Quiz 2 (Open book)

I pledge that this test has been completed in compliance with the Graduate Honor Code and that I have neither given nor received any aid on this test.

Student Name: ___________________________________________________________

Signed: __________________________________________________________________

1. (10 points.) Answer the following questions concisely based on the paper “RATEWeb: Reputation Assessment for Trust Establishment among Web services.”

(a) Is RateWeb proposed by the authors based on feedbacks only? Why?
   
   **Ans:** No, it also considers direct trust by using the first-hand interaction experience with a service provider.

(b) Which information among below is not used by RateWeb to rate a rater? (There is only one answer. No need to explain your reason.)
   
   i. Majority Rating
   ii. Past Rating History
   iii. Personal Experience for Credibility Evaluation
   iv. Personal Preferences
   v. Personal Experience for Reputation Assessment
   vi. Temporal Sensitivity

   **Ans:** (v) the “Personal Experience for Reputation Assessment,” or the first-hand interaction experience is to rate a service provider, not to rate a rater.

(c) Give one reason why RATEWeb can still provide the assessed reputation fairly consistent and close to the actual reputation in Fig. 7 in which low credibility raters out-number others.

   **Ans:** The answer is in the paper: This is mainly due to the incorporation of first-hand knowledge at the end of each transaction, which dilutes the effects of dishonesty by lowering (dishonest) rater credibilities.

(d) Give one reason RATEWeb performs better than PeerTrust in terms of reputation accuracy.

   **Ans:** The answer is in the paper: RATEWeb’s accuracy may be attributed to the way rater credibilities are evaluated and the use of personalized preferences for indirect trust assessment.
2. (10 points.) In the paper "Trustworthy Service Selection and Composition," the two main approaches proposed by the authors are the Bayesian Network approach and the Beta mixture approach. Answer the following questions based on the assumption that the quality trust of service $i$ ($\theta_i$) is based on the beta probability distribution with parameters $(\alpha_i, \beta_i)$. Also use the Bayesian network in Fig. 2 as an example.

(a) The Bayesian Network approach provides accurate quality trust estimate of a composite service despite incomplete data about quality trust of constituent services. Fig. 3 demonstrates the effectiveness of the approach. In one short paragraph, describe the basic principle used for achieving this objective.

**Ans:**

The basic principle is that since some variables are not observable, we can consider the variables without data as latent variables and calculate the expected values of those variables. For example, we can estimate the $(\alpha, \beta)$ values of $H$ if we know the quality information of $f$ in an observation. This allows the missing counts for $H$ to be estimated even if this data is missing. This is the $E$ step of the Expectation Maximization (EM) technique proposed in the paper. Then based on the completed data, Bayesian inference can be applied to calculate quality trust of $H$. This is the $M$ of the EM technique. Finally based on the relationship (SWITCH, SUM, PRODUCT, etc.) between the composite service and the constituent services, the overall trust of the composite service can be calculated.

(b) The Beta mixture approach allows the contribution of each service toward the composite service to be estimated, given that only composite service quality observations are available as input. Fig. 8 demonstrates the effectiveness of the approach. In one short paragraph, describe the basic principle used for achieving this objective.

**Ans:** The basic principle is that the trust distribution of the composite service is a beta mixture of beta distributions for the constituent services based on the relationship (SWITCH, SUM, PRODUCT, etc.) between the composite service and the constituent services. In particular $\pi_k$ in Eq. 1 for service $i$ is an indicator of service $i$’s responsibility, indicating how much contribution the component makes toward the composite quality. The EM technique can be applied here as well.
3. (10 points.) For the paper “Trust Management of Services in Cloud Environments: Obstacles and Solutions,” the authors classified trust management techniques into different categories: Policy, Recommendation, Reputation, and Prediction. Name one technique in each category that can be applied to assess trust of a cloud service.

Ans: The answers are in section 4.1 of the paper. Below are my answers.

(a) Policy: one can use SLA monitoring and auditing (or predefined policies) with a trust threshold to evaluate the credibility of a cloud service.

(b) Recommendation: one can use consensus (i.e., where trust feedback is aggregated from different cloud service consumers) and discounting (i.e., where trust feedback is weighted based on the trustworthiness of cloud service consumers) to derive trust from recommendations.

(c) Reputation: one can aggregate the reputation of a particular cloud service based on feedback using QoS and other attributes (e.g., elasticity, geographical location).

(d) Prediction: one can use a similarity technique (i.e., distinguishing similar minded cloud service consumers) to determine credible feedback from the misleading ones to assess trust toward a cloud service.
4. (10 points.) For the paper “Trust mechanisms for cloud computing,” the authors proposed two new mechanisms for trust judgement of cloud entities such as a cloud broker, a cloud service provider, etc. These two new mechanisms according to the authors are over and above existing mechanisms including reputation, QoS monitoring and SLA verification, self-assessment and information revealing, trust as a service, and formal accreditation. What are these two new mechanisms? Elaborate.

**Ans:** The answers are in the summary of the paper.

(a) a “formal” policy-based approach of trust judgment, by which the trust placed on a cloud service or a cloud entity is derived from a “formal” audit proving that the cloud entity conforms to some trusted policies.

(b) a “formal” attribute-based approach of trust judgment, by which particular attributes of a cloud service or attributes of a service provider are used as evidence for trust judgment, and the belief in those attributes is based on formal certification and chains of trust for validation.
5. (10 points.) In the paper “Hatman: Intra-cloud Trust Management for Hadoop,” the computation of the local trust matrix $T$ is done in a distributed manner. How does DataNode $i$ compute its trust toward DataNode $j$ based on node $i$’s and node $j$’s computational experiences? Explain your answer.

**Ans:** Specifically, $T_{ij} = \alpha_{ij} t_{ij}$ where $t_{ij}$ measures how much DataNode $i$ trusts DataNode $j$, and $\alpha_{ij}$ measures $i$’s relative confidence in his choice of $t_{ij}$. Both $t_{ij}$ and $\alpha_{ij}$ are obtained from direct experiences. That is, $t_{ij}$ is the percentage of jobs shared by $i$ and $j$ on which $i$’s group agreed with $j$’s group, i.e., $t_{ij} = A_{ij}/C_{ij}$ where $C_{ij}$ is the number of jobs shared by $i$ and $j$ and $A_{ij}$ is the number of those jobs on which their groups’ answers agreed. $\alpha_{ij}$ is the percentage of assessments of $j$ that have been voiced by $i$, i.e., $\alpha_{ij} = \frac{C_{ij}}{\sum_{k=1}^{N} C_{kj}}$. 

6. (10 points.) In the paper “Measuring Behavioral Trust in Social Networks,” the main contribution is to present measurable behavioral metrics for trust in social networks. The authors develop “statistical” algorithms to construct dyadic trust graphs ($T_C$ and $T_p$) for two social trust behavior patterns: conversation and propagation.

(a) The statistical algorithms are scalable to social networks on millions of nodes. Why?
   **Ans:** they only look at communication traffic stream (sender, receiver, time), and do not look at semantic content of the messages, so their algorithms are scalable to larger networks.

(b) Do they use retweets information to construct the two dyadic trust graphs ($T_C$ and $T_p$)?
   **Ans:** No. They only use retweets to validate $T_C$ and $T_p$.

(c) When using Twitter data, there is significant similarity between $T_C$ and $T_p$. What is the physical implication of this similarity?
   **Ans:** This says that the type of relationship the two trust graphs are capturing is similar.
7. (10 points.) The paper “A Survey of Trust in Social Networks,” concludes that the majority of trust evaluation models are based on network/graph structures. Discuss the shortcoming of network/graph-based trust models for web-based social networks. Discuss two approaches to overcome the shortcoming.

**Ans:** The shortcoming is that network graphs typically only consider the volume and frequency of interactions, but neglect an important aspect of social networks, namely the semantics/context information of interaction including the duration and intimacy of interactions and the types of interactions.

Two approaches to overcome the shortcoming are extracting the type and direction of interaction to provide further information about the trust relationship. Interactions could be active such as contributing posts, comments/feedbacks, sending friend requests, or passive such as reading others’ posts and responding to friend requests. Similarly, the direction of interaction indicates whether the member usually initiates interaction with others or only responds to others’ initiations. All of these factors could indicate different types of trust relationships and trust levels within the community.
8. (10 points.) In the paper “Predicting Trust and Distrust in Social Networks,” the authors point out that distrust is not transitive, so traditional algorithms based on the notion of the transitivity of trust may not work. What is the basic idea used by the authors to compute distrust? What is the limitation of their algorithm (name one)?

**Ans:** The basic idea is to classify an edge connecting two nodes in an undirected graph. They adopt a probabilistic treatment of trust combined with a modified spring-embedded layout algorithm to classify an edge. They first compute the path probability and spring embedding distance for each edge. Then they compute a separator based on these two quantities to classify each edge as a positive or negative trust relationship.

The biggest limitation is that the graph is undirected, so their algorithm cannot handle trust or distrust asymmetry.
9. (10 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.

**Ans:** 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 include both the opinion from the nodes with which it behaved maliciously and the opinion from the nodes with which it behaved benevolent.”

(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

**Ans:** interaction context is not used

(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:** Relation factor and centrality because both are social network aspects which are not considered by this P2P trust management protocol.
10. (10 points.) For the paper “Trust management system design for the Internet of Things: A context-aware and multi-service approach,” list two design features that distinguish the work from others in the literature for trust management in IoT systems.

**Ans:** There could be many answers. My answers are:

(a) Dynamic trust scores are assessed toward a node according to different contexts (such as node status while providing service) and different functions (such as service type). This effectively protects against selective behavior attack since distinct trust scores toward the same node are calculated for different services, so a malicious node cannot compensate its bad service in one service type by good service in another service type.

(b) Separating service trust above from quality of recommendation. Quality of recommendation is updated by performing a time-weighted sum calculation of the current quality of recommendation score and the history quality of recommendation scores, all of which are calculated based on the requesting node’s service feedback per recommendation. This effectively protects against bad-mouthing and ballot-stuffing attacks because the quality of recommendation is updated dynamically and is separate from service quality trust.