CS 6204 Spring 2017

Solution to Quiz 2 (Open book)

1. (12 points.) In the paper "CloudArmor: Supporting Reputation-Based Trust Management for Cloud Services," the authors introduce 4 credibility factors to be considered to assess the credibility of a customer c providing feedback toward a cloud service s. What are these 4 credibility factors? Among the 4 credibility factors which ones are about the credibility of all feedbacks from all customers toward cloud service s and which ones are about the credibility of the feedback provided by customer c?

   The authors use two performance metrics, recall and precision, to measure the performance of their credibility model. How are these two metrics related to true positive (when an attack is identified), false negative (when an attack is missed) and false positive (when a non-attack is identified as an attack)?

   Ans: The 4 credibility factors (each in the range of 0 to 1 and the higher the better) are (1) Feedback Density $D(s)$ for reducing the value of the multiple feedbacks from the same user; (2) Occasional feedback collusion $\mathcal{O}_f(s, t_0, t)$ which detects occasional change in the total number of trust feedbacks in a period of time; (3) Multi-Identity Recognition $\mathcal{M}_{id}(c)$ which detects the possibility of c taking multiple identities; and (4) Occasional Sybil Attacks $\mathcal{O}_i(s, t_0, t)$ which detects occasional change in the total number of established identities among the whole identity behavior in a period of time.

   Among the four credibility factors, only Multi-Identity Recognition $\mathcal{M}_{id}(c)$ is about the specific feedback provided by c. All the others are about the credibility of all feedbacks from all customers toward cloud service s.

   Precision is the ratio of a number of events you can correctly recall to a number of all events you recall (mix of correct and wrong recalls). So precision is True positive / (True positive + False positive).

   Recall is the ratio of a number of events you can correctly recall to a number of all correct events. So recall = True positive / (True positive + False negative).

2. (12 points.) In the paper "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage," the authors propose an owner-role trust model and a role-user trust model to calculate the owner-to-role trust $T_{\mathcal{O}}(R)$ from an owner O to a role R and the role-to-user trust $T_{\mathcal{R}}(U)$ from a role R to a user U, respectively. The major difference of these two trust models is that the owner-to-role trust computation needs to consider role inheritance. Provide two key computation steps to account for role inheritance in the owner-to-role trust computation.

   Ans: The two key computation steps to account for role inheritance in the owner-to-role trust computation are:

   (a) compute *Inheritance Trust* derived from the interaction history of the descendant roles that have inheritance relationships with role R. The equation for $T_{\mathcal{O}}(R)^I$ explains this computation step;

   (b) compute $T_{\mathcal{O}}(R)$ as the minimum value of the trust value of role R and the trust values of all its ancestor roles $\{R_1, ..., R_m\}$. The equation for $T_{\mathcal{O}}(R)$ explains this computation step. This is because the owners will trust role R at the same level as its ancestor role $R_i \in R_1, ..., R_m$ which has a lower trust value, as the users of its ancestor role R_i have the same level of access as the users in role R.

3. (12 points.) In the paper "Towards Trustworthy Multi-Cloud Services Communities: A Trust-based Hedonic Coalitional Game," the authors propose to use the Dempster-Shafer theory (Equations 3-6) to compute the beliefs in trustworthiness $belief_{S_i}^{S_j}(T)$, maliciousness $belief_{S_i}^{S_j}(M)$, and uncertainty $belief_{S_i}^{S_j}(U)$ of a service S_i toward another service S_j. Following the scenario in Section 4.4 that S_1 wants to establish a trust relationship toward S_5, so it solicits opinions of S_4, S_6, and S_7 which are the three neighbors of S_5. Explain how the information in the social network graph (in Figure 2) connecting S_1, S_5, S_4, S_6, and S_7 may be used to facilitate trust computation of $belief_{S_1}^{S_5}(T)$, $belief_{S_1}^{S_5}(M)$, and $belief_{S_1}^{S_5}(U)$?

   Suppose S_i now has computed the beliefs in trustworthiness $belief_{S_i}^{S_j}(T)$, maliciousness $belief_{S_i}^{S_j}(M)$, and uncertainty $belief_{S_i}^{S_j}(U)$ toward every other S_j, $S_j \neq S_i$. How would S_i decide whether or not to join a coalition C based on the trust-based hedonic coalition formation algorithm proposed by the authors?

   Ans:

   Two pieces of information in the social network graph are used for Dempster-Shafer theory based trust aggregation: (1) S_i's judgement on S_j based on previous interaction experiences, denoted by $S_i \rightarrow S_j \in$ T,M; (2) S_i's credibility score in judging S_j, denoted by $Cr(S_i \rightarrow S_j)$. In the scenario above, the judgements (T or M) from S_4, S_6, and S_7 toward S_5 will be provided to S_1 as feedbacks which will be weighted by the credibility scores $Cr(S_1 \rightarrow S_4)$, $Cr(S_1 \rightarrow S_6)$, and $Cr(S_1 \rightarrow S_7)$ based on Dempster-Shafer theory (Equations 3-6).

   Equation 12 allows S_i to decide whether or not to join a coalition C. The main intuition behind Equation 12 is to allow S_i to choose the coalition that maximizes its belief in trustworthiness (computed by $U_{S_i}(C) = \sum_{a \in C} belief_{S_i}^{a}(T)$ as defined by Equation 2), while avoiding the coalitions that S_i believes contain malicious members (true if $a \in C$ & $belief_{S_i}^{a}(T) < belief_{S_i}^{a}(M)$).

4. (12 points.) In the paper "Trust Evaluation in Online Social Networks Using Generalized Network Flow," the authors claim their generalized flow network model can address path dependence and trust decay in the domain of trust evaluation in online social networks. In two short paragraphs discuss specific mechanisms by which path dependence and trust decay are addressed in their trust propagation and aggregation algorithm design.

Ans: The path dependence issue is addressed by using the trust value $t(e)$ on edge e to represent its capacity, which limits the maximum flow (trust) that can pass through the edge. This design can avoid information reuse and information loss due to dependent paths. More specifically, it can avoid information reuse because the capacity of an edge will be decreased by exactly the amount of flows passing through it. Therefore, the trust value on an edge will not be overused. It can avoid information loss because every edge has the chance to be used for sending flows. Therefore, the trust value on every edge is considered. At the end, the trust value of s has toward d is the summation of all flows going from s to d.

The trust decay issue is solved by using the leakage model. The leakage of each intermediate node can be set flexibly, ranging from uniform, Cosine, exponential, to polynomial. Specifically, trust decay by an intermediate node on a path is transformed to leakage by an edge (by Algorithm 1) so that trust decay through a node maps to capacity leakage through an edge in the generalized flow network.

5. (13 points.) In the paper "A Trust-Aware System for Personalized User Recommendations in Social Networks," user u_j computes its local reputation rating toward user u_i, $LocalRating(u_j \rightarrow u_i, t_c)$, by Equation 1 and its collaborative rating toward user u_i, $CollRating(u_j \rightarrow u_i, t_c)$, by Equation 6. Answer the following questions.

   (a) What is the difference between $LocalRating(u_j \rightarrow u_i, t_c)$ and $CollRating(u_j \rightarrow u_i, t_c)$?

   (b) Once user u_j obtains $CollRating(u_j \rightarrow u_i, t_c)$ reputation ratings for all users u_i connected directly or indirectly with u_j, what can u_j do about this information at time t_c?

   (c) To compute $CollRating(u_j \rightarrow u_i, t_c)$, user u_j has to first contact Q witness users u_q to get their local reputation ratings $LocalRating(u_q \rightarrow u_i, t_c)$ toward user u_i weighted by the credibility of u_q in terms of $cred(u_j \rightarrow u_q, t_c)$. What equation is used by user u_j to compute $cred(u_j \rightarrow u_q, t_c)$ if u_j is directly connected to u_q? What equation is used by user u_j to compute $cred(u_j \rightarrow u_q, t_c)$ if u_j is not directly connected to u_q?

ANS:

(a) $LocalRating(u_j \rightarrow u_i, t_c)$ is based on u_j's own opinions toward u_i, while $CollRating(u_j \rightarrow u_i, t_c)$ is based on both u_j's own opinions toward u_i, and witness users' opinions toward u_i.

(b) This information enables user u_j to generate a personalized user ranking for u_j. From this ranking, the top-k users are provided to u_j as positive recommendations (thus, they could be added to the friend list $F(u_j)$), while the bottom-k users are provided as negative recommendations (thus, they could be added to the enemy list $E(u_j)$).

(c) Equation 7 is used by user u_j to compute $cred(u_j \rightarrow u_q, t_c)$ if u_j is directly connected to u_q, i.e., u_j and u_q are friends or enemies. Equation 8 is used by user u_j to compute $cred(u_j \rightarrow u_q, t_c)$ if u_j is not directly connected to u_q, i.e., u_j is connected to u_q through a number of witnesses which in line form a trust chain.

6. (13 points.) For the paper "Trust Management for SOA-Based IoT and Its Application to Service Composition," the authors propose two filtering mechanisms for trust computation of a IoT device: distributed collaborating filtering and adaptive filtering. In two short paragraphs, explain what these two filtering mechanisms are and how they improve the accuracy of trust computation.

   Ans: Distributed collaborating filtering is applied to select trust feedback from nodes sharing similar social interests (Equation 7), including friendship (representing intimacy), social contact (representing closeness) and CoI (representing knowledge and standard on the subject matter). It improves trust accuracy because users sharing similar social interests are more likely to provide trustworthy and credible feedback.

   Adaptive filtering is applied to dynamically adjust the weights associated with direct trust and indirect trust (Equation 8) so that the overall trust matches recent direct user satisfaction experiences. The basic design principle is that a successful trust management protocol should provide high trust toward devices who have more positive user satisfaction experiences and, conversely, low trust toward those with more negative user satisfaction experiences. It improves trust accuracy because it allows a user to dynamically adjust the direct and indirect trust weights in response to direct user satisfaction experiences recently received.

7. (13 points.) Answer the following questions concisely based on the paper "Trustworthiness Management in the Social Internet of Things."

   (a) In one short paragraph (less than 100 words), give the pros and cons of subjective vs. objective trust models proposed by the authors.

   (b) Which information among below is not used by the subjective model for peer-to-peer trust assessment? (There is only one answer. No need to explain your reason.)

      i. feedback
      ii. credibility
      iii. transaction factor
      iv. relation factor
      v. centrality
      vi. computation capability
      vii. trust transitivity
      viii. interaction context

   (c) Identify two design features among those listed in (b) above that contribute to the proposed trust model (either subjective or objective) outperforming TVM/DTC, a P2P trust management protocol. Why?

Ans:

(a) The pros and cons are given in the conclusion section of the paper. Namely, "The major difference between the two methods is that the subjective approach has a slower transitory response, which is particularly evident when dealing with nodes with dynamic behaviors. However, it is practically immune to behaviors typical of social networks, where a malicious person modifies her actions based on the relationships. On the contrary, the objective approach suffers from this kind of behavior, since a node's trustworthiness is global for the entire network and this includes both the opinion from the nodes with which it behaved maliciously and the opinion from the nodes with which it behaved benevolent."

(b) Interaction context is not used

(c) Relation factor and centrality because both are social network aspects which are not considered by this P2P trust management protocol.

8. (13 points.) Answer the following questions concisely based on the paper "Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies."

   (a) Provide reasons why a Social Internet of Things (SIoT) system can provide scalable service discovery compared with a centralized system or a hierarchical system.

   (b) To achieve service search efficiency, a SIoT system relies on the notion of network navigability measured by the average path length among all the pairs of nodes. Which of the 5 friend-selection strategies proposed by the authors will perform the best in local (network) navigability, i.e., in the ability of each node to reach the destination making use of only local information? Why?

   (c) Which of the 5 friend-selection strategies will perform the best in local (network) navigability after incorporating the authors' design to dynamically adjust the number of friends allowed per node (i.e., N_{max}) on the basis of the number of hubs in the network? Why?

Ans:

(a) A SIoT system performs service search in a totally distributed manner by which each object simply looks for desired service by using its friendship social network, querying its friends and the friends of its friends, thus providing an efficient and scalable discovery of objects and services. A centralized or a hierarchical system must use a centralized server to process queries from a huge number of IoT devices, making it unscalable.

(b) The "min local clustering" strategy (strategy 5) will perform the best in local network navigability. The reason why the "min local clustering" strategy (strategy 5) has the best performance in network navigability is that in the given network condition, there are too many hubs with their degree equal to the maximum number of friends (N_{max}) especially when N_{max} is small. In this case the network navigability deteriorates since a node has no clues which hub to select to deliver a message to. For this reason, when we reduce N_{max}, the properties for local navigability no longer apply and strategy 5 that performs best at global level can perform efficiently even at local level.

(c) The "max neighborhood degree" strategy (strategy 2) will have the best performance in local (network) navigability after incorporating the authors' design. The reason why the "max neighborhood degree" strategy (strategy 2) has the best performance in network navigability is that with the design (as shown in Figure 10 where x coordinate is the maximum percentage of hubs in the network, and y coordinate is the threshold for a node to become a hub) the number of hubs reaching N_{max} connections is greatly reduced. This improves network navigability as it allows a node to easily select a neighbor hub with the highest number of connections to deliver a message to. As strategy 2 can create hubs with a higher number of friends than strategy 5, strategy 2 performs the best.