Abstract – Reputation and Recommendation Systems

In most general terms, **Recommendation systems** are defined as the techniques used to predict the rating one individual will give to an item or social entity. These items can be books, movies, restaurants and things on which individuals have different preferences. These preferences are being predicted using two approaches first content-based approach which involves characteristics of an item and second collaborative filtering approaches which takes into account user's past behavior to make choices. In collaborative filtering, partners are chosen who will make recommendations because they share similar ratings history with the target user[2]. One partner who have similar ratings to the target user may not be a reliable predictor for a particular item. So the past record of the partner of making a reliable recommendation also needs to be take into consideration which is dictated by trustworthiness of a partner[2]. In order to keep track of past records of a recommender reputation systems comes into the picture those who actually assign reputation ratings to the partners.

Due to a high increase in mobile devices problem of information overload also arises in mobile ad-hoc networks and to tackle this we need recommendation systems in mobile ad-hoc networks. As in mobile ad-hoc networks mobile devices themselves work as routers and hosts there is a high possibility of being a malicious node present in network. This increases the need of a reputation system in mobile ad-hoc networks. Rehan Akbani, Turgay Korkmaz, and G. V. S. Raju[3] used SVM(Support vector machine) based approach to detect malicious nodes present in the system by modeling the past behavior of a node. They perceived reputation system problem as a time series prediction problem as which actually try to predict the value of a variable for a future time (t+1) if values of that variable in past(t,t-1,t-2,t-3,, t-n) are known. They build SVM models against different type of malicious behaviour and attach scenarios offline and uploaded them to the network. Nodes then can use these models to predict about a new node if that node can be malicious or not. Yao Wang, Julita Vassileva[4] proposed a bayesian network based trust model in which peers were able to update their recommendations with other peers in the network. In their model every node A has two kinds of trust in another node B. First the trust node A has in node B's capability for providing services and second the trust node A has in the recommendations provided by the node B. Sonja and Jean[4] went ahead to come up with a reputation system which was not just peer to peer rather it was a fully distributed reputation system. In their model every node i maintains two ratings of a node j which it care about. These ratings are trust ratings and reputation ratings. R_{ij} (Reputation rating) represent what node i think about node j's behavior in network. whereas T_{ij}(Trust rating) represent how much node i has trust in the first hand information published by node j. First hand information F_{ij} is the information maintained by node i for about node j and is the only information that is published to other nodes. Based on this first hand information R_{ij} & T_{ij} is updated. Another reputation based scheme was proposed by Song and Ma [5], which involved detection of malicious packet dropping in mobile ad hoc networks, where two different reputations were considered – self observation (first hand information) along with a fuzzy model to accommodate loss due to deliberate packet dropping and congestion and second hand information which can accelerate the detection and subsequent isolation of malicious nodes. Comprehensive reputation is calculated based on the local and social reputation. Mobile Ad hoc networks have security issues, which have been time and again tried to overcome. So we propose a scheme which models a reputation based recommendation system, on top of a trust layer modeled by the nodes which may or may not act as trusted node.

References:

1. http://en.wikipedia.org/wiki/Recommender_system

2. Trust in Recommender Systems
http://delivery.acm.org.lp.hscl.ufl.edu/10.1145/1050000/1040870/p167-odonovan.pdf?ip=159.178.22.27&acc=ACTIVE%20SERVICE&CFID=71096655&CFTOKEN=81181895&__acm__=1332118344_5025d239d038bf6e9f3afc9eea97f2c8

3. Defending against malicious nodes using an SVM based reputation system.

http://ieeexplore.ieee.org.lp.hscl.ufl.edu/stamp/stamp.jsp?tp=&arnumber=4753370

4. A Robust Reputation System for Mobile Ad-hoc Networks - Sonja Buchegger , Jean-Yves Le Boudec
http://mescal.imag.fr/membres/corinne.touati/Sandra/robust_report.pdf

5, A Reputation-based Scheme against Malicious Packet Dropping for Mobile Ad Hoc Networks -Song JianHua, Ma ChuanXiang
School of Mathematics and Computer Science, Hubei University, Wuhan 430062, Hubei, China
(http://ieeexplore.ieee.org.lp.hscl.ufl.edu/stamp/stamp.jsp?tp=&arnumber=5935316)