as well as bad node converges at 600 seconds after which the computed trust remains constant with time. Fig. 4 and Fig. 5 show the comparative analysis wherein the proposed RecommFilter scheme outperforms all the remaining three schemes.

In case of slandering attack as well as self-promoting attack, the convergence of trust using the RecommFilter scheme is closest to the actual trust metric reflecting the true nature of the node. In the case of RecommVerifier scheme, even though it uses two novel schemes for refining the results of the detection of dishonest recommenders, since the trust model is based upon Bayesian inference, the trust computation may not be accurate enough compared to the trust model based upon Dempsters Shafer Theory since it includes the quantification of uncertainty. The E-Hermes scheme based upon the personal experience based approach performs lesser than the RecommVerifier as it discards all the recommendations which are not consistent with its own but the dynamic nature of a MANET may result in the evaluating node's interaction experience being insufficient in reflecting the true nature of a node thereby resulting in a slow convergence rate. The WFS scheme performs the least compared to all the other schemes as it is based only upon majority rule based approach which may obscure many dishonest recommenders and result in the slowest convergence rate.

With 40% dishonest recommenders, the trust convergence rate for slandering attack and self-promoting attack are shown in Fig. 5. It can be observed that as number of dishonest recommenders decreases, the trust convergence rate is faster at 400 seconds (compared to 600 seconds with 80% dishonest recommenders) since the true nature of a node is revealed faster.

The comparative analysis also shows that, the proposed RecommFilter scheme performs better compared to RecommVerifier, E-Hermes and WFS schemes irrespective of the number of dishonest recommenders by having the computed trust closest to the actual trust reflecting its true nature. Another metric used for comparative analysis is the packet delivery fraction by varying the number of dishonest recommenders.

Packet delivery fraction is computed as the ratio of total number of packets received by the destination to the total number of packets sent by the source node. As expected, for all the schemes, as the number of dishonest recommenders increases the packet delivery fraction decreases. Fig. 6 shows that the proposed RecommFilter scheme has the highest average packet delivery fraction of 68.83% compared to 64.5%, 59.5%, and 56.83% of RecommVerifier, E-Hermes and WFS. Since the packet delivery fraction is directly proportional to the efficiency of trust model (since trust based routing is employed) which includes the efficiency in detection of dishonest recommenders, it is obvious that the proposed RecommFilter outperforms the remaining three schemes.

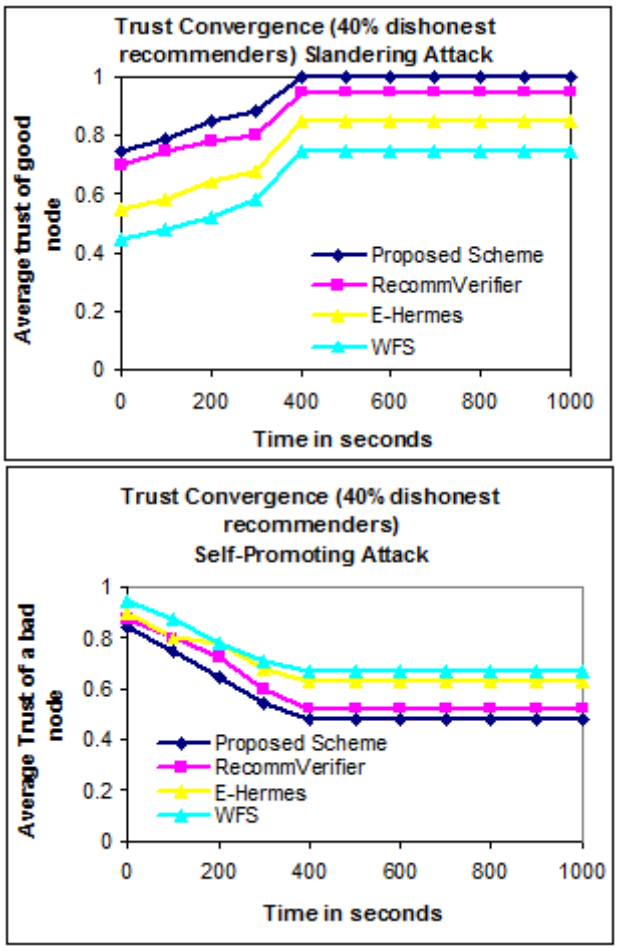

Figure 5: Trust Convergence rate of a good node and a bad node with Slandering and Self-Promoting attacks respectively with 40% dishonest recommenders

7. Conclusion

The novelty of the proposed RecommFilter scheme lies in the usage of Jousselmes distance to filter the recommendations. The trust model employs the Dempster Shafer Theory for quantifying uncertainty which is most appropriate in a dynamically changing environment of MANET. As far as we know, this work is the first one to utilize an opinion similarity measure through Jousselmes distance for filtering out the dishonest recommendations. The proposed scheme tries to overcome the limitations of the existing recommendation filtering defense schemes by employing a combination of multiple approaches including the majority rule based and the personal experience based along with a metric known as similarity index. The modules of Recommendation Selection, Recommendation Filtering, Recommendation Evaluation and Recommendation Trust Update work together collectively to efficiently detect dishonest recommenders with a reduced false positive proportion and a reduced false negative proportion. The recommendation selection module ensures that irrespective of the number of recommendations received, the precedence rules enable the selection of a fixed number of recommendations. The recommendation filtering module accepts as input the recommendation set obtained as the output of recommendation selection module. The input recommendation set is used to select a subset which represents a refined recommendations set. The

recommendation trust update module assists the recommendation selection module in choosing a subset of relatively credible recommendations out of the received set of recommendations. The simulations experiments show that the proposed RecommFilter scheme works efficiently even in the presence of 80% dishonest recommenders.

References

[1] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decis. Support Syst., vol. 43, no. 2, pp. 618–644, 2007
[2] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," Proc.IEEE, vol. 98, no. 10, pp. 1752–1754, Oct. 2010
[3] M. Carbone, M. Nielsen and V. Sassone, "A formal model for trust in dynamic networks," in In Proc. International conference on software engineering and formal methods, SEFM03, pp. 54–63, 2003
[4] C. Zouridaki, B.L. Mark, M. Hejmo, R.K. Thomas, E-Hermes: a robust cooperative trust establishment scheme for mobile ad hoc networks, Ad hoc Networks 7 (2009) 1156–1168.
[5] S. Ganeriwal, L.K. Balzano, M.B. Srivastava, Reputation-based framework for high integrity sensor networks, ACM Transactions on Sensor Networks 4 (2008) 1–37
[6] A. Whitby, A. Josang, J. Indulska, Filtering out unfair ratings in bayesian reputation systems, in: Proceedings of the Third International Joint Conference on Autonomous Agents and Multi Agent Systems, 2004, pp. 106–117.
[7] J. Feng, Y. Zhang, H. Wang, A trust management model based on evaluation in p2p networks, IEICE Transactions on Information and Systems 93 (2010) 466–472.
[8] S. Buchegger, J.-Y. L. Boudec, A robust reputation system for p2p and mobile ad-hoc networks, in: Proceedings of the 2nd Workshop on Economics of Peer-to-Peer Systems, 2004, pp. 1–6.
[9] L. Xiong, L. Liu, Peertrust: supporting reputation-based trust for peer-to-peer electronic communities, IEEE Transactions on Knowledge and Data Engineering 16 (2004) 843–857.
[10] R. Zhou, K. Hwang, Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing, IEEE Transactions on Parallel and Distributed Systems (2007) 460–473
[11] S. Chen, Y. Zhang, Q. Liu, and J. Feng, "Dealing with dishonest recommendation: The trials in reputation management court," Ad Hoc Networks, pp. 1603-1618, 2012
[12] H. Yu, S. Liu, A. C. Kot, C. Miao, and C. Leung, "Dynamic witness selection for trustworthy distributed cooperative sensing in cognitive radio networks," in Proc. 13th IEEE Int. Conf. Commun. Technol., pp. 1-6, Sep. 2011
[13] S.Buchegger, and J. Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems, " Communications Magazine, IEEE, pp. 101-107, 2005
[14] C. Zouridaki et al., "A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs," Proc. 3rd ACM Wksp. Sec. Ad Hoc and Sensor Networks, Alexandria, VA, Nov. 7, 2005
[15] N. Wilson, "Algorithms for Dempster-shafer theory," in Algorithms for Uncertainty and Defeasible Reasoning, pp. 421–475, Kluwer Academic Publishers, 2000
[16] A. Josang, R. Ismail, The beta reputation system, in: Proceedings of the 15th Bled Electronic Commerce Conference, 2002, pp. 324–337.
[17] F. Li, J. Wu, Mobility reduces uncertainty in MANETs, in: Proceedings of INFOCOM'07, 2007, pp. 1946–1954
[18] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, NJ, 1976
[19] A. Josang, Trust-based decision making for electronic transactions, in: Proceedings of NORDSEC'99, Stockholm University, Sweden, 1999
[20] A. L. Jousselme, D. Grenier, and E. Bosse, "A new distance between two bodies of evidence," Information Fusion, vol. 2, no. 2, pp. 91–101, 2001
[21] J.L. Herlocker, J.A. Konstan, L.G. Terveen and J.T. Riedl, "Evaluating collaborative filtering recommender systems", ACM Trans. Information Systems, Vol.22, no.1, pp.5-53, 2004
[22] R. Feng, S. Che, X. Wang, and N. Yu, "A credible routing based on a novel trust mechanism in ad hoc networks," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 652051, 12 pages, 2013
[23] X. Li, M. R. Lyu, and J. Liu, "A Trust Model Based Routing Protocol for Secure Ad Hoc Networks," in Proc. Aerospace Conference, IEEE, Vol. 2, pp. 1286-1295, 2004

Author Profile

Shirina Samreen did B.Tech in Computer Science & Engg from JNTU, Hyderabad, A.P., India in 2003 and M.Tech in Computer Science from JNTU, Hyderabad, A.P., India in 2006. She is currently working towards the Ph.D degree in the Department of Computer Science & Engineering, Jawaharlal Nehru Technological University, Hyderabad, A.P., India. She worked at various Engineering colleges and has 10 years technical teaching experience. Her current research interests include wireless security, secure routing, and trust management frameworks.