots + x_n = 0 \end{cases}$$

which can be expressed as:

$$y = (A_0 - A_n)x_0 + (A_1 - A_n)x_1 + \cdots + (A_{n-1} - A_n)x_{n-1}$$

There are an infinite number of normal vectors in the plane. To ensure that the angle between the normal vector and the negative axis of the y axis is an acute angle, a normal vector in the plane is selected as:

$$\lambda_1 = (A_0 - A_n, \ A_1 - A_n, \ \ldots, \ A_{n-1} - A_n, \ -1).$$

The vector corresponding to the negative axis of y is:

$$\lambda_2 = (0, \ 0, \ \ldots, \ 0, \ -1)$$

Because θ can reflect the size of the sensitivity index, to make the value of the sensitivity index size within the range of (0, 1) and with an increasing function of θ (always an acute angle), the sine function used in this paper represents the value of the multistate social network sensitivity index $S(i, k)$ as:

$$\begin{aligned} S(i,k) &= \sin\theta = \sqrt{1 - \cos^2\theta} = \frac{\lambda_1 \cdot \lambda_2}{||\lambda_1|| \cdot ||\lambda_2||} \\ &= \sqrt{1 - \frac{1}{1 + \sum_{j=0}^{n-1} (A_j - A_n)^2}}. \end{aligned}$$

Based on the definition of f_{ij},

$$A_j = \frac{\partial f_{ij}(p(e_i^j))}{\partial p(e_i^j)} = \frac{\partial Trust(S,T,k)}{\partial p(e_i^j)} = I_{BM}(i,j,k).$$

Then, the result is:

$$S(i,k)=\sqrt{1-\frac{1}{1+\sum_{j=0}^{n-1}(I_{BM}(i,j,k)-I_{BM}(i,n,k))^2}}.$$

IV. SENSITIVITY OF A MULTIPARTY MULTISTATE SOCIAL NETWORK SYSTEM

A multiparty social network is a social network that has multiple source nodes with one sink node, multiple sink nodes with one source node, or multiple sink nodes with multiple source nodes. Without loss of generality, in the multiparty social network $G(V,E)$, assume $S_1, S_2, \ldots, S_A$ and $T_1, T_2, \ldots, T_B$ denote the source nodes and sink nodes, respectively.

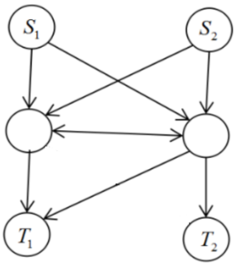

FIGURE 2. Schematic diagram of a multiparty (four parties) social network.

Fig. 2 shows a schematic diagram of a multiparty (two source nodes and two sink nodes) social network.

A. SENSITIVITY ANALYSIS

For multiparty multistate social network systems, sensitivity analysis is based on the results of a two-party multistate system.

Theorem 3: In a multiparty multistate social network, the state of links e_i is $0, 1, \ldots, n$, respectively, and the sensitivity $S(i,k)$ of edge e_i to state k of the social network system is:

$$S(i,k)=\sqrt{1-\frac{1}{1+\sum_{j=0}^{n-1}(I_{BM}(i,j,k)-I_{BM}(i,n,k))^2}} \tag{10}$$

where $I_{BM}(i,j,k) = \sum_{a=1}^{A}\sum_{b=1}^{B} I_{BM}(i,j,k,G_{a,b})$ and $I_{BM}(i,\ j,\ k,\ G_{a,b}) = \frac{\partial Trust(S_a,\ T_b,\ k)}{\partial p(e_i^j)}$.

A multiparty social network can decompose into multiple two-party social networks. Let $G_{a,b}$ denote a subfigure of G, where $G_{a,b}$ is a two-party social network probability graph from source node S_a to end node T_b. The multiparty social network has A source nodes and B end nodes. Then, probability graph G could be split to $A \times B$ two-party multistate social network subgraphs as follows:

$$G_{1,1},\ G_{1,2},\ \ldots,\ G_{1,B},\ G_{2,1},\ G_{2,2},\ \ldots,\ G_{2,B},\ldots,\ G_{A,1},\ G_{A,2},\ \ldots,\ G_{A,B},$$

and the set of all paths in the probability graph model G is:

$$Path = Path_{1,1} \cup Path_{1,2} \cup \cdots \cup Path_{a,b} \cup \cdots \cup Path_{A,B} \tag{11}$$

where $Path_{a,b}$ is the set of all paths from source node S_a to sink node T_b.

$Path_{a,b}^k$ refers to the set of all paths in the k-th system state of graph $G_{a,b}$. $Trust(S_a,\ T_b,\ k)$ is the trust value of the k-th social network state of subgraph $G_{a,b}$. Then,

$$Trust(S_a,\ T_b,\ k) = P(Path_{a,b}^k).$$

$Trust(S,\ T,\ k)$ denotes the trust value of state k in multiparty multistate social network probability figure G. Based on equation (11), $Trust(S,\ T,\ k)$ is obtained as follows:

$$\begin{aligned}
&Trust(S,T,k)\\
&= P(Path^k)\\
&= P(Path_{1,1}^k \cup Path_{1,2}^k \cup \cdots \cup Path_{a,b}^k \cup \cdots \cup Path_{A,B}^k)\\
&= P(Path_{1,1}^k)+P(Path_{1,2}^k)+\cdots+P(Path_{a,b}^k)+\cdots+P(Path_{A,B}^k)\\
&= \sum_{a=1}^{A}\sum_{b=1}^{B} Trust(S_a,T_b,k).
\end{aligned} \tag{12}$$

As

$$I_{BM}(i,\ j,\ k,\ G_{a,b}) = \frac{\partial Trust(S_a,\ T_b,\ k)}{\partial p(e_i^j)}, \tag{13}$$

from equations (12) and (13),

$$\begin{aligned}
I_{BM}(i,j,k) &= \frac{\partial Trust(S,T,k)}{\partial p(e_i^j)}\\
&= \frac{\partial}{\partial p(e_i^j)}\sum_{a=1}^{A}\sum_{b=1}^{B} Trust(S_a,T_b,k)\\
&= \sum_{a=1}^{A}\sum_{b=1}^{B}\frac{\partial Trust(S_a,T_b,k)}{\partial p(e_i^j)}\\
&= \sum_{a=1}^{A}\sum_{b=1}^{B} I_{BM}(i,j,k,G_{a,b}).
\end{aligned} \tag{14}$$

Based on the results in Section II, the sensitivity of a multiparty multistate social network is:

$$S(i,k)=\sqrt{1-\frac{1}{1+\sum_{j=0}^{n-1}(I_{BM}(i,j,k)-I_{BM}(i,n,k))^2}}$$

where $I_{BM}(i,j,k) = \sum_{a=1}^{A}\sum_{b=1}^{B} I_{BM}(i,j,k,G_{a,b})$ and $I_{BM}(i,\ j,\ k,\ G_{a,b}) = \frac{\partial Trust(S_a,\ T_b,\ k)}{\partial p(e_i^j)}$.

V. EXAMPLES

A. TWO-PARTY MULTISTATE SOCIAL NETWORK

As shown in Fig. 3, in a two-party multistate social network diagram, a circle represents an individual, and a link represents a trust connection between individuals.

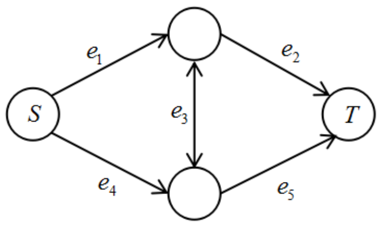

FIGURE 3. Two-party multistate social network diagram.

Each link has three states: ''complete distrust'', ''doubtful'' and ''full trust'', denoted as 0, 1 and 2, respectively. For links e_i, $i = 1, 2, 3, 4, 5$, $\bar{e}_i$ denotes that the link is in state 0, and e_i indicates that the link is in state 1 or 2. e_i^j represents that edge e_i is in state j, where $i = 1, 2, 3, 4, 5$, $j = 0, 1, 2$, and the probabilities of occurrence of the three states are:

$$(P(e_i^0), P(e_i^1), P(e_i^2)) = (0.2\ ,\ 0.3\ ,\ 0.5).$$

The social network has three states: 0, 1, and 2. In a land concentration from the source node to the end node, except for an edge with state 0, for all the remaining edges, if no edge is in state 2, then the social network is in state 0; if there is one and only one edge in state 2, then the social network is in state 1; and if at least two edges are in state 2, the social network is in state 2. Social network statuses of 0, 1, and 2 are understood to be the worst, general, and best three states of social network credibility, respectively.

1) STEP (1): ORDER THE SOCIAL NETWORK LINKS

There are 5 edges in the above figure: $e_1,\ e_2,\ e_3,\ e_4,\ e_5$. Assume that the following ranking method is applied: first, find any path from the source node to the end node, for example, $e_1,\ e_2$; then, step back and find the path to the end node. The order in which the edges are finally obtained is:

$e_1 < e_2 < e_3 < e_5 < e_4$, abbreviated as $e_1,\ e_2,\ e_3,\ e_5,\ e_4$.

2) STEP (2): FIND THE PATH

There are 5 edges in the probability map model, and each edge is either ''blocked'' or ''unblocked''; the 5 sides have $2^5 = 32$ plans. The obtained path is:

$$e_1e_2, e_1e_3e_5, e_2e_3e_4, e_4e_5. \tag{15}$$

According to the state definition of the social network, all paths corresponding to each state can be obtained. For a social network status of 0, there are 48 paths as follows:

$$\begin{aligned}
&Path_1^0 = e_1^0e_2^0, \quad Path_2^0 = e_1^0e_2^1, \ Path_3^0 = e_1^0e_2^2,\\
&Path_4^0 = e_1^1e_2^0, \quad Path_5^0 = e_1^2e_2^0, \ Path_6^0 = e_1^0e_3^0e_5^0,\\
&Path_7^0 = e_1^0e_3^0e_5^1, \quad Path_8^0 = e_1^0e_3^0e_5^2, \ Path_9^0 = e_1^0e_3^1e_5^0,\\
&Path_{10}^0 = e_1^0e_3^2e_5^0, \quad Path_{11}^0 = e_1^1e_3^0e_5^0, \ Path_{12}^0 = e_1^2e_3^0e_5^0,\\
&Path_{13}^0 = e_1^0e_3^1e_5^1, \quad Path_{14}^0 = \ e_1^0e_3^1e_5^2, \ Path_{15}^0 = e_1^0e_3^2e_5^1,\\
&Path_{16}^0 = e_1^0e_3^2e_5^2, \quad Path_{17}^0 = e_1^1e_3^0e_5^1, \ Path_{18}^0 = e_1^1e_3^0e_5^2,\\
&Path_{19}^0 = e_1^2e_3^0e_5^1, \quad Path_{20}^0 = e_1^2e_3^0e_5^2, \ Path_{21}^0 = e_1^1e_3^1e_5^0,\\
&Path_{22}^0 = e_1^1e_3^2e_5^0, \quad Path_{23}^0 = e_1^2e_3^1e_5^0, \ Path_{24}^0 = e_1^2e_3^2e_5^0,\\
&Path_{25}^0 = e_4^0e_3^0e_2^0, \quad Path_{26}^0 = e_4^0e_3^0e_2^1, \ Path_{27}^0 = e_4^0e_3^0e_2^2,\\
&Path_{28}^0 = e_4^0e_3^1e_2^0, \quad Path_{29}^0 = e_4^0e_3^2e_2^0, \ Path_{30}^0 = e_4^1e_3^0e_2^0,\\
&Path_{31}^0 = e_4^2e_3^0e_2^0, \quad Path_{32}^0 = e_4^0e_3^1e_2^1, \ Path_{33}^0 = e_4^0e_3^1e_2^2,\\
&Path_{34}^0 = e_4^0e_3^2e_2^1, \quad Path_{35}^0 = e_4^0e_3^2e_2^2, \ Path_{36}^0 = e_4^1e_3^0e_2^1,\\
&Path_{37}^0 = e_4^1e_3^0e_2^2, \quad Path_{38}^0 = e_4^2e_3^0e_2^1, \ Path_{39}^0 = e_4^2e_3^0e_2^2,\\
&Path_{40}^0 = e_4^1e_3^1e_2^0, \quad Path_{41}^0 = e_4^1e_3^2e_2^0, \ Path_{42}^0 = e_4^2e_3^1e_2^0,\\
&Path_{43}^0 = e_4^2e_3^2e_2^0, \quad Path_{44}^0 = e_4^0e_5^0, \ Path_{45}^0 = e_4^0e_5^1,\\
&Path_{46}^0 = e_4^0e_5^2, \quad Path_{47}^0 = e_4^1e_5^0, \ Path_{48}^0 = e_4^2e_5^0.
\end{aligned}$$

For a social network status of 1, there are a total of 20 paths as follows:

$$\begin{aligned}
&Path_1^1 = e_1^1e_2^1, \quad Path_2^1 = e_1^1e_2^2, \ Path_3^1 = e_1^2e_2^1,\\
&Path_4^1 = e_1^1e_3^1e_5^1, \quad Path_5^1 = e_1^1e_3^1e_5^2, \ Path_6^1 = e_1^1e_3^2e_5^1,\\
&Path_7^1 = e_1^2e_3^1e_5^1, \quad Path_8^1 = e_1^1e_3^2e_5^2, \ Path_9^1 = e_1^2e_3^1e_5^2,\\
&Path_{10}^1 = e_1^2e_3^2e_5^1, \quad Path_{11}^1 = e_4^1e_3^1e_2^1, \ Path_{12}^1 = e_4^1e_3^1e_2^2,\\
&Path_{13}^1 = e_4^1e_3^2e_2^1, \quad Path_{14}^1 = e_4^2e_3^1e_2^1, \ Path_{15}^1 = e_4^1e_3^2e_2^2,\\
&Path_{16}^1 = e_4^2e_3^1e_2^2, \quad Path_{17}^1 = e_4^2e_3^2e_2^1, \ Path_{18}^1 = e_4^1e_5^1,\\
&Path_{19}^1 = e_4^1e_5^2, \quad Path_{20}^1 = e_4^2e_5^1.
\end{aligned}$$

For a social network status of 2, there are 4 paths as follows:

$$\begin{aligned}
&Path_1^2 = e_1^2e_2^2, \quad Path_2^2 = e_1^2e_3^2e_5^2,\\
&Path_3^2 = e_2^2e_3^2e_4^2, \quad Path_4^2 = e_4^2e_5^2.
\end{aligned}$$

3) STEP (3): GENERATE THE MDD MODEL

A multivalued decision graph is generated for each social network state. The multivalued decision graphs are shown in Figs. 4-7.

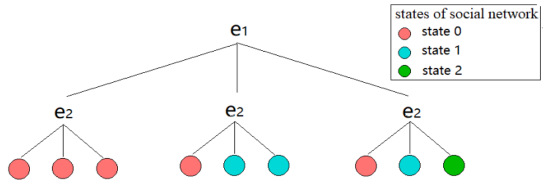

FIGURE 4. The multivalued decision graph for a social network state of e_1e_2.

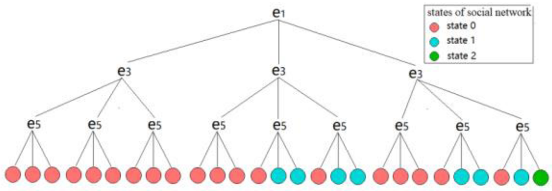

FIGURE 5. The multivalued decision graph for a social network state of $e_1e_3e_5$.

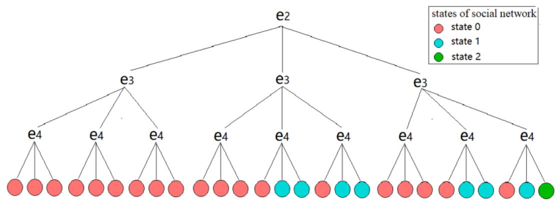

FIGURE 6. The multivalued decision graph for a social network state of $e_2e_3e_4$.

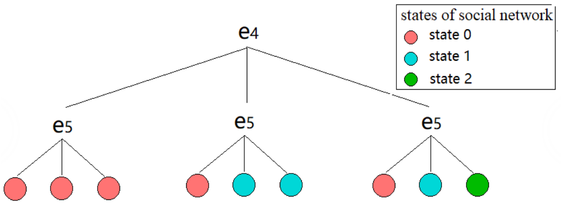

FIGURE 7. The multivalued decision graph for a social network state of e_4e_5.

4) STEP (4): SENSITIVITY AND CRITICALITY IMPORTANCE FACTOR

According to equation (3), when $k = 0$,

$$
\begin{aligned}
&Trust(S,\ T,\ 0)\\
&= \sum_{t=1}^{48} P(Path_t^0)\\
&= p(e_1^0)p(e_2^0) + \cdots + p(e_1^0)p(e_3^0)p(e_5^0) + \cdots + p(e_4^2)p(e_5^0)\\
&= 1.736\\
&I_{BM}(1,\ 0,\ 0)\\
&= \frac{\partial Trust(S, T,\ 0)}{\partial p(e_1^0)}\\
&= p(e_2^0) + p(e_2^1) + p(e_2^2) + p(e_3^0)p(e_5^0) + p(e_3^0)p(e_5^1)\\
&\quad + p(e_3^0)p(e_5^2) + p(e_3^1)p(e_5^0) + p(e_3^2)p(e_5^0) + p(e_3^1)p(e_5^1)\\
&\quad + p(e_3^1)p(e_5^2) + p(e_3^2)p(e_5^1) + p(e_3^2)p(e_5^2)\\
&= 2.\\
&I_{BM}(1,\ 1,\ 0)\\
&= \frac{\partial Trust(S, T,\ 0)}{\partial p(e_1^1)}\\
&= p(e_2^0) + p(e_3^0)p(e_5^0) + p(e_3^0)p(e_5^1)\\
&\quad + p(e_3^0)p(e_5^2) + p(e_3^1)p(e_5^0) + p(e_3^2)p(e_5^0)\\
&= 0.56\\
&\quad \vdots\\
&I_{BM}(5,\ 2,\ 0)\\
&= \frac{\partial Trust(S, T,\ 1)}{\partial p(e_5^2)}\\
&= p(e_4^0) + p(e_1^0)p(e_3^0) + p(e_1^0)p(e_3^1)\\
&\quad + p(e_1^0)p(e_3^2) + p(e_1^1)p(e_3^0) + p(e_1^2)p(e_3^0)\\
&= 0.56.
\end{aligned}
$$

For any i and j, $I_{BM}(i, j,\ 0)$ of social network status $k = 0$ can be expressed by Tab. 1 as follows:

TABLE 1. $I_{BM}(i, j, 0)$ of social network status $k = 0$.

j \ i	1	2	3	4	5
0	2	2	2	2	2
1	0.56	0.56	0.6	0.56	0.56
2	0.56	0.56	0.6	0.56	0.56

When $k = 1$:

$$
\begin{aligned}
Trust(S,\ T,\ 1) &= \sum_{t=1}^{20} P(Path_t^1).\\
I_{BM}(1,\ 0,\ 1) &= \frac{\partial Trust(S, T,\ 1)}{\partial p(e_1^0)} = 0.\\
I_{BM}(1,\ 1,\ 1) &= \frac{\partial Trust(S, T,\ 1)}{\partial p(e_1^1)} = 1.44.\\
&\ \vdots\\
I_{BM}(5,\ 2,\ 1) &= \frac{\partial Trust(S, T,\ 1)}{\partial p(e_5^2)} = 0.69.
\end{aligned}
$$

$I_{BM}(i, j,\ 1)$ of social network status $k = 1$ can be expressed by the following Tab. 2:

TABLE 2. $I_{BM}(i, j, 1)$ of social network status $k = 1$.

j \ i	1	2	3	4	5
0	0	0	0	0	0
1	1.44	1.44	1.28	1.44	1.44
2	0.69	0.69	0.78	0.69	0.69

When $k = 2$, $I_{BM}(i, j,\ 2)$ can be expressed by Tab. 3 as follows:

Based on Theorem

$$
S(i, k) = \sqrt{1 - \frac{1}{1 + \sum_{j=0}^{n-1} (I_{BM}(i, j, k) - I_{BM}(i, n, k))^2}}.
$$

$S(i, k)$ is as follows:

The results of $I_{CIF}(i, j,\ k)$ for different system states k are shown in Tabs. 5-7 as follows:

Then, $C(i, k)$ can be expressed by Tab. 8 as follows:

TABLE 3. $I_{BM}(i, j, 2)$ of social network status $k = 2$.

j i	1	2	3	4	5
0	0	0	0	0	0
1	0	0	0	0	0
2	0.75	0.75	0.5	0.75	0.75

TABLE 4. Values of $S(i, k)$.

k i	1	2	3	4	5
0	0.821	0.821	0.814	0.821	0.821
1	0.714	0.714	0.680	0.714	0.714
2	0.728	0.728	0.577	0.728	0.728

TABLE 5. $I_{CIF}(i, j, 0)$ of social network status $k = 0$.

j i	1	2	3	4	5
0	0.230	0.230	0.230	0.230	0.230
1	0.097	0.097	0.104	0.097	0.097
2	0.161	0.161	0.173	0.161	0.161

TABLE 6. $I_{CIF}(i, j, 1)$ of social network status $k = 1$.

j i	1	2	3	4	5
0	0	0	0	0	0
1	0.278	0.278	0.247	0.278	0.278
2	0.222	0.222	0.251	0.222	0.222

5) STEP (5): RESULTS ANALYSIS

According to the results of the sensitivity index $S(i, k)$, for the social network state $k = 0$, the sensitivity index is sorted as follows:

$$S(1,\ 0) = S(2,\ 0) = S(4,\ 0) = S(5,\ 0) > S(3,\ 0).$$

When the system is in state 0, the sensitivities of e_1, e_2, e_4 and e_5 are equal, and the largest, e_3, has the smallest value.

TABLE 7. $I_{CIF}(i, j, 2)$ of social network status $k = 2$.

j i	1	2	3	4	5
0	0	0	0	0	0
1	0	0	0	0	0
2	0.750	0.750	0.333	0.750	0.750

For the social network state $k = 1$, the sensitivity index is sorted as follows:

$$S(1,\ 1) = S(2,\ 1) = S(4,\ 1) = S(5,\ 1) > S(3,\ 1).$$

For the social network state $k = 2$, the sensitivity index is sorted as follows:

$$S(1,\ 2) = S(2,\ 2) = S(4,\ 2) = S(5,\ 2) > S(3,\ 2).$$

For the social network state $k = 0$, the importance index is sorted as follows:

$$C(1,\ 0) = C(2,\ 0) = C(4,\ 0) = C(5,\ 0) > C(3,\ 0).$$

In other words, when the system state is 0, the importance of e_1, e_2, e_4 and e_5 is equal, and the largest, e_3, has the smallest value.

For the social network state $k = 1$, the importance index is sorted as follows:

$$C(3,\ 1) > C(1,\ 1) = C(2,\ 1) = C(4,\ 1) = C(5,\ 1).$$

For the social network state $k = 2$, the importance index is sorted as follows:

$$C(1,\ 2) = C(2,\ 2) = C(4,\ 2) = C(5,\ 2) > C(3,\ 2).$$

As described in [2], in a two-state social network, the results of these two indicators are not always the same but are slightly different. The data in Tab. 4 and Tab. 8 are satisfied.

TABLE 8. Values of $C(i, k)$.

k i	1	2	3	4	5
0	0.094	0.094	0.089	0.094	0.094
1	0.223	0.223	0.243	0.223	0.223
2	0.728	0.728	0.426	0.728	0.728

B. MULTIPARTY MULTISTATE SOCIAL NETWORK

For the multiparty multistate social network shown in Fig. 8, assume that all links have 3 trust levels 0, 1, 2, where state 0 indicates "complete distrust", state 1 means "doubtful", and state 2 means "full trust". The entire social network system also has three states: 0, 1, and 2.

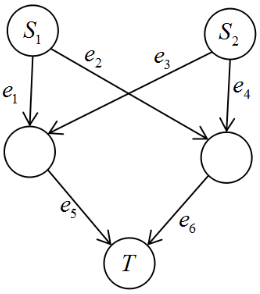

FIGURE 8. Multiparty multistate social network diagram.

Fig. 8 can be decomposed into the following two subgraphs:

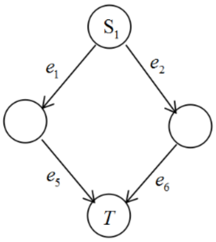

FIGURE 9. Subgraph 1.

First, in Fig. 9, there are four edges: e_1, e_2, e_5, e_6, and the order of the edges is: $e_1 < e_5 < e_2 < e_6$.

There are three states of the social network, 0, 1, and 2, and each of the states has the following definition. In the link path from the source node to the end node, excluding the edge in state 0, for all remaining edges, if none of the edges are in state 2, then the social network is in state 0; if there is only one edge in state 2, then the social network is in state 1; if there are at least two sides in state 2, then the social network is in state 2. The path is shown below:

$$e_1e_5, \quad e_2e_6$$

If $j = 0$, e_i^0 is the $\bar{e}_i$ in the above path, else if $j = 1, 2$, e_i^j is e_i in the above path. Based on the definition of the state of social network, all paths at each state can be calculated.

For social network state 0, all the paths are shown below:

$$\begin{aligned} &Path_1^0 = e_1^0e_5^0, \quad Path_2^0 = e_1^0e_5^1, \; Path_3^0 = e_1^0e_5^2, \\ &Path_4^0 = e_1^1e_5^0, \quad Path_5^0 = e_1^2e_5^0, \; Path_6^0 = e_2^0e_6^0, \\ &Path_7^0 = e_2^0e_6^1, \quad Path_8^0 = e_2^0e_6^2, \; Path_9^0 = e_2^1e_6^0, \\ &Path_{10}^0 = e_2^2e_6^0. \end{aligned}$$

For social network state 1, all the paths are shown below:

$$\begin{aligned} &Path_1^1 = e_1^1e_5^1, \quad Path_2^1 = e_1^1e_5^2, \; Path_3^1 = e_1^2e_5^1, \\ &Path_4^1 = e_2^1e_6^1, \quad Path_5^1 = e_2^1e_6^2, \; Path_6^1 = e_2^2e_6^1. \end{aligned}$$

For social network state 2, all the paths are shown below:

$$Path_1^2 = e_1^2e_5^2, \quad Path_2^2 = e_2^2e_6^2.$$

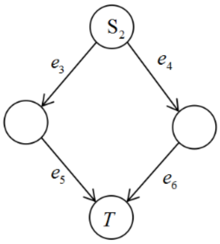

FIGURE 10. Subgraph 2.

The corresponding multivalued decision diagrams are generated for each social network state in subgraph 1, as shown in Figs. 11 and 12.

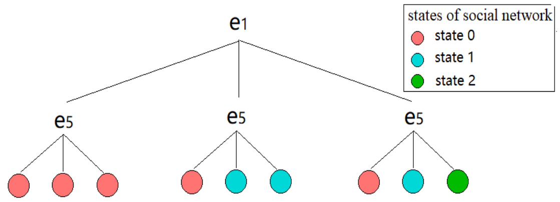

FIGURE 11. The multivalued decision graph for a social network state of e_1e_5 in subgraph 1.

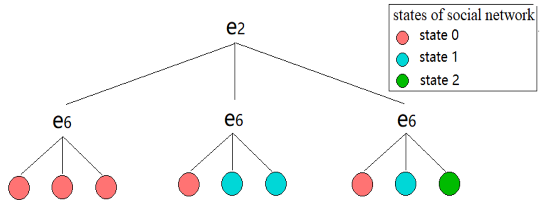

FIGURE 12. The multivalued decision graph for a social network state of e_2e_6 in subgraph 1.

First, calculate $I_{BM}(i, j, \; k, G_{1,1})$ of system state k. When $k = 0$,

$$\begin{aligned} Trust(S_1, \; T_1, \; 0) &= p(e_1^0)p(e_5^0)+p(e_1^0)p(e_5^1)+\cdots+p(e_2^2)p(e_6^0) \\ &= 0.72. \end{aligned}$$

Then

$$\begin{aligned} I_{BM}(1, \; 0, \; 0, G_{1,1}) &= \frac{\partial Trust(S_1, T_1, \; 0)}{\partial p(e_1^0)} = 1 \\ I_{BM}(1, \; 1, \; 0, G_{1,1}) &= \frac{\partial Trust(S_1, T_1, \; 0)}{\partial p(e_1^1)} = 0.2 \\ &\vdots \\ I_{BM}(6, \; 2, \; 0, G_{1.1}) &= \frac{\partial Trust(S_1, T_1, \; 0)}{\partial p(e_6^2)} = 0.2. \end{aligned}$$

For any i and j, $I_{BM}(i, j, \; 0, G_{1,1})$ can be indicated by the following Tab. 9:

When $k = 1$,

$$\begin{aligned} Trust(S_1, T_1, 1) &= p(e_1^1)p(e_5^1)+p(e_1^1)p(e_5^2)+\cdots+p(e_2^2)p(e_6^1) \\ &= 0.78. \end{aligned}$$

TABLE 9. $I_{BM}(i, j, 0, G_{1,1})$ of social network status $k = 0$ in subgraph 1.

j \ i	1	5	2	6
0	1	1	1	1
1	0.2	0.2	0.2	0.2
2	0.2	0.2	0.2	0.2

then

$$I_{BM}(1,\ 0,\ 1, G_{1,1}) = \frac{\partial Trust(S_1, T_1,\ 1)}{\partial p(e_1^0)} = 0.$$

$$I_{BM}(1,\ 1,\ 1, G_{1,1}) = \frac{\partial Trust(S_1, T_1,\ 1)}{\partial p(e_1^1)} = 0.8.$$

$$\vdots$$

$$I_{BM}(6,\ 2,\ 1, G_{1.1}) = \frac{\partial Trust(S_1, T_1,\ 1)}{\partial p(e_6^2)} = 0.8.$$

For any i and j, $I_{BM}(i, j,\ 1, G_{1,1})$ can be indicated by the following Tab. 10:

TABLE 10. $I_{BM}(i, j, 1, G_{1,1})$ of social network status $k = 1$ in subgraph 1.

j \ i	1	5	2	6
0	0	0	0	0
1	0.8	0.8	0.8	0.8
2	0.3	0.3	0.3	0.3

When $k = 2$:

$$Trust(S_1, T_1, 2) = p(e_1^2)p(e_5^2) + p(e_2^2)p(e_6^2) = 0.5$$

Then, for any i and j, $I_{BM}(i, j,\ 2, G_{1,1})$ can be indicated by the following Tab. 11:

TABLE 11. $I_{BM}(i, j, 2, G_{1,1})$ of social network status $k = 2$ in subgraph.

1

j \ i	1	5	2	6
0	0	0	0	0
1	0	0	0	0
2	0.5	0.5	0.5	0.5

TABLE 12. $I_{BM}(i, j, 0, G_{2,1})$ of social network status $k = 0$ in subgraph.

2

j \ i	3	5	4	6
0	1	1	1	1
1	0.2	0.2	0.2	0.2
2	0.2	0.2	0.2	0.2

TABLE 13. $I_{BM}(i, j, 1, G_{2,1})$ of social network status $k = 1$ in subgraph 2.

j \ i	3	5	4	6
0	0	0	0	0
1	0.8	0.8	0.8	0.8
2	0.3	0.3	0.3	0.3

TABLE 14. $I_{BM}(i, j, 2, G_{2,1})$ of social network status $k = 2$ in subgraph.

2

j \ i	3	5	4	6
0	0	0	0	0
1	0	0	0	0
2	0.5	0.5	0.5	0.5

TABLE 15. $I_{BM}(i, j, 0)$ of social network status $k = 0$.

j \ i	1	2	3	4	5	6
0	1	1	1	1	2	2
1	0.2	0.2	0.2	0.2	0.4	0.4
2	0.2	0.2	0.2	0.2	0.4	0.4

Similarly, subgraph 2 in Fig. 10 can also obtain results similar to Tab. 9-11. The $I_{BM}(i, j,\ k, G_{2,1})$ values obtained for each social network state k of subgraph 2 are shown in Tab. 12-14.

Next, as subgraph 1 and subgraph 2 both contain edges e_5 and e_6, after combining Fig. 8 to Fig. 12, the index values of e_5 and e_6 need to be added. Finally, the indicator values in different social network states of the multiparty social network are obtained in Fig. 8:

TABLE 16. $I_{BM}(i, j, 1)$ **of social network status** $k = 1$.

j i	1	2	3	4	5	6
0	0	0	0	0	0	0
1	0.8	0.8	0.8	0.8	1.6	1.6
2	0.3	0.3	0.3	0.3	0.6	0.6

TABLE 17. $I_{BM}(i, j, 2)$ **of social network status** $k = 2$.

j i	1	2	3	4	5	6
0	0	0	0	0	0	0
1	0	0	0	0.	0	0
2	0.5	0.5	0.5	0.5	1	1

TABLE 18. **Values of** $S(i, k)$.

k i	1	2	3	4	5	6
0	0.63	0.63	0.63	0.63	0.85	0.85
1	0.50	0.50	0.50	0.50	0.76	0.76
2	0.58	0.58	0.58	0.58	0.82	0.82

Finally, the multiparty social network's indicated values $S(i, k)$ of Fig. 8 are shown in Tab. 18:

According to the results of the sensitivity index $S(i, k)$, for the social network state $k = 0, 1, 2$, the sensitivity index is sorted as follows:

$$S(1,\ k)=S(2,\ k)=S(3,\ k)=S(4,\ k) < S(5,\ k)=S(6,\ k).$$

That means, whether the system is in state 0, state 1 or state 2, the sensitivities of e_5 and e_6 are equal, and the largest, e_1, e_2, e_3 and e_4 are equal and have the smallest value.

VI. CONCLUSION

Social networks are usually very complex and may consist of multiple parties. Additionally, trust always has properties of being diversified and asymmetric. Binary and symmetrical system models are inadequate for modeling and analyzing some social networks exhibiting multiple states. This paper generalizes the research object from two-state social networks to multiple states since the trust grades for people in real may have multiple levels, including the research for importance and sensitivity of two-sided and multisided multistate social networks. Trust sensitivity indexes are derived for two classes of social network systems, including two-party multistate and multiparty multistate social networks. As demonstrated through numerical examples, the formulas derived in this work can be used to evaluate trust sensitivity and identify which direct link in the social network contributes the most to a party trust relationship or which direct link is the weakest link.

As one possible direction of future work, we will extend the proposed model to consider large relational networks and other types of social network structures.

REFERENCES

[1] S. Wasserman and K. Faust, "Social network analysis in the social and behavioral sciences," in *Social Network Analysis: Methods and Applications*. London, UK: Cambridge Univ. Press, 1994, pp. 1–27.

[2] L. Xing, H. Wang, C. Wang, and Y. Wang, "BDD–based two–party trust sensitivity analysis for social networks," *Int. J. Secur. Netw.*, vol. 7, no. 4, pp. 231–242, Jan. 2012.

[3] M. Deutsch, "Cooperation and trust: Some theoretical notes," in *Proc. Nebraska Symp. Motivat.*, 1962, pp. 275–319.

[4] A. Jøsang, R. Hayward, and S. Pope, "Trust network analysis with subjective logic," in *Proc. 29th Australasian Comput. Sci. Conf.*, Darlinghurst, OX, Australia, 2006, pp. 85–94.

[5] J. A. Golbeck, "Computing and applying trust in Web-based social networks," Ph.D. dissertation, Dept. Comput. Sci., Maryland Univ. Park, Maryland, MD, USA, 2005.

[6] P. Avesani, P. Massa, and R. Tiella, "A trust-enhanced recommender system application: Moleskiing," in *Proc. ACM Symp. Appl. Comput.*, Santa Fe, NM, USA, 2005, pp. 1589–1593.

[7] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust," in *Proc. 13th Int. Conf. World Wide Web*, New York, NY, USA, 2004, pp. 403–412.

[8] W. Jiang, J. Wu, F. Li, G. Wang, and H. Zheng, "Trust evaluation in online social networks using generalized network flow," *IEEE Trans. Comput.*, vol. 65, no. 3, pp. 952–963, Mar. 2016.

[9] G. Wang, W. Jiang, J. Wu, and Z. Xiong, "Fine-grained feature-based social influence evaluation in online social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2286–2296, Sep. 2014.

[10] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," in *Proc. 12th Int. World Wide Web Conf.*, Budapest, Hungary, 2003, pp. 640–651.

[11] Y. Katz and J. Golbeck, "Social network-based trust in prioritized default logic," in *Proc. 21st Nat. Conf. Artif. Intell.*, Boston, MA, USA, 2006, pp. 1345–1350.

[12] U. Kuter and J. Golbeck, "Sunny: A new algorithm for trust inference in social networks using probabilistic confidence models," in *Proc. 22nd Nat. Conf. Artif. Intell.*, Vancouver, BC, Canada, 2007, pp. 1377–1382.

[13] G. Liu, Q. Chen, Q. Yang, B. Zhu, H. Wang, and W. Wang, "OpinionWalk: An efficient solution to massive trust assessment in online social networks," in *Proc. IEEE Conf. Comput. Commun.*, Atlanta, GA, USA, May 2017, pp. 1–9.

[14] M. Richardson, R. Agrawal, and P. Domingos, "Trust management for the semantic Web," in *Proc. 2nd Int. Conf. Comput. Electr. Eng.*, Washington, DC, USA, 2009, pp. 3–6.

[15] C.-N. Ziegler and G. Lausen, "Spreading activation models for trust propagation," in *Proc. IEEE Int. Conf. E-Technol., E-Commerce E-Service*, Washington, DC, USA, Mar. 2004, pp. 83–97.

[16] D. Quercia, S. Hailes, and L. Capra, "Lightweight distributed trust propagation," in *Proc. 7th IEEE Int. Conf. Data Mining*, Omaha, NE, USA, Oct. 2007, pp. 282–291.

[17] C.-W. Hang, Y. Wang, and M. P. Singh, "Operators for propagating trust and their evaluation in social networks," in *Proc. 8th Int. Conf. Auto. Agents Multiagent Syst.*, Budapest, Hungary, 2009, pp. 1025–1032.

[18] L. Xing and J. B. Dugan, "Analysis of generalized phased-mission system reliability, performance, and sensitivity," *IEEE Trans. Rel.*, vol. 51, no. 2, pp. 199–211, Jun. 2002.

[19] S. Si, M. Liu, Z. Jiang, T. Jin, and Z. Cai, "System reliability allocation and optimization based on generalized Birnbaum importance measure," *IEEE Trans. Rel.*, vol. 68, no. 3, pp. 831–843, Sep. 2019.

[20] X. Zhao, K. N. Al-Khalifa, A. M. Hamouda, and T. Nakagawa, "Age replacement models: A summary with new perspectives and methods," *Rel. Eng. Syst. Saf.*, vol. 162, pp. 95–105, May 2017.
[21] Y. Zeng, Y. Sun, L. Xing, and V. Vokkarane, "A study of online social network privacy via the TAPE framework," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1270–1284, Oct. 2015.
[22] L. Xing and S. V. Amari, "Effective component importance analysis for the maintenance of systems with common-cause failures," *Int. J. Rel., Qual. Saf. Eng.*, vol. 14, no. 5, pp. 459–478, 2017.
[23] Y. Karabulut, J. C. Mitchell, P. Herrmann, and C. D. Jensen, *Trust Management II*. New York, NY, USA: Springer, 2008.
[24] X. Jia, J. Shen, F. Xu, R. Ma, and X. Song, "Modular decomposition signature for systems with sequential failure effect," *Rel. Eng. Syst. Saf.*, vol. 189, pp. 435–444, Sep. 2019.
[25] X. Jia, J. Shen, and R. Xing, "Reliability analysis for repairable multistate two-unit series systems when repair time can be neglected," *IEEE Trans. Rel.*, vol. 65, no. 1, pp. 208–216, Mar. 2016.
[26] S. B. Akers, "Binary decision diagrams," *IEEE Trans. Comput.*, vol. C-27, no. 6, pp. 509–516, Jun. 1978.
[27] R. E. Bryant, "Graph-based algorithms for Boolean function manipulation," *IEEE Trans. Comput.*, vol. C-35, no. 8, pp. 677–691, Aug. 1986.
[28] D. M. Miller, "Multiple-valued logic design tools," in *Proc. 23rd Int. Symp. Multiple-Valued Logic*, Sacramento, CA, USA, May 1993, pp. 2–11.
[29] L. Xing and S. V. Amari, "Fundamentals of binary decision diagrams," in *Binary Decision Diagrams and Extensions for system Reliability Analysis*. Beverly, MA, USA: Scrivener, 2015.
[30] M. Rausand and A. Høyland, "System reliability theory: Models, statistical methods, and applications," *Technometrics*, vol. 38, no. 1, pp. 79–80, 2004.

XUEYING SONG is currently pursuing the master's degree with the College of Science, Minzu University of China, in 2017. She is a member of the Reliability Branch of Operations Research Society of China. Her research interests include stochastic modeling and reliability engineering.

XUJIE JIA received the Ph.D. degree in management science and engineering from the Beijing Institute of Technology, in 2019. She is currently an Associate Professor with the College of Science, Minzu University of China. Her main research interests include stochastic modeling, quality and reliability engineering, and applications of probability and statistics.

NANNAN CHEN received the M.S. degree in mathematical statistics from the Minzu University of China. Her research interests include stochastic modeling and reliability engineering.