Solution to Quiz 1 (Open book)

1. (12 points.) In the paper "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs," the basic idea is for an evaluating node (i) to use three criteria to judge whether a recommending node (k) is dishonest while providing a recommendation toward the evaulated node (j) and to filter out the dishonest recommendation. What are the three criteria? Explain how node i (the evaluating node) measures (i.e., computes) these three criteria of node k (the recommender). Among the three criteria, which one is the least effective based on the experimental results obtained?

   Ans: The three criteria are: (a) interaction intensity of i with k, called confidence value, computed as the variance of the beta distribution with α_{ik} and β_{ik} parameters; (b) trust deviation between the trust of i toward j, and the trust of k toward j, called the deviation value, computed by $T_{ij}^d - T_{kj}^r$ where T_{ij}^d is the direct trust value of i about j, and T_{kj}^r is the received trust value of k about j; and (c) closeness between i and k, called the closeness centrality value, computed by the physical distance between i and k. Among the three criteria, deviation value is the least effective based on the experimental results obtained.

2. (12 points.) In the paper "Trustworthy Parking Communities: Helping Your Neighbor to Find a Space," the trust system used by the authors is Josang's Beta reputation system such that a node i keeps two varables r_j and s_j for a recommender j. Explain the meaning of these two variables and how i updates r_j and s_j dynamically for calculating the reputation score of i toward j, i.e., $Rep_j(r_j, s_j)$. Suppose that i is the originator node and j is a malicious node. Give a reason why j's reputation score is updated so accurately as shown in Figure 6 of the paper.

   Ans: r_j is the number of times j's response is correct and s_j is the number of times j's response is incorrect. $Rep_j(r_j, s_j)$ is calculated as $(1 + r_j)/(r_j + s_j + 2)$ (Equation 5). Node i updates r_j and s_j based on self experience, i.e., Node i scans the street for available spots itself and compares the actual situation with j's response. If j's response is a match, r_j is incremented by 1. Otherwise, s_j is incremented by 1. The reason why j's reputation score is updated so accurately as shown in Figure 6 of the paper is that r_j and s_j are updated based on i's self observations (ground truth) only. In other words, only direct trust is used for $Rep_j(r_j, s_j)$ computation, i.e., node i does not combine its $Rep_j(r_j, s_j)$ score with other $Rep_j(r_j, s_j)$ scores provided by other nodes in the system. This eliminates the problems associated with ballot stuffing or bad-mouthing attacks.

3. (13 points.) In the paper "A Probabilistic Misbehavior Detection Scheme Towards Efficient Trust Establishment in Delay-Tolerant Networks," when given that the inspection probability is $p_b = (g + \epsilon)/(w + C)$, a rational node will choose to forward packets since the payoff to forward packets $\pi_w(W)$ is greater than the payoff to deny forwarding $\pi_w(S)$.

   Decide if the trusted authority (TA) will choose to inspect a node, when given that the **offending** probability of the node is $p_f = (h + \epsilon)/(w + C)$.

   Give your reason in terms of the payoff $\pi_{TA}(I)$ to inspect the node and the payoff $\pi_{TA}(N)$ not to inspect the node.

   Ans: If a TA chooses I, its payoff is $\pi_{TA}(I) = p_f \times (C - h) + (1 - p_f) \times (\nu - w - h) = \nu - w - \nu p_f + \epsilon$ after substituting in $Cp_f + wp_f = h + \epsilon$. If a TA chooses N, its payoff is $\pi_{TA}(N) = p_f \times (-w) + (1 - p_f) \times (\nu - w) = \nu - w - \nu p_f$. Since $\pi_{TA}(I) > \pi_{TA}(N)$, a rational TA will choose to inspect.

4. (13 points.) In the paper "PROVEST: Provenance-based Trust Model for Delay Tolerant Networks," the main idea is that a destination node (DN) can collect indirect trust evidence of a message carrier (MC) through provenance information (PI) embedded in a message routed to it.

   (a) Explain why this idea is particularly attractive for delay tolerant networks.

   (b) Each MC will create and embed a PI piece to put in the message routed to the DN. What information is contained in this PI piece? What trust metrics (or dimensions) are being evaluated by the DN when it receives the message? There is no need to give explanations.

   (c) Which one of the following four variants of PROVEST: PROVEST-Pessimistic, PROVEST-Optimistic, PROVEST-Realistic, and PROVEST-Hybrid, is the same as Josang's Beta Reputation System using a MC's trust relative to T_{min} to decide whether or not the MC' opinion toward the previous MC can be accepted or rejected?

Ans:

(a) In a DTN, nodes do not often encounter with each other, so relying on recommendation information exchanged during encounters to collect indirect evidence may not be practical. Further, collecting recommendation information from nodes far away is especially impractical because there is no guarantee of end-to-end connectivity, thus causing high delay and high overhead when collecting recommendations. In PROVEST, a DTN node collects indirect evidence information through provenance information embedded in messages being routed through the nodes acting as MCs. This greatly increases trust accuracy and routing protocol performance without incurring high communication overhead.

(b) The PI piece MC i put in is its opinion (direct trust) toward the previous MC j in terms of $r'_{i,j}$, $s'_{i,j}$, and $u'_{i,j}$, which can be used by the DN as indirect trust information of MC j. Other information put in is the IDs of MCs i and j for authentication and availability assessment.

(c) PROVEST-Realistic is the same as Josang's Beta Reputation System. The recommendation filtering is based on if MC i's trust is greater than T_{min}. If yes, MC i's opinion toward the previous MC j is taken in as is for trust aggregation.

5. (13 points.) For the paper "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," the authors proposed a design concept of identifying the best way to form and use trust for application performance maximization. They applied the design concept to two wireless sensor network applications: trust-based secure routing and trust-based intrusion detection. Explain briefly for each of these two applications (a) what application performance metrics are being used to measure application performance, and (b) what trust parameters are being controlled to maximize application performance.

   ANS: For trust-based routing, the performance metric for performance maximization is delivery ratio. The parameters to be controlled to maximize application performance are the weights of individual trust components, i.e., closeness, honesty, energy, and unselfishness.

   For trust-based intrusion detection, the performance metric for performance maximization is the false alarm probability including the false positive probability (P_{fp}) and the false negative probability (P_{fn}). The parameters to be controlled to maximize application performance are the weights of individual trust components and the minimum trust threshold, T_{th}, below which a node is considered compromised.

6. (13 points.) For the paper "An Efficient Distributed Trust Model for Wireless Sensor Networks," what are the differences of the folowing four trust measures: (a) direct trust, (b) recommendation trust, (c) integrated trust, and (d) indirect trust. Suppose node i and node j are neighbors, and node k is 3-hop away. Which trust measures among 4 above would apply to node i toward node j? Which trust measures among 4 above would apply to node i toward node k?

   Ans:

   Direct trust is one node's trust toward another neighbor node's behavior based on direct observations.

   Recommendation trust is one node's trust toward another neighbor node's behavior based on recommendations received from neighbor recommenders.

   Integrated trust is a weighted sum of direct trust and recommendation trust, so it is the overall trust of one node toward another neighbor node.

   Indirect trust is one node's trust toward a non-neighbor node's behavior based on recommendations received from nodes in a trust chain. Since there is no direct trust (toward a non-neighbor node), indirect trust is the overall trust of one node toward a non-neighbor node.

   In the scenario described, direct trust, recommendation trust, and integrated trust would apply to node i toward node j, while only indirect trust would apply to node i toward node k.

7. (13 points.) For the paper "Trust-based Service Composition and Binding with Multiple Objective Optimization in Service-Oriented Mobile Ad Hoc Networks," the authors discuss the concepts of trust component, trust computation, trust formation, and trust usage for service-oriented MANETs. Discuss exactly how these concepts are implemented in the paper.

Ans:

Trust component is implemented by considering two distinct trust components: competence and integrity.

Trust computation is implemented based on Josang's Beta Reputation with belief discounting being applied to each of the two trust components separately. For the *competence* trust component, a positive experience is recorded for all SP members executing task m if the service quality received is higher than the minimum user satisfaction thershold for task m (UST_m); otherwise, a negative experience is recorded for each culprit SP member identified. For the integrity trust component, a positive experience is recorded on an SP if the SP's advertised Q, D, C scores are close to the SP's actual Q, D, C cores; otherwise, a negative experience if recorded for the SP. Upon receiving recommendation evidence (in terms of positive and negative experience counts for each trust component) from a recommender, a node applies belief discounting before merging its own evidence with the recommendation evidence.

Trust formation is implemented by treating integrity trust as confidence to competence trust. Two schemes are implemented in the paper: (a) TRM: if integrity trust falls below the minimum integrity trust threshold, competence trust drops to zero; (b) SRM: competence trust scales up (to 1 maximum) or down (to 0 minimum), depending on whether integrity trust is higher or lower than the threshold. Equations (12) and (13) compute the overall trust for the TRM and SRM schemes, respectively.

Trust usage is implemented by multiplying the SR's trust toward an SP with the SP's advertised scaled Q, D, C scores. The basic idea of trust-based service composition and binding is that an SP's advertised Q, D and C scores are discounted by the SR's trust towards the SP. When the trust estimate is accurate, it can effectively defend against malicious nodes performing attacks.

8. (13 points.) For the paper "CATrust: Context-Aware Trust Management for Service-Oriented Ad Hoc Networks," provide reasons why CATrust outperforms both Beta Reputation and Adaptive Trust Management (as demonstrated in Figures 7 and 8) and why the false negative probability (P_{fn}) is around **0.6** and the false positive probability (P_{fp}) is around **0.4** for both Beta Reputation and Adaptive Trust Management (as demonstrated in Figures 7 and 8).

Ans:

The fundamental reason that CATrust outperforms both Beta Reputation and Adaptive Trust Management is attributed to the fundamental difference in trust protocol design logic. CATrust infers a service trust value for each context environment based on the trustee node's predicted service behavior in that context environment, while Beta Reputation or Adaptive Trust Management just maintains one service trust variable across all context environments. Consequently, P_{fn} (missing a trustee node's bad service) tends to converge to the probability that the trustee node is providing good service, i.e., the node's average service trust value, which is equivalent to the node satisfactory service ratio P_{ssr}=0.6. On the other hand, P_{fp} (missing a node's good service) tends to converge to the probability that the node is providing bad service, which is 1-P_{ssr}=1-0.6=0.4. In contrast, CATrust is not bound by the satisfactory service ratio. Rather, by learning the trustee node's service behavior, CATrust infers a service trust value that is as close to the ground truth service satisfaction as possible in a particular context environment.