A Robust Approach to Finding Trustworthy Influencer in Trust-Oriented E-Commerce Environments

Feng Zhu[1,2], Guanfeng Liu[1,2(✉)], Yan Wang[3], Mehmet A. Orgun[3], An Liu[1,2], Zhixu Li[1,2], and Kai Zheng[1,2]

[1] School of Computer Science, Soochow University, 215006 Suzhou, China
{gfliu,anliu,zhixuli,zhengkai}@suda.edu.cn
[2] Collaborative Innovation Center of Novel Software Technology and Industrialization, Nanjing, Jiangsu, China
[3] Department of Computing, Macquarie University, Sydney, NSW 2102, Australia
{yan.wang,mehmet.orgun}@mq.edu.au

Abstract. With the recognition of the significance of OSNs (Online Social Networks) in the recommendation of services in e-commerce, there are more and more e-commerce platform being combined with OSNs, forming *social e-commerce*, where a participant could recommend a product to his/her friends based on the participant's corresponding purchasing experience. For example, at Epinions, a buyer could share product reviews with his/her friends. In such platforms, a buyer providing lots of high quality reviews is very likely to influence many potential buyers' purchase behaviours. Such a buyer is believed to have *strong* social influence. However, dishonest participants in OSNs can deceive the existing social influence evaluation models, by mounting attacks, such as *Constant* (Dishonest advisors constantly provide unfairly positive/negative ratings to sellers.) and *Camouflage* (Dishonest advisors camouflage themselves as honest advisors by providing fair ratings to build up their trustworthiness first and then gives unfair ratings.), to obtain fake strong social influence. Therefore, it is crucial to devise a robust social influence evaluation model that can defend against attacks and deliver more accurate social influence evaluation results. In this paper, we propose a novel robust Trust-Aware Social Influencer Finding, *TrustINF*, method that considers the evolutionary trust relationship and the variations of historical social influences of participants, which can help deliver more accurate social influence evaluation results in social e-commerce. Our experiments conducted on four real social network datasets validate the effectiveness and robustness of our proposed method, which is greatly superior to the state-of-the-art method.

1 Introduction

1.1 Background

On trust-oriented e-commerce platforms, like Epinions (epinions.com), after a transaction, a buyer can provide a review to introduce the quality of the

Q.Z. Sheng et al. (Eds.): ICSOC 2016, LNCS 9936, pp. 387–401, 2016.
DOI: 10.1007/978-3-319-46295-0_24

purchased product and the experience of the transaction. This review is visible to other buyers, and is much valuable to their decision-making of purchasing. In addition, a buyer can rate the existing reviews given by others as *Not Helpful*, *Somewhat Helpful*, *Helpful*, or *Very Helpful* based on his/her own experiences [1]. If a buyer usually provides *Very Helpful* product reviews in a specific domain, like Digital Cameras, his/her recommendation is believed to be trustworthy in that domain. As indicated in the studies of *Social Psychology* [2] and *Computer Science* [3–5], a buyer is very likely to make a purchase decision following the recommendations (product reviews) given by trustworthy buyers. Such trustworthy buyers posses strong influences and can impact many buyers' purchase behaviours in a specific domain. These trustworthy buyers are called the *advisors* of those participants who trust their product reviews.

1.2 The Problem

In e-commerce environments, a buyer can write product reviews and rate others' reviews freely, and thus the product review scheme is highly vulnerable to some typical attacks [1]. For example, in order to obtain a strong influence, a dishonest advisor can cheat the product review system via some typical attacks, such as *Constant*[1] and *Camouflage*[2] [6], by (1) recommending a low quality product, and/or (2) providing an unfair review to a high quality product, each of which severely harms the benefits of both potential buyers and sellers. The problem of unfair rating becomes more and more concerned by not only industrial circles but also academic circles in this filed. Plenty of unfair ratings exist in the reviews of products, which significantly affect the decision-making of buyers [7,8].

In the literature, the existing influence evaluation methods mainly focus on studying the influence maximization under the popular linear threshold (LT) model and independent cascade (IC) model [9], and evaluating social influence through the process of information diffusion [10]. However, they do not apply any strategies to defend against the afore-mentioned typical attacks, and thus the existing models might recommend a participant as an advisor who has obtained the fake strong social influence by cheating the review systems via the above mentioned typical attacks. Some methods have been proposed to defend against collusive [11] or spamming rating attacks [12], which however cannot be directly applied in defending against the typical *Camouflage* and *Constant* attacks in trust-oriented e-commerce environment. The following *Example* 1 illustrates the process of the typical Camouflage attack in e-commerce platforms.

Example 1. *Fig. 1 depicts a trust-oriented e-commerce environment, which contains two sellers* S_1 *and* S_2 *and three buyers* B_1 *to* B_3*. Firstly,* B_1 *and* B_3 *bought the same product (such as digital camera) from* S_1*, so there exist the* transaction relationships *between* B_1 *and* S_1*, and between* B_3 *and* S_1*, respectively (represented by* arrows with dashed lines *in Fig. 1). Next, suppose both* B_1

[1] Dishonest advisors constantly provide unfairly positive/negative ratings to sellers.
[2] Dishonest advisors camouflage themselves as honest advisors by providing fair ratings to build up their trustworthiness first and then gives unfair ratings.

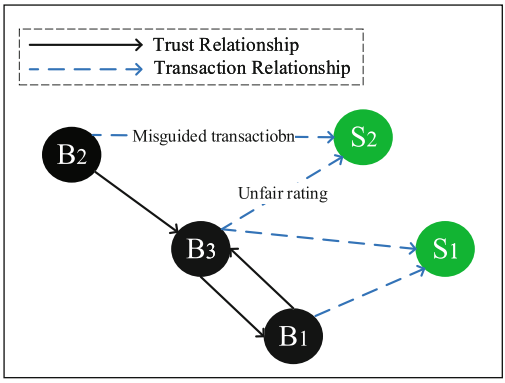


Fig. 1. The camouflage attack

and B_3 wrote a review for the camera sold by S_1, and they find that their purchase experiences are similar with each other. Then B_1 and B_3 trust each other, and thus there exist trust relationships *between B_1 and B_3 (represented by* arrows with solid lines *in Fig. 1). Finally, B_2 regards the review of B_3 is* Very Helpful*, then a trust relationship is established between them. In such a situation, if B_2 wants to buy a new camera, B_3's review has a strong influence on B_2's decision making. But suppose B_3 wrote an unfair positive review to the camera sold by S_2, whose camera has a low quality. If B_2 wants to buy a new digital camera, naturally B_2 would choose the camera sold by S_2 because B_2 trusts B_3. Then B_2 makes a wrong decision misled by B_3's dishonest action. In such a scenario, B_3 is a* Camouflage *attacker who establishes fake trustworthiness first and then misleads other buyers.*

The above discussed typical attacks widely exist in trust-oriented e-commerce, which leads to severe deviation of the reliability of the recommendations [6]. This motivates us to develop a robust influence evaluation method to accurately find the participants who have real strong influence under the typical attacks mounted by dishonest buyers in e-commerce environments.

1.3 Contributions

The main contributions of this paper are summarized as follows:

- We propose a novel Trustworthy Influencer Finding method *TrustINF* based on the evolutionary trust model [6] and the variations of historical influences of participants, which can measure the attack probability for each buyer, and defend against the typical attacks, *Constant* and *Camouflage*.
- To the best of our knowledge, this is the first work that defends *Camouflage* and *Constant* attacks in influence evaluation. The proposed *TrustINF* approach is based on *Skyline* [13] and its time complexity achieves $\mathcal{O}(n^2)$, where n is the number of buyers in e-commerce environments.

– We have conducted experiments on the four real social e-commerce datasets, i.e., *Epinions*, *Slashdot*, *Amazon* and *BeerAdvocate*. The average *Attacker Identification Ratios* of our TrustINF under *Constant* attack and *Camouflage* attack achieve 66.33 % and 81.33 % respectively. On average, our *Trust-IMM* can improve the robustness of *IMM* by 85.82 %.

2 Related Work

In the literature, according to different influence problems, we categorize them as influence maximization, individual influence evaluation and the unfair rating identification in influence evaluation.

Influence maximization is to find important applications in viral marketing [14], where a product provider selects K influencers in an OSN and provides them with incentives (e.g., free samples) to accept a new product, excepting the social influence of these influencers can work and attract more potential users. [15] propose an algorithm that has a simple tunable parameter, for users to control the balance between the running time and the influence spread. [16] propose an algorithm IRIE that integrates the advantages of influence ranking (IR) and influence estimation (IE) methods. [17] provide a scalable influence approximation algorithm, Independent Path Algorithm (IPA). [18] investigate a *novelty decay* phenomenon where the influence of a participant decays with the increase of the number of sending the same message to others in OSNs. Then they [19] investigate the effect of the novelty decay in the influence maximization in OSNs. Recently, [20] proposed an algorithm which is based on martingales, a classic statistical tool, to support a larger class of information diffusion model over the existing methods. Moreover, [21] propose a local influence maximization problem. This problem is to find a group of nodes that have the maximal impact on a specified participant. In addition, [22] propose a probabilistic model to discover the latent influence between participants in OSNs.

In individual social influence evaluation, [23] propose an approach, called SoCap, to find influencers in OSNs by using the social capital value. They model the problem of finding influencers in OSNs as a value-allocation problem, where the allocated value denotes the individual social capital. In addition, [24] propose a method to identify influential agents in open multi-agent systems without centralised control and individuals have equal authority. The above existing methods in influence evaluation did not consider any strategies defending against attacks, and thus are vulnerable to the attacks, like *Camouflage* and *Constant*, from dishonest participants.

In order to identify the unfair ratings and improve the robustness of influence evaluation models, some approaches [11,12] have been proposed to defend against the collusive and the spamming rating attacks respectively in trust-oriented e-commerce environments. However, their methods cannot be used directly to defend against the Camouflage and Constant attacks that widely exist in e-commerce environments.

3 Preliminary

3.1 Trust Relationship

In e-commerce environments, a *Trust Relationship* is a relationship between a buyer and an advisor, which illustrate the probability of a buyer who will make the purchase decision based on the reviews of the advisor. This type of trust relationship widely exist in trust-oriented e-commerce, like Epionions, Amazon, FilmTrust, etc. Let $T_{i,j}$ to denote the trust relationship between B_i and B_j.

3.2 Transaction Relationship

In trust-oriented e-commerce environment, a *Transaction Relationship* is a relationship between a buyer and a seller when they have at least one transaction. Let $R_{i,j}$ denote the transaction relationship between B_i and S_j. If B_i have bought m items from S_j, and the rating values to those m items are $r_{i,j} = \{r^1_{i,j}, ..., r^m_{i,j}\}$, $m > 0$, then

$$R_{i,j} = \frac{1}{m} \sum_{k=1}^{m} r^k_{i,j}. \tag{1}$$

3.3 Evolutionary Trust Model

The Evolutionary Trust Model [6] is usually used to cope with unfair rating attacks from dishonest advisors. By using this model, if a buyer finds the real transactional experience is different with the reviews given by an advisor, the buyer could evolve his/her trust relationships to absorb the advisors whose reviews better match the buyer's purchase experience and distrust the previous advisor whose review is not recognized by the buyer. The following Example 2 illustrates the evolutionary process.

Example 2. *In Fig. 2, suppose there is a low rating given by* B_2 *to* S_2 *(i.e.,* $R_{2,2} = 0.2$*), which is quite different with* B_3*'s review with* $R_{3,2} = 1.0$*. Then* B_2 evolves *his/her trust relationships to form a new trust relationship* $T_{2,1} = 1.0$ *with* B_1 *as* B_1*'s review with* $R_{1,1} = 0.2$ *matches* B_2*'s purchase experience. Meanwhile* B_2 *removes the trust relationship with* B_3*. Finally,* B_1 *becomes a new advisor of* B_2*. This process is called the* Trust Evolution.

The below fitness function in Eq. (2) is used for buyers to measure the quality of their trust networks by comparing the two types of derived reputation values of sellers [6].

$$f(VT_i) = \frac{1}{m} \sum_{j=1}^{m} |R_{i,j} - \widetilde{R}_{i,j}| \tag{2}$$

where m is the number of sellers who have been rated by both B_i and B_i's advisors. $\widetilde{R}_{i,j} = \frac{1}{|A(B_i)|} \sum_{k=1}^{|A(B_i)|} R_{k,j}$ denotes the average rating value given

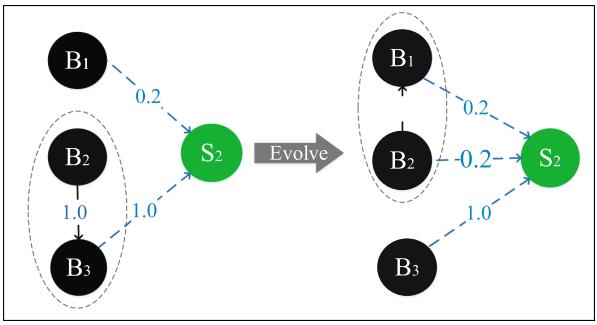


Fig. 2. Evolutionary process

by B_i's advisors to seller S_j. $f(VT_i)$ means that the little difference of ratings given by a buyer and his/her advisors illustrating the high quality of their trust relationship.

The following Eq. (3) is used to measure the difference of trust relationships between two buyers B_i and B_j.

$$\text{diff}(VT_i, VT_j) = \frac{1}{m'} \sum_{k=1}^{m'} |T_{i,k} - T_{j,k}| \tag{3}$$

where m' is the number of both B_i's and B_j's advisors; it reflects the difference between the trust relationships of B_i and B_j. The less the value of $\text{diff}(VT_i, VT_j)$ the less the difference of the trust value from B_i and B_j to their common advisors.

Equation (4) is used to measure the difference of fitness.

$$\text{diff}(f(VT_i), f(VT_j)) = |f(VT_i) - f(VT_j)| \tag{4}$$

In evolutionary process, a function $\delta(\cdot)$ is used to judge the compatibility of new trust relationship resource and calculated as follows:

$$\begin{aligned} \delta(VT_i, VT_j) =& (\text{diff}(VT_i, VT_j) - 0.5) \\ & \times (\text{diff}(f(VT_i), f(VT_j)) - 0.5) \end{aligned} \tag{5}$$

Here, we set threshold as 0, only when two buyers B_i and B_j satisfy $\delta(VT_i, VT_j) > 0$.

4 Impact Factors of Influence

With adopting the *Evolutionary Trust Model*, we propose two impact factors which have significant impact on real influence evaluation of participants in e-commerce.

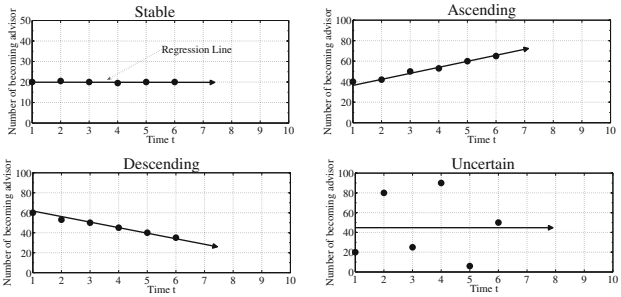


Fig. 3. Four typical cases of FTBA

4.1 Fluctuant Trend of Becoming Advisor (FTBA)

Observing the trend of buyers' trust can largely recognize their reputations [1]. Here, we use the historical data of trust relationships to regress the trend of trust for each buyer, i.e., Fluctuant Trend of Becoming Advisor (FTBA), which illustrates the fluctuant trend of a buyer to become an advisor of a buyer in a certain period. The typical cases of FTBA are depicted in Fig. 3, i.e., "stable", "ascending", "descending" and "uncertain". "stable" means no more other buyers trust the buyer in this period; "ascending" means more and more buyers trust the buyer; "descending" means less and less buyers trust the buyer based on his/her reviews; "uncertain" means the trend of becoming an advisor of the buyer is unclear. We utilize a regression line to model FTBA, whose gradient (denoted as *grad*) and mean distance (denoted as *md*) can measure FTBA well [25].

Let x_i^j denote the number of becoming advisors of B_i at time t_j, and let $(t_s, x_i^s), (t_2, x_i^2), ..., (t_e, x_i^e)$ denote the given data points of B_i from t_s to t_e. In this paper, t_s denotes the start time of the historical transactions and t_e denotes the end time of transactions. Then FTBA can be computed by Eq. (6):

$$y = kt + b \tag{6}$$

where k and b are constants to be determined, and k represents the *grad* value.

Then the shortest distance from point (t_j, x_i^j) to the regression line can be computed by Eq. (7):

$$d_i^j = \frac{x_i^j - b - kt_j}{\sqrt{1+k^2}}. \tag{7}$$

Based on the theory of least squares [26], the sum of squares of the distance can be calculated:

$$S_i^p = \sum_{j=1}^{p} (d_i^j)^2 = \sum_{j=1}^{p} \frac{(x_i^j - b - kt_j)^2}{1+k^2}. \tag{8}$$

Next we minimise the sum of squares of the distance S_i^p with respect to the parameters k and b, with the method of undetermined coefficients. Since the

Algorithm 1. TrustINF

Input: Buyer set B, the parameter sets of all buyers X, the number of buyer set n;
Output: The set of probability of attack of all buyers $P = \{P_i\}$;

$P \longleftarrow \emptyset$;
$N \longleftarrow \emptyset$ /* The dominating numbers of buyers */
$N' \longleftarrow \emptyset$ /* The numbers dominated by other buyers for all buyers */
for *each* X_i *in* X **do**
  for *each* X_j *in* X, $j \neq i$ **do**
    /* Confirming whether X_i dominates X_j, which is based on Definition 1 */
    $m = 0$;
    $flag = false$;
    for $k = 1$ *to* 4 **do**
      if $(X_i^k > X_j^k)$ **then**
        $m++$;
        $flag = true$;
      end if
      if $(X_i^k == X_j^k)$ **then**
        $m++$;
      end if
    end for
    if ($m == 4$ and $flag$) **then**
      N_i++;
      $N_j'++$; /* B_j is dominated by B_i */
    end if
  end for
end for
for *each* B_i *in* B **do**
  $P_i = (N_i' - N_i)/(n-1)$
end for
Return P;

function S_i^p is continuous and differentiable, as we know, based on the method of two variables' function extremum, the minimization point of S_i^p makes the first derivative of function S_i^p be zero, and the second derivative positive, which could be easily proved by Taylor formula for function of two variables [26]. For this purpose, we differentiate S_i^p with respect to k and b, and set the results to zero. Then we can obtain:

$$k = grad_i = (-u - \sqrt{u^2 + 4})/2 \tag{9}$$

and

$$b = \frac{S_f - kS_t}{n}, \tag{10}$$

where $u = \frac{pS_{f2} - S_f^2 + S_t^2 - pS_{t2}}{S_f S_t - pS_{ft}}$, $S_{f2} = \sum_{j=1}^{p} (x_i^j)^2$, $S_f = \sum_{j=1}^{p} x_i^j$, $S_t = \sum_{j=1}^{p} t_j$, $S_{t2} = \sum_{j=1}^{p} t_j^2$ and $S_{ft} = \sum_{j=1}^{p} x_i^j \cdot t_j$.

According to above results, the equation of mean distance can be computed by Eq. (11):

$$md_i = \frac{\sum_{j=1}^{p} |x_i^j - b - kt_j|}{p\sqrt{1+k^2}}. \tag{11}$$

4.2 Fluctuant Trend of Total Trustworthiness (FTT)

Here, we propose another impact factor of influence evaluation, Fluctuant Trend of Total Trustworthiness (FTT), together with FTBA to measure the probability of attack for each buyer. FTT illustrates the fluctuant trend of total trustworthiness which is the total value of trust given by buyers to an advisor from t_s to t_e. We use a regression line to model FTT, which is based on the theory of least squares [26]. The gradient and mean distance of the regression line are denoted as $grad'$ and md' respectively. Let x'^j_i denote the total trust value at time t_j, and $(t_s, x'^s_i), (t_2, x'^2_i), (t_3, x'^3_i)$,...,$(t_e, x'^e_i)$ denote the given data points of B_i from t_s to t_e.

$$x'_i = \sum_{k=1}^{m} T_{k,i} \tag{12}$$

where m is the number of buyers who have trust relationship with B_i.

Then FTT can be computed by using the theory of least squares [26] (i.e., replace (t_j, x_i^j) with (t_j, x'^j_i) in Eqs. (9–11)).

Intuitively, these trends are conducive to indicate the changing process of trust of a buyer and detect the behaviors of the typical attacks. FTT reflects the changing trend of the quality of trust, but FTBA reflects the changing trend of the amount of trust.

Thus, in order to indicate the trust of a buyer more completely, both FTBA and FTT are needed to be combined to in the measurement of trust for a buyer in trust-oriented e-commerce environments.

5 Trust-Aware Influencer Finding Algorithm

In this section, we propose a Trust-Aware Influencer Finding method, *TrustINF*, that considers four parameters, i.e., FTBA's gradient, FTBA's mean distance, FTT's gradient and FTT's mean distance which have significant impact on trust-oriented influence evaluation. Finding influencers with multi-attributes is a typical multi-criteria optimal decision making problem [27]. Let P denote the parameter sets of all buyers, and let $X_i = \{X_i^k | k = 1, ..., 4\}$ denote FTBA's gradient, FTBA's mean distance, FTT's gradient and FTT's mean distance respectively. Intuitively, a buyer with lower gradients and higher mean distances will have a higher probability to be an attacker. Without loss of generality, we equally treat four parameters by setting X_2 as the negative value of FTBA's mean distance and X_4 as the negative value of FTT's mean distance in our algorithm.

A *skyline query* retrieves all points that are not dominated by any other point, which is an import method to solve the multi-criteria optimal decision

Table 1. The details of datasets

Data set	Epinions	Slashdot	Amazon	BeerAdvocate
Nodes	4,553	5,155	782	7,116
Links	16,939	9,674	2,385	103,690
Average In-degree	3.72	1.877	3.05	14.571

making problem [13]. In order to accurately identify attackers, we adopt a Skyline method to evaluate the probability of an advisor to be an attacker, and propose the concept of *Influencer Domination* based on the definitions in [28] as follows.

Definition 1 ***Influencer Domination:*** *A buyer* B_i dominates *another buyer* B_j *on an trust-oriented e-commerce platform if and only if for all* $k \in \{1, ..., 4\}$, $X_i^k \geq X_j^k$ *and* $\exists\ t \in \{1, ..., 4\}$, $X_i^t > X_j^t$.

Based on *Definition* 1, we use $N = \{N_i\}$ and $N' = \{N_i'\}$ to denote the dominating number of buyer B_i and the number dominated by other buyers respectively. If N_i' has a large value and N_i has a small value, the trust trend of B_i is downward, causing by the drastic change of ratings to sellers, which is a representative feature of *Camouflage* attack [6]. Thus, we define a function to measure the probability of B_i to be an attacker as Eq. (13).

$$P_i = (N_i' - N_i)/(n-1), \tag{13}$$

where n is the number of buyers and $P_i \in [-1, 1]$.

The pseudo-code of the *TrustINF* algorithm is given in Algorithm 1. As the impact factors have been pre-calculated and pre-stored, Algorithm 1 only needs to calculate $N = \{N_i\}$ and $N' = \{N_i'\}$ by iteratively scanning the set of impact factors n times. Thus, the time complexity of *TrustINF* is $\mathcal{O}(n^2)$, where n is the number of buyers.

Summary: In our TrustINF, firstly, we improves evolutionary trust model and adopt it to evolve trust network after every transaction to obtain the trustworthy historical ratings. Secondly, we calculate every buyer's FTBA and FTT based on these historical ratings to indicate the trust trend of each buyer. Finally, as the social influence evaluation with defending against attacks is a typical multi-criteria optimal decision making problem, and the Skyline method is an important method to solve such a problem, we adopt the skyline method in our TrustINF.

6 Experiments

6.1 Experimental Setting

Dataset. In our experiments, we collect four real trust oriented e-commerce datasets, i.e., *Epinions*, *Slashdot*, *Amazon* and *BeerAdvocate* from

snap.stanford.edu/data/, to investigate the performance of our *TrustINF* algorithm. These datasets have been widely used in the literature for the studies trust-oriented e-commerce [6]. The details of these datasets are listed Table 1.

The Setting of Attacks. In our experiments, we consider two typical attacks, i.e., *Constant* and *Camouflage*. We randomly choose α buyers from each of the dataset as attackers, $\alpha \in [5\,\%, 10\,\%, 15\,\%, 20\,\%, 25\,\%]$. Then, we investigate the *attacker identification ratio* of our *TrustINF*, and investigate the performance of our *Trust-IMM* and *IMM* [20]. Based on the definitions of the two types of attacks [6], we define the typical attackers in our experiments as below:

Constant Attacker: Dishonest buyers constantly provide unfairly positive/negative ratings to sellers [6].

For an attacker B_i, we set the ratings of B_i to give all products which B_i will buy from different sellers as extremely positive ([0.9,1]) or extremely negative ([0,0.1]) values. In our experiments, we randomly select $\alpha/2$ negative attackers and $\alpha/2$ positive attackers. The rating of product p_k can be calculated as below:

$$r_{i,k} = \begin{cases} \text{rand}(0.1) & \text{if } B_i \text{ is negative,} \\ 1 - \text{rand}(0.1) & \text{otherwise.} \end{cases} \tag{14}$$

Camouflage Attacker: Dishonest buyers camouflage themselves as honest buyers by providing fair ratings to build up their trustworthiness first and then gives unfair ratings [6].

For an attacker B_i, if B_i rated product p_k, then

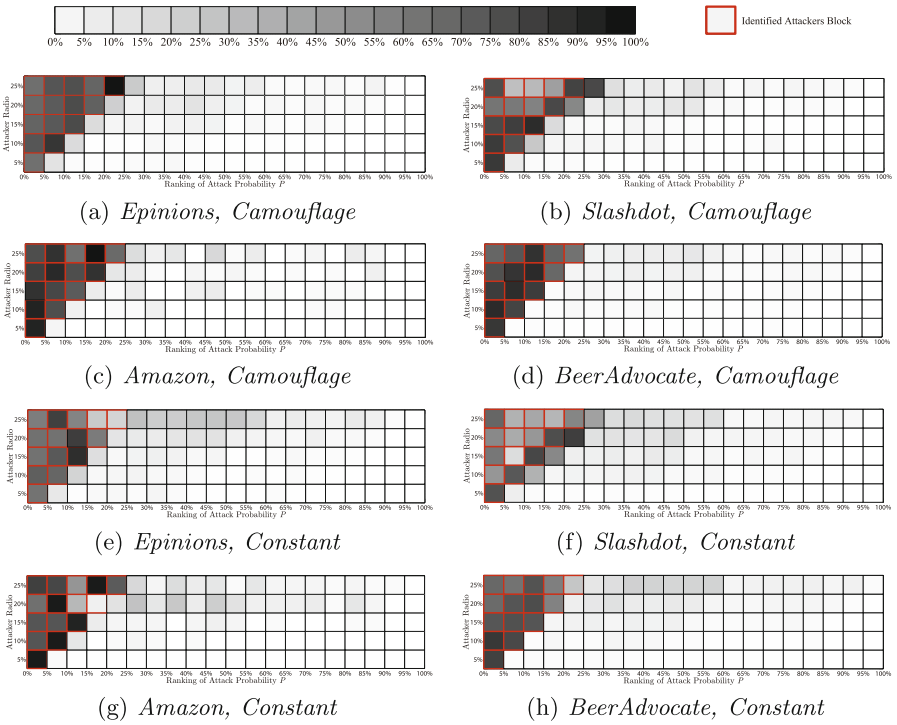
$$r_{i,k} = (r_{i,k} + 0.5) \; mod \; 1. \tag{15}$$

After updating all ratings of B_i based on Eq. (19), B_i becomes a *Camouflage* attacker in our experiments. In

We define the *Identified Attacker* and *Attacker Identification Ratio* to measure the performance of our method:

Definition 2 ***Identified Attacker****: Attacker B_i is an* Identified Attacker *if and only if B_i is an attacker and the probability of attack P_i for B_i is ranked in* Top-α*, where α is the ratio of attackers included in trust-oriented e-commerce environments. This means that these attackers can be identified by influencer finding approaches.*

Definition 3 ***Attacker Identification Ratio****:* Attacker Identification Ratio *is the ratio of identified attackers to the all attackers, which is to measure the scale of identifying attackers delivered by influencer finding approaches.*



(a) *Epinions, Camouflage* (b) *Slashdot, Camouflage*

(c) *Amazon, Camouflage* (d) *BeerAdvocate, Camouflage*

(e) *Epinions, Constant* (f) *Slashdot, Constant*

(g) *Amazon, Constant* (h) *BeerAdvocate, Constant*

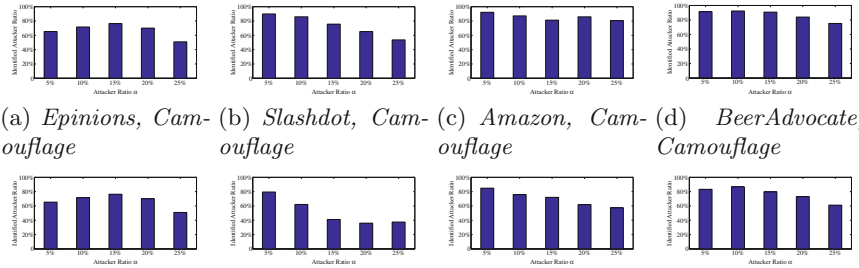
Fig. 4. The Attacker Identification on the four datasets. The color of each block reflects the proportion of the attackers in different ranges of ranking. (Color figure online)

Parameters in IMM and Diffusion Models. In this paper, we adopt two typical diffusion models, i.e., *Linear Threshold (LT)* model [29] and *Independent Cascade (IC)* model [9] to investigate the performance of *Trust-IMM*.

- **IMM:** *IMM* [20] is an influence maximization algorithm which adopts sampling method to return an approximate solution under the triggering model. In this experiments, we consider two kinds of triggering models, i.e., *LT* and *IC*. For *IMM*, we set $\varepsilon = 0.5$, $\ell = 1$, and $K \in [10, 20, 30, 40, 50]$.
- **Linear Threshold (LT) Model:** *LT* model is the first model to imitate the diffusion process of information. The approach is based on the node-specific thresholds [29]. In the model, at time step t, all buyers that were influenced in step $t-1$ remain being influenced. A buyer B_i is influenced based on a monotonic function of its influenced neighbors $f(In(i,t)) \in [0,1]$ (see Eq. (16)) and a threshold $\theta_i \in [0,1]$, i.e., B_i is influenced at time t if $f(In(i,t)) \geq \theta_i$.

$$f(In(i,t)) = \sum_{B_j \in In(i,t)} b_{i,j} \tag{16}$$

where $In(i,t)$ is the influenced neighbors of B_i at time step t. Here, we set $b_{i,j} = T_{i,j} / \sum_{B_k \in Ad_i} T_{i,k}$; Ad_i is the advisor of B_i and $\sum_{B_j \in Ad_i} b_{i,j} \leq 1$.



(a) *Epinions, Camouflage* (b) *Slashdot, Camouflage* (c) *Amazon, Camouflage* (d) *BeerAdvocate, Camouflage*

(e) *Epinions, Constant* (f) *Slashdot, Constant* (g) *Amazon, Constant* (h) *BeerAdvocate, Constant*

Fig. 5. The attacker identification ratio on the four datasets.

In our experiments, in order to investigate the effectiveness of our method based on different thresholds, for each B_i, we set $\theta_i = rand()$.

– **Independent Cascade (IC) Model:** *IC* model is a dynamic cascade model for the diffusion process. The model is based on the interacting particle system from probability theory [9]. At each time step t, each buyer is either influenced or susceptible. A buyer B_j that was influenced at time step $t-1$ has a single chance to influence each of its incoming neighbors B_i. The influence succeeds with probability $P_{i,j}$ (see Eq. (17)). Therefore, for buyer B_i, if at least one of its influenced advisors succeeds, B_i gets influenced. The probability of buyer B_i getting influence at time step t is:

$$f(i,t) = 1 - \prod_{B_j \in In(i,t-1)} (1 - P_{i,j}) \tag{17}$$

where $In(i, t-1)$ is the influenced neighbors of B_i at time step $t-1$. Here, we set $P_{i,j} = T_{i,j}$, i.e., the trust value from B_i to B_j.

Experimental Environment. All experiments were run on a machine powered by two Intel Core i5-3470 CPU 3.20 GHz processors with 8 GB RAM, using Windows 7 operating system. The code was implemented using Java 8 and the experimental data was managed by MySQL Server 5.6.

6.2 Experimental Results and Analysis

Figure 4 plots the probabilities of the identified attackers who are ranked in Top-α delivered by *TrustINF* model on four datasets. From the Fig. 4, we can see that our *TrustINF* method can identify the attackers who have been ranked in the top of the e-commerce (the dark color of blocks). Namely, our *TrustINF* method can help identify those influencers who have fake strong influence. In addition, with the increase of α, $\alpha \in [5\,\%, 10\,\%, 15\,\%, 20\,\%, 25\,\%]$, our *TrustINF* can always identify the attackers with the corresponding Top-α ranking (the triangle area of the dark blocks). This is because our *TrustINF* has considered the

historical data of trust and regress the trend of trust to measure the probability of a buyer to be an attacker. Figure 5 plots the *Attacker Identification Ratio* of our *TrustINF* on the four datasets, where we can see that the range of *Attacker Identification Ratio* delivered by *TrustINF* is [36.02 %, 86.64 %] under the *Constant* attack, and is [53.67 %, 92.41 %] under the *Camouflage* attack. Based on the statistics, on average, the *Attacker Identification Ratio* of *Constant* attack is 66.33 %; and 81.33 % for *Camouflage* attack. This is because when an advisor providing unfair ratings to sellers, the buyers will no longer trust them based on the trust evolutionary model, and *FTBA* and *FTT* of the advisor will descend.

Summary: From the above experimental results, we can see that our *TrustINF* method can effectively identify the attackers who involve in the *Camouflage* attack and the *Constant* attack. In addition, *TrustINF* can effectively identify the attackers who have fake strong influence, which can greatly help buyers and sellers in the transactions in trust-oriented e-commerce environments.

7 Conclusion and Future Work

In this paper, we have proposed a novel Trust-Aware Influencer Finding (TrustINF) method which can defend against the *Camouflage* and the *Constant* attacks in trust-oriented e-commerce environments. The experiments conducted on four real e-commerce datasets have demonstrated our proposed *TrustINF* method can greatly help identify the attackers in the influencer finding, and can greatly improve the robustness of the influence maximization in trust-oriented e-commerce environments.

In future work, we plan to incorporate our *TrustINF* method into some influence evaluation methods in real e-commerce systems to further investigate the effectiveness of our model in defending against attacks.

Acknowledgement. This work was partially supported by Natural Science Foundation of China (Grant Nos. 61303019, 61572336, 61532018, 61402313, 61502324), Doctoral Fund of Ministry of Education of China (20133201120012), Postdoctoral Science Foundation of China (2015M571805, 2015M581859), Open Project Program of the Key Laboratory of Intelligent Information, Institute of Computing Technology, Chinese Academy of Science, and Collaborative Innovation Center of Novel Software Technology and Industrialization, Jiangsu, China.

References

1. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decis. Support Syst. **43**(2), 618–644 (2007)
2. Fiske, S.T.: Social Beings: Core Motives in Social Psychology. Wiley, New York (2009)
3. Bedi, P., Kaur, H., Marwaha, S.: Trust based recommender system for semantic web. In: IJCAI, pp. 2677–2682 (2007)
4. Liu, G., Wang, Y., Orgun, M.A.: Optimal social trust path selection in complex social networks. In: AAAI, pp. 1391–1398, July 2010

5. Liu, G., Wang, Y., Orgun, M.A.: Social context-aware trust network discovery in complex contextual social networks. In: AAAI, pp. 101–107 (2012)
6. Jiang, S., Zhang, J., Ong, Y.S.: An evolutionary model for constructing robust trust networks. In: AAMAS, pp. 813–820 (2013)
7. Liu, A., Zheng, K., Li, L., Liu, G., Zhao, L., Zhou, X.: Efficient secure similarity computation on encrypted trajectory data. In: ICDE 2015, pp. 66–77 (2015)
8. Liu, A., Li, Q., Huang, L., Xiao, M.: Tolerant composition of transactional web services. IEEE Trans. Serv. Comput. **3**(1), 46–59 (2010)
9. Kempe, D., Kleinberg, J., Tardos, É.: Maximizing the spread of influence through a social network. In: KDD, pp. 137–146 (2003)
10. Kimura, M., Saito, K.: Tractable models for information diffusion in social networks. In: PKDD, pp. 259–271 (2006)
11. Wang, D., Muller, T., Zhang, J., Liu, Y.: Quantifying robustness of trust systems against collusive unfair rating attacks using information theory. In: IJCAI, pp. 111–117 (2015)
12. Gao, J., Dong, Y., Shang, M., Cai, S., Zhou, T.: Group-based ranking method for online rating systems with spamming attacks. Europhys. Lett. (2015)
13. Borzsonyi, S., Kossmann, D., Stocker, K.: The skyline operator. In: ICDE, pp. 421–430 (2001)
14. Domingos, P., Richardson, M.: Mining the network value of customers. In: KDD, pp. 57–66. ACM (2001)
15. Chen, W., Wang, C., Wang, Y.: Scalable influence maximization for prevalent viral marketing in large-scale social networks. In: KDD, pp. 1029–1038 (2010)
16. Jung, K., Heo, W., Chen, W.: IRIE: Scalable and robust influence maximization in social networks. In: ICDM, pp. 918–923 (2012)
17. Kim, J., Kim, S.K., Yu, H.: Scalable and parallelizable processing of influence maximization for large-scale social networks? In: ICDE, pp. 266–277 (2013)
18. Ver Steeg, G., Ghosh, R., Lerman, K.: What stops social epidemics? In: ICWSM (2011)
19. Feng, S., Chen, X., Cong, G., Zeng, Y., Chee, Y.M., Xiang, Y.: Influence maximization with novelty decay in social networks. In: AAAI, pp. 37–43 (2014)
20. Tang, Y., Shi, Y., Xiao, X.: Influence maximization in near-linear time: a martingale approach. In: SIGMOD, pp. 75–86. ACM (2015)
21. Guo, J., Zhang, P., Zhou, C., Cao, Y., Guo, L.: Personalized influence maximization on social networks. In: CIKM, pp. 199–208 (2013)
22. Iwata, T., Shah, A., Ghahramani, Z.: Discovering latent influence in online social activities via shared cascade Poisson processes. In: KDD, pp. 266–274 (2013)
23. Subbian, K., Sharma, D., Wen, Z., Srivastava, J.: Finding influencers in networks using social capital. In: ASONAM, pp. 592–599 (2013)
24. Franks, H., Griffiths, N., Anand, S.S.: Learning influence in complex social networks. In: AAMAS, pp. 447–454 (2013)
25. Li, L., Wang, Y.: A trust vector approach to service-oriented applications. In: ICWS, pp. 270–277 (2008)
26. Okelo, B., Boston, S., Minchev, D.: Advanced Mathematics The Differential Calculus for Multi-variable Functions. LAP Lambert Academic, Saarbrücken (2012)
27. Velichenko, V.V.: Sufficient conditions for absolute minimum of the maximal functional in the multi-criterial problem of optimal control. In: Marchuk, G.I. (ed.) Optimization Techniques 1974. LNCS, vol. 27, pp. 220–225. Springer, Heidelberg (1975)
28. Chan, C.Y., Jagadish, H., Tan, K.L., Tung, A.K., Zhang, Z.: Finding k-dominant skylines in high dimensional space. In: SIGMOD, pp. 503–514 (2006)
29. Granovetter, M.: Threshold models of collective behavior. Am. J. Soci. **83**(6), 1420–1443 (1978)