TRUST ASSESSMENT IN ONLINE SOCIALNETWORKS

[1]Sreedhar Reddy, [2] Saipriya Bethi, [3]Muni Sekhar Velpuru, [4]Ramesh Karnati

[1,2]Student, [3,4]Associate Professor, [1, 2,3]Department of Information Technology,
[4]Department of Computer Science & Engineering,
[1, 2, 3,4]Vardhaman College of Engineering,
Hyderabad, Telangana, India

***Abstract*—Assessing trust in Online Social Networks (OSN)is critical for many applications such as online marketing and network security. However, it is a challenging problem due tothe difficulties of dealing with complex social network structures and making accurate assessment in these structures. To meetthese challenges, we model confidence by proposing a three- valued subjective logic model (3VSL). 3VSL correctly formulatesthe uncertainties present in confidence, and is thus able to compute confidence in arbitrary graphs. We have theoretically demonstrated the ability of 3VSL on the basis of a Dirichlet- Categorical (DC) distribution and its validity in arbitrary OSN topologies. Based on the 3VSL model, we also design the Trust Assessment (AT) algorithm to accurately calculate the trust between any connected OSN users. We validate 3VSL againsttwo real-world OSN data sets: Advogato and Pretty Good Privacy(PGP). Experimental results indicate that 3VSL can accurately model trust between any pair of indirectly connected Advoga to and PGP users.**

Index Terms—Trust Assessment, Online Social networks, Three-valued Subjective Logic, Trust Model.

INTRODUCTION:

Motivation and Problem Statement:

Online social networks (OSNs) are one of the most visited places on the Internet. OSN not only helps people strengthen their social connections with known friends, but also expands their social circles to friend friends that they may not have known before. Trust is the driving force behinduser interaction with OSN and is important for almost allOSN applications. For example, trust in recommended or crowdsourced systems can help identify [1] trusted opinions and users [2]. Trust is used in online marketing applications [3]to identify trusted sellers. Active Friendship Building System [4] allows you to discover potential friendships through trust. In the wireless network domain, trust helps cellular devices find trusted peers to transfer data [5, 6]. In the security domain, trust is considered an important indicator for detectingmalicious users and websites [7, 8, and 9]. Given the application above, the mysterious question is how much one user cantrust another in OSN. This paper addresses the basic issuesof OSN reliability assessment. Given the OSN, how to model and calculate the trust between users? Trust is traditionally considered a reputation or the possibility that the user is benign. In online marketing, users evaluate each other based ontheir interactions, so user trust can be derived from aggregated However, in the network security domain, the trust ofa particular user is defined as the probability that that userwill be successful in the in the future. Based on the resultsof previous studies [10, 11], trust is defined as the probability that a trustee will behave as expected from the trustee’s point of view. Here, both the trust and the trustee are regular usersof OSN, and the trust wants to know how reliable the trustee is. Through this general definition of trust, a wide range of applications.

To solve problem P1, we propose a three-valued subjective logic model (3VSL) that can accurately model reliability based on user interactions in OSN. 3VSL is based on a subjective logic (SL) model [27]. However, it is significantly different from the SL. Instead of defining confidence as a binary value in SL, 3VSL treats it as a cubic value (i.e. trust, doubt, and uncertainty). In other words, users in OSN canbe trusted, untrusted, or untrusted. Therefore, the probabilityof a user being trustworthy can be modeled by the Dirichlet Categorical (DC) distribution that is characterized by three parameters, and. Here, represents the number of positive interactions/evidence that supports the user is trust worthy.For example, we observed that the user behaved as expected times in the past. Denotes the amount of negative evidence indicating the user is not trustworthy. Is the amount of neutral evidence that neither supports nor opposes the useris trustworthy? The reason for introducing state of uncertainty in 3VSL is that it can accurately model reliable transmissionin OSN.

In the process of spreading beliefs, some evidence measured in + becomes “distorted” and becomes uncertain evidence, measured in. Distorted evidence is common inreliability assessments, however, it is completely eliminatedin SL. To solve problem P2, we propose a reliability calculation algorithm, called Assess Trust (AT), based on 3VSL model. AT decomposes the subsegment between trustees and trustees into a parse tree, providing the correct ordering oftrust transmission application and trust merging to calculate indirect trust between trustees. Trustee and trustee. Here, trust propagation and fusion are modeled by two basic operations: discounting and combining operations. Leveraging the proper-ties of 3VSL, AT is proven to be able to accurately compute the trustworthiness between any two users connected withinan OSN. Because 3VSL uses a probability distribution to describe whether a user is trustworthy, AT offers more accurate trust assessment, compared to the topology and graph based solutions. On the other hand, while AT makes use of the socialconnections between the trustor and trustee to compute their trust, it outperforms the probability based models that areonly applicable for direct trust. Experiment results indicatethat AT achieves the best accuracy of trust assessment inOSNs. Specifically, AT achieves the F1 scores of 0.7 and0.75, in trust assessment, using the Advogato and Pretty GoodPrivacy (PGP) datasets, respectively. AT can also be used to rate users based on how trustworthy they are. We measure the accuracy of the rating results using Kendall’s tau coefficient, which is related to the underlying truth rating. The results of the experiments showed that AT gave an average Kendall tau coefficient of 0.73 and 0.77 in Advogato and PGP, respectively.

Technical challenges and solutions:

The first technical challenge is that 3VSL needs an accuratemodel for spreading and integrating trust into OSNs. Thisis a challenge because the prevalence of trust in OSNs ispoorly understood, although it has been widely adopted bythe research community. We address this challenge by using an opinion to represent confidence and to model confidence spread based on a DC distribution and several generally accepted assumptions. The second technical challenge is that 3VSL must be able to operate on OSNs with non-serial parallel network architectures. This presents a challenge because the only operations allowed in trust assessment are trust propagation and trust consolidation. However, these two processes require that the network topology be either serial and/or parallel. This requirement cannot be met in online social networks in the real world. We meet this challengeby distinguishing between distorted and original views. For example, if Alice trusts Bob and Bob trusts Charlie, then Al- ice's opinion of Bob is called the distorted opinion, and Bob's opinion of Charlie is the original opinion. We find that originalopinions can only be combined once, but distorted opinions can be combined any number of times. This finding lays the foundation for the proposed recursive confidence evaluation algorithm. The third technical challenge is that 3VSL needsto handle social networks with arbitrary structures, even with sessions. This is a challenge because it is impossible to test 3VSL in all possible network architectures. We address this challenge by proving that 3VSL operates mathematically in random networks. The evidence relies on the characteristicsof the Dirichlet distribution and the characteristics of different opinions in the process of calculating confidence. Ultimately, the EvalTrust algorithm is designed to calculate trust between any OSN users.

RELATED WORK:

A. Trust Models in OSNs:

Trust is built on social connections between users and the way trust is modeled in online social networks has attracted more attention in recent OSN studies. Several studies existon trust models in social networks. The models proposed in these works can be classified as topological-based, PageRank- based, probabilistic-based, and based on subjective logic. In this section, we briefly describe this work. Topology-based trust models treat a trust social network as a graph, where an edge represents a trust relationship between two neighboring nodes. The advantage of these methods is that they take advantage of random walking for reliability assessment, and thus can be easily applied in large-scale NSOs. By analyzing the network topology, the works of [7], [8], [15], [16] can identify unreliable nodes in OSN. Their basic idea is to identify untrusted nodes by distinguishing untrusted regions from trusted regions in the network. Specifically, they play randomly from a trustee and evaluate the probability of hitting a trustee. A low probability indicates that the administratoris not in the trusted zone and vice versa. Then people start modeling indirect trust by looking at trust values among users.In [34], the trust relationship between two users is considered as a probabilistic value. All users and their associated trust relationships form a graph. Then, the trust inference problem indirectly becomes a network accessibility problem. In [11],a reliable network is considered to be a resistive networkwhere the resistance of each edge is derived from edge reliability. In [12], [13], for a trusted network, a depth-first search algorithm is used to calculate the reliability between two users. A Reliability Model based on PageRank uses the PageRank algorithm to calculate the relative trustworthinessof interested users. For example, the Eigen Trust algorithm, proposed in a peer-to-peer system, starts from a peer andsearches for trusted peers based on some rules. It moves from one peer to another with a probability proportional tothe confidence score of the other peer, i.e. the higher theconfidence score, the higher the probability of migration. Thisway, Eigen Trust is more likely to reach trusted peers. Then, the relative reliability of websites is investigated in to identify spam my sites. The Trust Rank algorithm proposed in [17] againuses the "PageRank" algorithm to rank the trustworthiness of web pages. Eigen Trust and Trust Rank can be considered a variation of the PageRank algorithm, a well-known solution for assigning importance scores to pages on the Internet. However, these algorithms only generate trust rankings, ratherthan absolute peer/page trust values. Probability-based trust models treat direct confidence as a probability distribution,in which the trustor uses the trustee's past interactions and observations to build a model of certainty. Approximation to the trustee's future behavior. The advantage of these models isthat reliability can be accurately calculated based on a variety of statistical and probabilistic techniques, including hidden Markov series, maximum likelihood estimation, etc.

The main limitation of the SL model is that uncertaintyin confidence is considered constant, however, uncertainty in confidence opinion will increase as it spreads from one userto another. To address this issue, we propose three-valuedSubjective logic (3VSL) to model trust between users in OSN, by redefining trust uncertainty. Designing a 3VSL model isa challenging task as the spread of trust in OSNs is poorly understood, despite its widespread use in many applications. We address this challenge by modeling confidence as an opin-ion, and representing the probability distribution over three different cases, i.e., trustworthy, untrustworthy and uncertain. By investigating how these opinion states change during trust deployment, we redesign the trust discounting process. Takingadvantage of the Dirichlet distribution, we also redesigned the integration. Furthermore, we discover a mechanism for howto properly apply opinion processes to trust assessment within OSN, which leads to the design of the EvalTrust algorithm.

A. Existing system:

Confidence has been extensively studied in the fields of psychology, sociology, and management. Rousseau summarized an accepted definition of trust in [10], based on a review ofthe interdisciplinary literature:" Confidence is a psychologicalstate that includes the intention to accept vulnerability based on positive expectations of another person's intentions or behaviors." Despite the different definitions of trust, it issimilar to Rousseau's definition, i.e. it can be concluded that trust consists of two parts: expectancy and vulnerability. Whilethe former indicates the possibility that the trustee will actas expected, and the latter shows the trustee's desire to relyon the trustee. Specifically, the word vulnerability emphasizesthe trustee's concerns about the uncertainty [32, 33] of the trustee's future behaviors. The definition of trust in this letter is inspired by the studies mentioned above, and we define trustas the probability that the trustee will act as expected, fromthe trustee's viewpoint. Although trust and reputation are often confused, they are two different concepts. Previous works have identified positive relationships between reputation and trust. However, reputation does not equate to trust. According to thedefinition from Merriam-Webster Dictionary and Wikipedia, reputation is the popular opinion people have about someone or something, i.e. the general or personal quality as seen or judged by people in general. In essence, reputation comesfrom public opinion and public opinion. However, trust comesfrom individual opinions, i.e. from custodian to custodian withan emphasis on personal interactions. On the other hand, reputation is a summary of past events while trust is the intent and expectations in the future. How to build trust among users in OSN has attracted a lot of attention in recent years. Existing confidence models can be categorized intofour groups: topology-based models, pagination-based models,probability-based models, and subjective logic-based models. In this section, we briefly present these works. There is less security on outsourced data due to the lack of probabilistic interpretation of trust on the data. Direct trust consists of the trustee's direct interactions with the trustee while indirect trust is not inferred from the recommendations of others.

PROPOSED SYSTEM:

The system proposes an algorithm for evaluating confidence,called confidence assessment (AT), based on the 3VSL model.The AT algorithm analyzes the network between the trustee and the trustee as a parsing tree that provides the correct order to apply trust operations to the indirect trust between the two users. Here, the trust operations available in the trust account are the discount operation and the addition operation. Taking advantage of these two processes, AT is proven to be able to accurately calculate trust between any connected OSN users. Because 3VSL adequately handles confidence uncertainty, ATdelivers more accurate confidence ratings, compared to chassisand graphics based solutions. On the other hand, since ATaims to calculate indirect trust between users, it outperforms probability-based models that focus only on direct trust. The trial results show that the assistive technology yields the most accurate confidence assessment results. Specifically, AT achieves F1 scores of 0.7 and 0.75, using the Advogato and Pretty Good Privacy (PGP) data sets, respectively. AT can rankusers based on their trust values. We measure the accuracy of the ranking results using Kendall's tau coefficients. Experimentresults show that, on average, AT presents Kendall's tau coefficient of 0.73 and 0.77, in Advogato and PGP, respectively.

Advantages:

Rather than analyzing the entire structure of a social network, solutions based on PageRank are inspired by theassumption that trustworthy users are likely to have moreconnections than other users. In contrast to the above model which treat confidence as binary or real numbers, the probability-based model considers confidence as a probability, that is, the probability that the trustee is trustworthy. Confidence models based on probability usually represent confidence as a probability distribution.

IMPLEMENTATION:

Based on 3VSL and inference and summation operations, we design a reliability evaluation algorithm (TA) to perform reliability assessment in arbitrarily structured social networks. Here we treat the social network as a two-way graph (TTDG) where administrators and administrators are represented respectively. It is clear that the trustee and the trustee must be different users as the trustee will never establish the sametrust. Since TTDG does not have to be an a.c. directed graph, there can be cycles in the network. To ensure that AT works inrandom topologies, we need to first demonstrate AT's ability to handle non-sequential parallel network architectures, which is difficult because the operations the only operations available for calculating confidence are the subtraction and additionoperations. The transfer/merge process requires the network architecture to be serial/parallel. We address this challengeby distinguishing distorted opinion from original opinion in propagating trust. For example, if a trusts B and B trustsC, then A's opinion of B is called a distorted opinion, andB's opinion of C is the original opinion. We found thatin trust merge, original comments can only be used once, but distorted comments can be used multiple times. Indeed,a distorted opinion reduces the value of certain evidence and makes it uncertain, i.e. it does not change the total amount of evidence. On the other hand, when the two original (reduced) opinions are combined, the total amount of evidence in the resulting opinion increases. Furthermore, we show that AT acts in arbitrary TTDGs. This is challenging because it isnot possible to test AT in all possible network architectures. We address this challenge by demonstrating that AT works in random networks.

CONCLUSION & FUTURE WORK:

Based on 3VSL and inference and summation operations, we design a reliability evaluation algorithm (TA) to perform reliability assessment in arbitrarily structured social networks. Here we treat the social network as a two-way graph (TTDG) where administrators and administrators are represented re- spectively. It is clear that the trustee and the trustee must be different users as the trustee will never establish the sametrust. Since TTDG does not have to be an a.c. directed graph, there can be cycles in the network. To ensure that AT works inrandom topologies, we need to first demonstrate AT's ability to handle non-sequential parallel network architectures, which is difficult because the operations the only operations available for calculating confidence are the subtraction and additionoperations. The transfer/merge process requires the network architecture to be serial/parallel. We address this challengeby distinguishing distorted opinion from original opinion in propagating trust. For example, if A trusts B and B trusts C, then A's opinion of B is called a distorted opinion, andB's opinion of C is the original opinion.. We found thatin trust merge, original comments can only be used once,but distorted comments can be used multiple times.

Indeed,a distorted opinion reduces the value of certain evidence and makes it uncertain, i.e. it does not change the total amount of evidence. On the other hand, when the two original (reduced) opinions are combined, the total amount of evidence in the resulting opinion increases. Furthermore, we show that AT acts in arbitrary TTDGs. This is challenging because it isnot possible to test AT in all possible network architectures. We address this challenge by demonstrating that AT works in random networks. For papers published in translation journals, please give the English citation first, followed by the original foreign-languagecitation [6].

REFERENCES:

[1] Anirban Basu, Jaideep Vaidya, Juan Camilo Corena, Shinsaku Kiy-omoto, Stephen Marsh, Guibing Guo, Jie Zhang, and Yutaka Miyake. Opinions of people: Factoring in privacy and trust. SIGAPP Appl. Comput. Rev., 14(3):7–21, September 2014.

[2] Jun Zou and Faramarz Fekri. A belief propagation approach for detecting shilling attacks in collaborative filtering. In Proceedings of the 22Nd ACM International Conference on Conference on Informa- tion 38;Knowledge Management, CIKM ’13, pages 1837–1840, New York, NY,USA, 2013. ACM.

[3] Paul Resnick, Ko Kuwabara, Richard Zeckhauser, and Eric Fried- man. Reputation systems. Communications of the ACM, 43(12):45– 48, 2000.

[4] De-NianYang,Hui-JuHung,Wang-ChienLee,andWeiChen.Max- imizing acceptance probability for active friending in online social networks.In Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD ’13, pages 713–721, NewYork, NY, USA, 2013. ACM.

[5] Tiffany Hyun-Jin Kim, Payas Gupta, Jun Han, Emmanuel Owusu, JasonHong, Adrian Perrig, and Debin Gao. Oto: Online trust oracle for user- centric trust establishment. In Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS ’12, pages 391–403, New York, NY, USA, 2012. ACM.

[6] Lu Shi, Shucheng Yu, Wenjing Lou, and Y.T. Hou. SybilShield: An agent-aided social network-based sybil defense among multiple com- munities. In INFOCOM, 2013 Proceedings IEEE, pages 1034– 1042, 2013.

[7] Haifeng Yu, P.B. Gibbons, M. Kaminsky, and Feng Xiao. Sybil- Limit: Anear-optimal social network defense against sybil attacks. Networking, IEEE/ACM Transactions on, 18(3):885–898, June 2010.

[8] HaifengYu,MichaelKaminsky,PhillipB.Gibbons,andAbrahamD. Flaxman. Sybilguard: Defending against sybil attacks via socialnetworks. IEEE/ACM Trans. Netw., 16(3):576–589, June 2008.

[9] Denise M Rousseau, Sim B Sitkin, Ronald S Burt, and Colin Camerer. Not so different after all: A cross-discipline view of trust. Academy of management review, 23(3):393–404, 1998.

[10] David Gefen, Elena Karahanna, and Detmar W. Straub. Trust and tamin online shopping: An integrated model. MIS Q., 27(1):51–90, March 2003.

[11] Diego Gambetta. Trust: Making and Breaking Cooperative Rela- tions, volume 52. Blackwell, 1988.

[12] D Harrison McKnight, Vivek Choudhury, and Charles Kacmar. Devel- oping and validating trust measures for e-commerce: An in- tegrative typology. Information systems research, 13(3):334–359, 2002.

[13] Rino Falcone and Cristiano Castelfranchi. Social trust: A cognitive approach. In Trust and deception in virtual societies, pages 55–90. Springer, 2001.

[14] TK Ahn and Justin Esarey. A dynamic model of generalized social trust.Journal of Theoretical Politics, 20(2):151–180, 2008.

[15] Larue Tone Hosmer. Trust: The connecting link between organi- zationaltheory and philosophical ethics. Academy of management Review, 20(2):379–403, 1995.

[16] Jomi F Hu bner, Emiliano Lorini, Andreas Herzig, and Laurent Ver- couter. From cognitive trust theories to computational trust. In Proceed- ings of the 12th International Workshop on Trust in Agent Societies, Budapest, Hungary, volume 10, pages 2009–11. Citeseer, 2009.

[17] Wei Wei, Fengyuan Xu, C.C. Tan, and Qun Li. Sybildefender: Defend against sybil attacks in large social networks. In INFOCOM, 2012 Proceedings IEEE, pages 1951–1959, March 2012.